



Boletín temático
de jurisprudencia

DERECHOS en el escenario DIGITAL y de las TIC

Justicia  Clara



Corte Constitucional de Colombia

Sala Plena 2026

Paola Andrea Meneses Mosquera

Presidenta

Natalia Ángel Cabo

Vicepresidenta

Carlos Camargo Assis

Héctor Alfonso Carvajal Londoño

Juan Carlos Cortés González

Lina Marcela Escobar Martínez

Vladimir Fernández Andrade

Jorge Enrique Ibáñez Najar

Miguel Polo Rosero

Andrea Liliana Romero López

Secretaria General



DERECHOS en el escenario DIGITAL y de las TIC



Coordinación editorial

Ana María Ramos Serrano
Magistrada Auxiliar de Sala Plena

María del Pilar Forero Ramírez
Relatora de Constitucionalidad

José Francisco Ortega Bolaños
Relator de tutela

Édgar Raúl Rodríguez Arango
Relator de Conflictos entre
Jurisdicciones

Juan Camilo Rivadeneira Vélez
Jefe de Divulgación y Prensa

Equipo editorial

Daniela Alejandra Pascuaza Sánchez
Abogada Grado 21

Pablo Andrés Martínez Díaz
Oficial Mayor

Daniela Campo Rayo
Auxiliar Judicial Grado 2

Diseño y diagramación

Clara Patricia Montoya Henao
Profesional Universitario Grado 14

Andrés Eduardo Segura Barón
Profesional Universitario Grado 14



DERECHOS en el escenario DIGITAL y de las TIC



ÍNDICE

ÍNDICE



DERECHOS en el escenario DIGITAL y de las TIC



Presentación	9
Índice de siglas y abreviaturas	12
Glosario	15
Listado de sentencias	24
1. Contexto general	26
2. Acceso a internet y su utilización como herramienta para materializar otros derechos	29
2.1. Acceso a internet en el marco del ejercicio del derecho a la protesta social.....	33
2.2. Acceso a internet como parte de la faceta prestacional del derecho a la educación	35
2.3. Acceso a internet para garantizar el derecho a la salud	36
3. Derecho a la libertad de expresión en el contexto digital	38
3.1. Procedencia de la tutela en casos donde se advierta un abuso del derecho a la libertad de expresión en redes sociales.....	40
3.2. Límites a la libertad de expresión y discursos no protegidos.....	43
3.3. Alcance de la responsabilidad y de las facultades sancionatorias de los intermediarios y administradores de plataformas digitales.....	45
3.4. Libertad de opinión y de información en el entorno digital.....	52
3.5. Difusión de acusaciones y expresiones difamatorias en redes sociales.....	53
3.6. La denuncia pública de violencia contra las mujeres como discurso especialmente protegido “Escache”	56
3.7. Deberes de las y los funcionarios públicos que interactúan en redes sociales.....	61
3.8. Estándares de protección de derechos fundamentales en el ejercicio del periodismo digital	63



4. Derecho a la imagen en entornos digitales.....	70
4.1 Difusión de videos y fotografías en páginas web o redes sociales....	73
4.2 Alcance constitucional de la autorización para el uso de la propia imagen.....	77
4.3. Protección del derecho a la imagen de los niños, niñas y adolescentes en entornos digitales	79
4.4. Uso de imágenes para fines distintos a los concertados con la persona titular	81
4.5. Imágenes captadas por cámaras de video de seguridad	83
5. La administración de justicia en el marco del uso de nuevas tecnologías y de la inteligencia artificial.....	88
5.1. Competencia de los jueces constitucionales colombianos para dirimir asuntos que involucran intermediarios con sede extranjera	92
5.2. Publicación de información y administración de los sistemas de consulta de la página web de la Rama Judicial.....	94
5.3. Valoración probatoria de los mensajes de datos y las capturas de pantalla.....	96
5.4 Acceso a la información privada enviada por correo electrónico para servir como medio de prueba en procesos judiciales.....	101
5.5. Notificación personal para la presentación y sustentación de recursos judiciales por medios electrónicos.....	102
5.6. Uso de la inteligencia artificial en la administración de justicia.....	103
6. Derechos de acceso a la información pública y de petición en contextos digitales	110
6.1. Derecho al acceso a la información pública a través de redes sociales.....	115
6.2. Derecho de acceso a la información pública relacionada con sistemas de toma de decisiones automatizadas.....	118



6.3. Derecho de petición por medios tecnológicos	124
7. Derecho a la participación política en el plano de la democracia digital.....	127
7.1. Encuestas electorales realizadas a través de internet	128
7.2. Derecho a la participación política a través de redes sociales y protección a las mujeres ante todo tipo de violencia.....	129
7.3. Transmisión por parte de la ciudadanía de sesiones de los órganos colegiados del Estado a través de redes sociales a través de redes sociales	130
8. Derecho al habeas data en el marco del uso de nuevas tecnologías	132
8.1. Tratamiento de información sobre transacciones económicas realizadas en Internet	140
8.2. Administración de datos personales relacionados con anotaciones, requerimientos, antecedentes y procesos judiciales o administrativos	141
8.3. Administración de información relacionada con programas sociales del Estado e inscripciones a pruebas académicas.....	143
8.4. Administración de datos personales contenidos en historias clínicas	146
8.5. Derecho al habeas data financiero	147
8.6. Administración de datos contenidos en la historia laboral.....	150
8.7. Uso de datos personales recopilados en el marco de medidas de protección	152
8.8. Bases de datos que solo contienen datos negativos ²³	152
9. Derecho al trabajo a través del uso de medios tecnológicos y digitales.....	154
9.1. Teletrabajo como medida de inclusión laboral a personas con afectaciones de salud	160



9.2. Teletrabajo como opción de protección a la unidad familiar	162
9.3. Trabajo en casa como medida de protección a las víctimas del desplazamiento forzado	163
9.4. Trabajo sexual por medio de plataformas digitales (modelaje webcam)	164
9.5. Protección constitucional de las actividades desarrolladas por los y las influenciadoras digitales	166
10. Derecho a la personalidad jurídica y a la identificación a través de documentos digitales.....	170
10.1. Identidad de género en la cédula digital	171
10.2. Garantías para el uso de la firma digital	172
10.3. Protección de datos e implementación de sistemas de identificación biométrica	176
11. Protección constitucional frente a riesgos asociados a la interacción en el escenario digital.....	178
11.1. Violencia digital o violencia en línea	179
11.2. Ciberacoso o cyberbullying escolar	181
11.3. Sharenting o exposición de información de niños o niñas en redes sociales por parte de sus padres.....	183
11.4. Ciberdelincuencia y suplantación de identidad en trámites virtuales	184
11.5. Uso indebido de las redes sociales como mecanismos extraprocesales de cobro	185
Buscador de Relatoría	187
Índice de normas.....	188



DERECHOS en el escenario DIGITAL y de las TIC



PRESENTACIÓN

INDICE



DERECHOS en el escenario DIGITAL y de las TIC



La Relatoría de la Corte Constitucional presenta este boletín temático sobre derechos en el escenario digital y de las tecnologías de la información con el objetivo de divulgar, de manera clara, accesible y efectiva las decisiones adoptadas por la Corte. Este documento busca que las personas puedan conocer y utilizar la jurisprudencia constitucional como una herramienta efectiva para la protección de sus derechos. Con ese fin, se sistematizan breves reseñas de las providencias en las que se abordaron casos relacionados con la protección de derechos en entornos digitales. Además, estas síntesis o referencias incluyen extractos textuales de las decisiones, los cuales se destacan en recuadros.

Respecto al contenido, luego de exponer (i) un contexto general sobre el tema, la información jurisprudencial se agrupa en diversos ejes relacionados con: (ii) acceso a internet y su utilización como herramienta para materializar otros derechos; (iii) el derecho a la libertad de expresión en el contexto digital; (iv) el derecho a la imagen en entornos digitales; (v) la administración de justicia en el marco del uso de nuevas tecnologías y de la inteligencia artificial; (vi) los derechos de acceso a la información pública y de derecho de petición en contextos digitales; (vii) el derecho a la participación política en el plano de la democracia digital; (viii) el derecho al habeas data en el marco del uso de nuevas tecnologías; (ix) el derecho al trabajo a través del uso de medios tecnológicos y digitales; (x) el derecho a la personalidad jurídica y a la identificación a través de documentos digitales; y por último, (xi) la protección constitucional frente a la violencia y la delincuencia en el escenario digital.



Es importante destacar que la clasificación temática utilizada en este boletín responde únicamente a fines organizativos y didácticos. De esa forma, no debe perderse de vista que los casos estudiados por la Corte que aquí se mencionan trascienden categorías únicas ya que, muchas veces, los derechos amparados son interdependientes y los pronunciamientos abordan una pluralidad de asuntos relevantes en materia constitucional. Por ello, los resúmenes buscan facilitar la comprensión, pero no pretenden simplificar ni reemplazar los análisis detallados de las sentencias. Para un entendimiento completo y preciso de los pronunciamientos, se recomienda consultar siempre los textos originales de las providencias.

Con el fin de facilitar la consulta, el documento está enriquecido con recursos como tablas y gráficas. Asimismo, se ofrecen hipervínculos para el acceso directo a las providencias completas, las cuales pueden ser ubicadas también mediante el [Buscador de la Relatoría](#). Es importante notar que las sentencias se citan bajo dos formatos: extendido (p. ej., T-567 de 2023) para el texto principal y abreviado (T-567/23) en cuadros y gráficos.

Adicionalmente, se han incorporado herramientas de referencia como: (i) un índice de siglas y abreviaturas; (ii) un glosario con conceptos claves extraídos de la jurisprudencia y la normatividad allí citada; (iii) un índice de normas nacionales e internacionales relacionadas con la protección de derechos en el contexto digital conforme con la jurisprudencia y; (iv) algunos hipervínculos que dirigen a videos producidos por la Corte, los cuales ofrecen una descripción complementaria de los casos mencionados.



DERECHOS en el escenario DIGITAL y de las TIC



ÍNDICE DE SIGLAS Y ABREVIATURAS

ÍNDICE



DERECHOS en el escenario DIGITAL y de las TIC



- ANE** Agencia Nacional del Espectro
- AND** Agencia Nacional de Gobierno Digital
- CADH** Convención Americana sobre Derechos Humanos
- CCVTT** Circuito Cerrado de Televisión
- CIDH** Comisión Interamericana de Derechos Humanos
- CNE** Consejo Nacional Electoral
- CP** Constitución Política
- Cons.S.Jud** Consejo Superior de la Judicatura
- DIAN** Dirección de Impuestos y Aduanas Nacionales
- DNP** Departamento Nacional de Planeación
- EPS** Entidades Promotoras de Salud
- FGN** Fiscalía General de la Nación
- FLIP** Fundación para la Libertad de Prensa
- IA** Inteligencia Artificial
- ICBF** Instituto Colombiano de Bienestar Familiar
- MinTic** Ministerio de Tecnologías de la Información y las Comunicaciones
- OCDE** Organización para la Cooperación y el Desarrollo Económicos
- OEA** Organización de Estados Americanos
- OIT** Organización Internacional del Trabajo
- ONAC** Organismo Nacional de Acreditación de Colombia
- ONU** Organización de las Naciones Unidas
- PIDCP** Pacto de Derechos Civiles y Políticos



DERECHOS en el escenario DIGITAL y de las TIC



- PETD** Plan Estratégico de Transformación Digital para la Rama Judicial
- PGN** Procuraduría General de la Nación
- REDAM** Registro de Deudores Alimentarios Morosos
- SDA** Sistema de Toma de Decisiones Automatizadas
- SENA** Servicio Nacional de Aprendizaje
- SGSSP** Sistema General de Seguridad Social en Pensiones
- SIC** Superintendencia de Industria y Comercio
- SIEL** Servicio de Interpretación en Línea
- SPA** Sustancias Psicoactivas
- SPOA** Sistema Penal Oral Acusatorio
- TEDH** Tribunal Europeo de Derechos Humanos
- TEA** Trastorno del Espectro Autista
- TIC** Tecnologías de la Información y la Comunicación
- UNP** Unidad Nacional de Protección
- VCMP** Violencia Digital contra las Mujeres en Política
- VIH** Virus de Inmunodeficiencia Humana



DERECHOS en el escenario DIGITAL y de las TIC



GLOSARIO



INDICE



Algoritmo: serie de pasos ordenados que hacen que una información de entrada - “input”- se convierta en un resultado –“output”, y puede ser implementado en forma de un programa de computación que resuelve el problema de forma automatizada y mucho más veloz. Sin embargo, para que un computador tenga la capacidad de entender y procesar un algoritmo, este debe ser traducido a un lenguaje computacional. [\(T-067 de 2025\)](#)

Base de datos: corresponde al conjunto sistematizado de información personal que puede ser tratada de alguna manera, como ocurre con el ejercicio de los atributos de recolección, uso, almacenamiento, circulación o supresión. [\(T-020 de 2014\)](#)

Big Data: existencia de altos volúmenes de datos, de gran complejidad y variedad, que pueden ser utilizados por los sistemas computacionales para la toma de decisiones. [\(T-067 de 2025\)](#)

Brecha digital: diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a las TIC y aquellas que no, y también hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las TIC de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica. [\(T-193 de 2021\)](#)¹.

Censura: en un sentido negativo, consiste en la obstaculización del flujo comunicativo o la prohibición de publicar un mensaje total o parcialmente; y en un sentido positivo, se da cuando se exige la adecuación de un contenido a los parámetros fijados por el censor. [\(T-475 de 2024\)](#)

¹ Ministerio de Tecnologías de la Información y las Comunicaciones. “Brecha digital”. Texto citado en la sentencia T-193 de 2021. M.P Antonio José Lizarazo Ocampo



Censura previa: cualquier mecanismo directo o indirecto dirigido a realizar un control previo sobre (i) los medios de comunicación y su funcionamiento; (ii) el acceso a la información; (iii) los periodistas; o (iv) el contenido de determinada información se encuentra proscrito en nuestro ordenamiento jurídico. [\(T-145 de 2019\)](#)

Ciberacoso (hostigamiento): ejercicio abusivo de la libertad de expresión con tres características esenciales: (i) la publicación reiterada y sistemática de vejaciones, insultos y expresiones desproporcionadas en contra de una persona en redes sociales y medios digitales; (ii) la “intención dañina y ofensiva” del emisor y, (iii) el desconocimiento del “derecho a vivir sin humillaciones reconocido por la jurisprudencia como parte integral de la dignidad humana. [\(T-242 de 2022\)](#)

Circuito Cerrado de Televisión o Closed Circuit Television–CCTV-: conjunto de componentes directamente entrelazados, compuesto de una o varias cámaras de vigilancia conectadas a uno o más monitores o televisores, los cuales reproducen imágenes capturadas que crean un circuito de imágenes. Estas imágenes pueden ser almacenadas en medios analógicos o digitales. [\(T-114 de 2018 y C-094 de 2020\)](#)

Código fuente: es la columna vertebral del software o la aplicación, y es lo que proporciona la estructura y las directrices necesarias para que se ejecuten las instrucciones o pasos previstos en el algoritmo. Estos pasos pueden consistir en procesar datos, tomar decisiones y producir resultados. [\(T-067 de 2025\)](#)

Dato personal: corresponde, según el artículo 3° de la Ley 1581 de 2012, a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Por ende, la noción de dato personal no está asociada, como común y erróneamente suele considerarse, con algún atributo sobre la circulación del dato, sino simplemente sobre su naturaleza como información descriptiva acerca de un determinado sujeto. [\(T-294 de 2023\)](#)



Derecho al olvido: también conocido como el “principio de la caducidad del dato negativo”, ha sido reconocido por la jurisprudencia constitucional como el derecho que tiene el titular de un dato negativo a que dicho dato sea eliminado de la base de datos respectiva, por el paso del tiempo. ([T-125 de 2025](#))

El derecho a la supresión o al olvido supone una extensión de los principios superiores de privacidad, autodeterminación y libertad. En consecuencia, la información de un sujeto no debe mantenerse a perpetuidad en una base de datos, sin que medie, o la autorización del titular de los datos, o un mandato legal explícito. ([T-294 de 2023](#))

Discurso de odio: se trata de un mensaje oral, escrito o simbólico que excede la simple emisión de una palabra u opinión, el cual es dirigido contra personas o grupos que han sido sistemáticamente discriminados y que es capaz de producir un daño. ([SU-355 de 2019](#))

Educación en línea: supone la interacción de mediadores y estudiantes en un entorno digital y de manera sincrónica, mediante recursos tecnológicos y facilidades proporcionadas por el internet y las redes sociales, en donde los estudiantes deben coincidir en los horarios de la sesión. En este modelo los mediadores reciben el nombre de “tutores” porque, a diferencia de un aula física, su rol es acompañar y asistir al estudiante en su proceso autónomo de aprendizaje. ([SU-032 de 2022](#))

Educación virtual: requiere de recursos tecnológicos obligatorios, conexión a internet y una plataforma virtual interactiva. La educación virtual funciona de manera asincrónica, es decir, los estudiantes pueden y deben revisar los materiales debidamente preparados con suficiente antelación sobre el curso en cualquier momento, sin que sus horarios deban coincidir con los de las sesiones definidas por los mediadores o tutores. ([SU-032 de 2022](#))

Educación a distancia: puede tener un porcentaje presencial y otro virtual. En este modelo los alumnos tienen control sobre el tiempo, el espacio y el



ritmo de su aprendizaje. No necesita conexión a internet o recursos tecnológicos. Los materiales son normalmente físicos, como cuadernos, plumas, colores, o memorias USB, CD, entre otros, e incluso estos se transmiten mediante el correo postal, la radio o la televisión. ([SU-032 de 2022](#))

Exceptio veritatis: consiste en una herramienta de defensa que tienen las personas señaladas de afectar la honra o buen nombre de otras. Es liberadora de responsabilidad cuando se pruebe la veracidad de las informaciones dentro del proceso. ([T-277 de 2018](#) y [T-145 de 2025](#)).

IA Generativa: sistemas computacionales que se comunican en lenguaje natural, es decir, se comunican de manera similar a como lo harían los humanos, que son capaces de dar respuestas a preguntas relativamente complejas y pueden crear contenidos, proporcionar un texto, imagen o sonido, siguiendo una pregunta formulada o instrucciones (prompt). La IA generativa, en lugar de conservar las páginas web existentes, genera nuevos contenidos de forma automática en respuesta a instrucciones en interfaces conversacionales de lenguaje natural (prompts). Normalmente, las aplicaciones informáticas conocidas como chatbots operan a partir de estos sistemas.² ([Acuerdo PCS-JA24-12243](#))³.

Es un sistema basado en una máquina que, ya sea para alcanzar objetivos explícitos o implícitos, infiere -a partir de la entrada que recibe- cómo generar salidas, tales como predicciones, contenidos, recomendaciones o decisiones, las cuales pueden influir en entornos físicos o virtuales. Los diferentes sistemas de IA varían en sus niveles de autonomía y capacidad de adaptación después de su implementación. ([T-323 de 2024](#))⁴.

²

³ Acuerdo PCSJA24-12243 del 16 de diciembre de 2024 expedido por el Consejo Superior de la Judicatura "Por el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial".

⁴ El memorando realiza aclaraciones a la definición de sistema de IA contenida en el documento Recommendation of The Council of Artificial Intelligence (OCDE, 2019), adoptadas el 21 de mayo de 2019. Citado en la sentencia T-323 de 2024.



Información privada: esta es información personal y, por encontrarse en un ámbito privado, solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, los documentos privados y la información extraída a partir de la inspección del domicilio. [\(T-153 de 2024\)](#)

Información pública: es aquella que, según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si se trata de información general, privada o personal. En esta categoría se encuentran, por ejemplo, los documentos públicos, las providencias judiciales debidamente ejecutoriadas, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Este tipo de información se puede solicitar por cualquier persona de manera directa y no existe el deber de satisfacer algún requisito para obtenerla. [\(T-153 de 2024\)](#)

Información reservada: es la que versa sobre información personal y guarda estrecha relación con los derechos fundamentales del titular a la dignidad, a la intimidad y a la libertad. Por ese motivo se encuentra reservada a su órbita exclusiva y, según la sentencia T-828 de 2014, “no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones”. Algunos ejemplos sobre este tipo de información son la información genética, aquellos datos relacionados con la ideología, la orientación sexual, los hábitos de la persona o la historia clínica. [\(T-153 de 2024\)](#)

Información semiprivada: se refiere a los datos que versan sobre información personal o impersonal, su acceso y conocimiento presenta un grado mínimo de limitación. Así, solo puede ser obtenida y ofrecida por orden de autoridad en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Dos ejemplos de este tipo de información pueden ser los datos relativos a las relaciones con las entidades de la seguridad social y al comportamiento financiero de las personas. [\(T-153 de 2024\)](#)



Medios electrónicos: herramientas que permiten la producción, almacenamiento o transmisión digitalizada de documentos, datos e informaciones, a través de cualquier red de comunicación abierta o restringida. ([T-230 de 2020](#))

Mensaje de datos: información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.⁵ ([C-604 de 2016](#))⁶

Neutralidad de la red: libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet, ejercicio que no debe estar condicionado, direccionado o restringido, por medio de bloqueo, filtración, o interferencia. Se trata de una condición necesaria para ejercer la libertad de expresión en Internet en los términos del artículo 13 de la Convención Americana. ([SU-420 de 2019](#))

Poder informático: especie de dominio social sobre el individuo, que consiste en la posibilidad de acumular informaciones en cantidad ilimitada. La administración de cualquier base de datos personales confiere poder informático a quien la controla, o a quien puede tener acceso (autorizado o no) a sus contenidos. ([T-509 de 2020](#), [SU-458 de 2012](#) y [T-414 de 1992](#)) .

Prueba electrónica: cualquier prueba presentada informáticamente y que estaría compuesta por dos elementos: uno material, que depende de un hardware, es decir la parte física de la prueba y visible para cualquier usuario de a pie, por ejemplo, la carcasa de un Smartphone o un USB; y por otro lado un

⁵

⁶ Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones” Art. 2 a): La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax. Citado en la sentencia C-604 de 2016. M.P Luis Ernesto Vargas Silva.



DERECHOS en el escenario DIGITAL y de las TIC



elemento intangible que es representado por un software, consistente en metadatos y archivos electrónicos modulados a través de unas interfaces informáticas. [\(T-043 de 2020\)](#)⁷

Red social: espacio digital que ha promovido la comunicación inmediata entre distintos actores y el acceso directo a información, casi que en tiempo real. Funciona como una plataforma de comunicaciones que permite conectar gente que se conoce o que desea conocerse, y que les permite centralizar recursos, como fotos y videos, en un lugar fácil de acceder y administrados por los usuarios mismos. [\(T-230 de 2020\)](#)⁸.

Servicio de redes sociales: servicios basados en la web que permiten a los usuarios construir un perfil público o semipúblico dentro de un sistema delimitado, conectar con otros usuarios y explorar sus redes. Estos servicios de redes sociales habitan Internet como espacios dinámicos y en constante actualización, donde la comunicación fluye de manera inmediata y global. [\(T-256 de 2025\)](#)

Tecnologías de la Información y las Comunicaciones (TIC): conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. [\(T-230 de 2020\)](#)

⁷ Federico Bueno de Mata, “Prueba electrónica y proceso 2.0”, editorial Tirant lo Blanch extraído de la sentencia. Citado en la sentencia T-043 de 2020 M.P José Fernando Reyes Cuartas.

⁸ Manual de Gestión de la Comunicación en Redes Sociales, Gobierno de Colombia. Texto citado en la Sentencia T-230 de 2020. M.P Luis Guillermo Guerrero Pérez.



DERECHOS en el escenario DIGITAL y de las TIC



Violencia Digital contra las Mujeres en Política (VCMP): esta violencia se manifiesta a través de conductas que intentan ridiculizar y deslegitimar la capacidad de liderazgo, gestión y conocimientos de las mujeres en política a través de la reproducción de estereotipos de género que buscan limitar la presencia de las mujeres en el espacio público y la toma de decisiones. Este tipo de violencia se basa en el uso de internet y redes sociales como mecanismo de discriminación, silenciamiento y control de las mujeres en el ejercicio político en espacios digitales. ([T-149 de 2025](#))





DERECHOS en el escenario DIGITAL y de las TIC



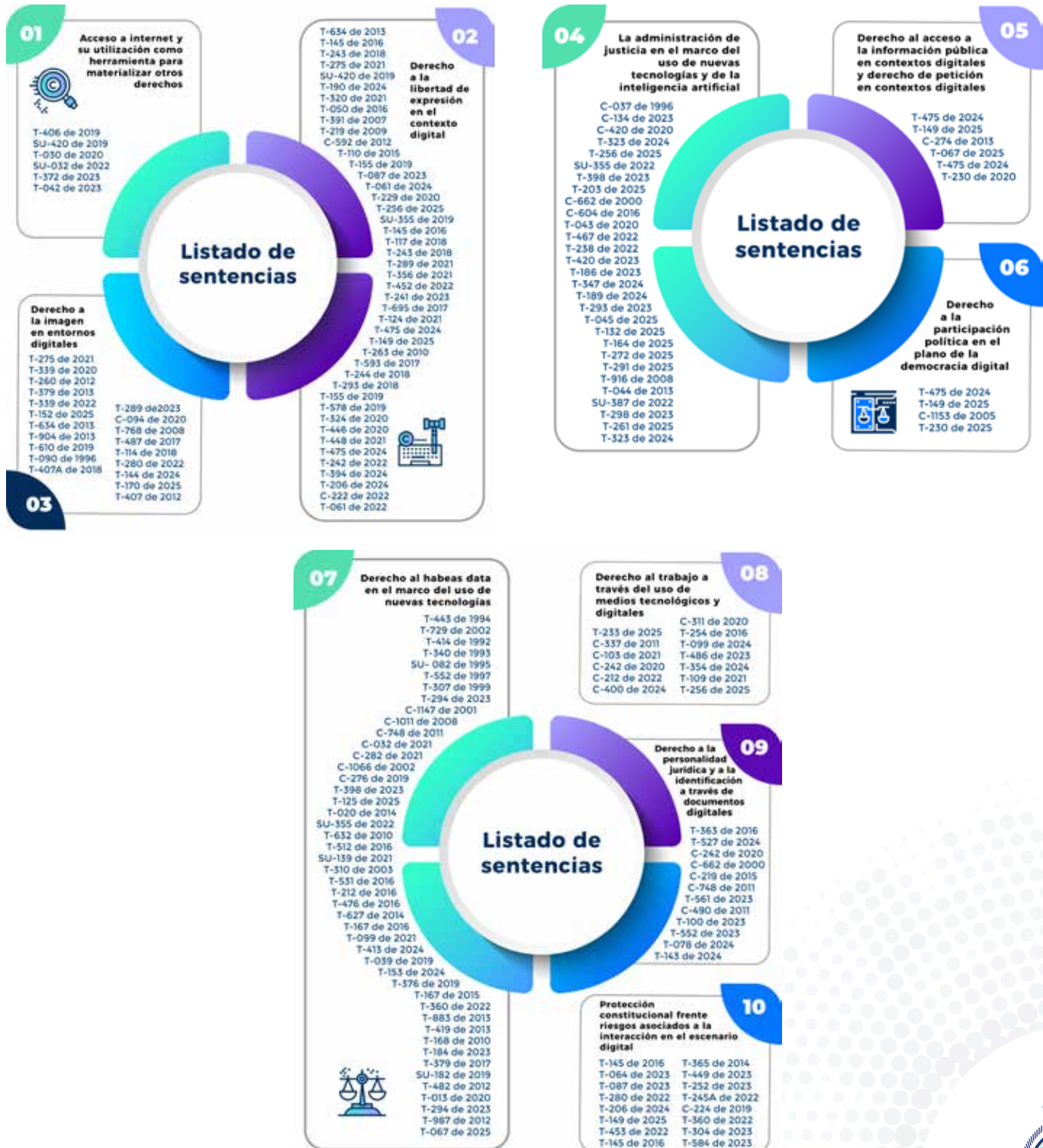
LISTADO DE SENTENCIAS



INDICE



DERECHOS en el escenario DIGITAL y de las TIC





DERECHOS en el escenario DIGITAL y de las TIC



1. CONTEXTO GENERAL





La jurisprudencia constitucional ha reconocido el aporte y el desafío que representa el uso de nuevas tecnologías de la información y de las comunicaciones y su impacto en la garantía de los derechos constitucionalmente protegidos. Al respecto, en la sentencia [C-662 de 2000](#) la Corte mencionó que los progresos e innovaciones tecnológicas logrados principalmente durante las dos últimas décadas del siglo XX revolucionaron las comunicaciones gracias al surgimiento de redes informáticas, las cuales han puesto a disposición de la humanidad, nuevos medios de intercambio y de comunicación.

En el mismo sentido, la sentencia [C-1147 de 2001](#) resaltó que el sistema jurídico se ve constantemente forzado a evolucionar debido al incesante progreso de la ciencia y la tecnología. Añadió esta providencia que los desarrollos como nuevas técnicas de producción o complejas formas de comunicación transforman la estructura política y económica, lo que obliga al derecho a crear respuestas para regular sus efectos en las transacciones, la distribución de bienes y servicios y el ejercicio de los derechos fundamentales.



Sentencia **C-1147 de 2001**

A nadie escapa el valor que tienen dentro de un sistema global de comunicaciones, como Internet, derechos y libertades tan importantes para la democracia como el derecho a la igualdad, la intimidad y el habeas data, la libertad de conciencia o de cultos, la libertad de expresión, el libre ejercicio de una profesión u oficio, el secreto profesional y el ejercicio de los derechos políticos que permiten a los particulares participar en las decisiones que los afectan, por citar tan sólo algunos ejemplos. Nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales.



DERECHOS en el escenario DIGITAL y de las TIC



Este contexto ha llevado al juez constitucional a enfrentarse a nuevos y variados problemas jurídicos vinculados a la protección de derechos fundamentales en el marco del uso del Internet, de plataformas digitales, de redes sociales o de herramientas como la Inteligencia Artificial -IA. Cabe anotar que la pandemia de Covid-19, aceleró drásticamente el uso de algunas de estas herramientas y motivó un amplio despliegue institucional para regular su utilización. Incluso muchas de las disposiciones o de las medidas adoptadas en esa coyuntura se mantienen en el ordenamiento jurídico, como respuesta a esa realidad postpandémica, cada vez más inmersa en el entorno digital.

En ese sentido, la Corte ha abordado diversos asuntos en sede de tutela y de constitucionalidad relacionados con este tema, sobre los cuales se hará referencia en los capítulos siguientes. Cada una de las providencias adoptadas por la Corte en esta materia, refleja el intento por construir un precedente sólido y garante de la vigencia de la Constitución Política, con el fin de que estas herramientas siempre estén al servicio de las personas y no en detrimento de sus derechos.



Sentencia *T-323 de 2024*

Se trata de aprender de la historia de la humanidad y de los desarrollos tecnológicos, siempre en cambio, así como de afrontar el reto de racionalizar sobre estos y de aprender sobre sus inusitados alcances, para que, sin caer en la esclavitud ante ellos, el ser humano los apropie como herramientas para potenciar las mejores condiciones de vida individuales, sociales y globales.



DERECHOS en el escenario DIGITAL y de las TIC



2. ACCESO A INTERNET Y SU UTILIZACIÓN COMO HERRAMIENTA PARA MATERIALIZAR OTROS DERECHOS

“En nuestro actual modo de vida en sociedad, el internet permite al individuo, no solo informarse y adquirir conocimiento, sino también tomar decisiones vitales e interrelacionarse adecuadamente en comunidad. Es decir que el internet hoy no puede entenderse como un simple servicio público, sino que su acceso se constituye en un verdadero derecho”.

Sentencia T-372 de 2023



La Corte Constitucional reconoce la existencia de nuevas formas de comunicación marcadas por los avances tecnológicos, en ese contexto se destaca el papel protagónico del internet.⁹



Sentencia **T-372 de 2023**

El acceso a internet se traduce en un derecho subjetivo del cual se desprenden unos deberes de abstención y prestación a cargo del Estado. Por un lado, una primera faceta protege a los ciudadanos frente a restricciones ilegítimas y en ese sentido resultan aplicables los parámetros –en términos generales equiparables de la libertad de expresión– de legalidad, necesidad y proporcionalidad. Por otro lado, en su faceta prestacional, corresponderá al legislador dotar su contenido a partir, entre otros parámetros, del reconocimiento de la brecha digital existente.

Por su parte, en la sentencia [SU-420 de 2019](#), la Corte refirió que la finalidad de la neutralidad de la red como regla que surge de los principios de acceso en condiciones de igualdad y de no discriminación, es “evitar situaciones de bloqueo, interferencia o filtración (...)”. Sin embargo, advirtió que, pese a que este estándar es de aplicación general para todo el tráfico de información en la red, el mismo admite algunas excepciones:

⁹ Sentencia T-372 de 2023. M.P. Natalia Ángel Cabo.



Sentencia SU-420 de 2019

Se han identificado tres excepciones a este mandato por parte de la Relatoría Especial sobre Libertad de Expresión de la CIDH, estas son: (i) preservar la integridad y seguridad de la red; (ii) para prevenir la transmisión de contenidos no deseados por expresa solicitud –libre y no incentivada– del usuario; y (iii) para gestionar temporal y excepcionalmente la congestión de la red.

De igual forma, en este pronunciamiento la Corte hizo referencia, con base en algunas intervenciones, a los actores en Internet, cuál es su autorregulación y cuál es su régimen de responsabilidad, así:

- **Los usuarios en las nuevas tecnologías:** se pueden clasificar en identificables o anónimos, dado que su interacción normalmente se da a través de perfiles. Los perfiles identificables son usados por personas que tienen un amplio reconocimiento social (políticos, actores, cantantes, deportistas, entre otros), normalmente certificados por las propias plataformas, y aquellos propios de las personas que no cuentan con estas especiales características.

Por su parte, el anonimato y los pseudónimos en la red surgen como una necesidad de contrarrestar el uso invasivo que efectuaban algunas compañías dentro de la web, o incluso gobiernos, sobre la información de los usuarios. En consecuencia, el anonimato y el uso específico de nombres falsos se han convertido en una opción para esconder la identidad de los usuarios, para navegar en la red y hacer uso de los diversos servicios que ofrece Internet.



- **Los intermediarios en el uso de las nuevas tecnologías:** son actores, en la mayoría de los casos privados, que de una u otra forma determinan y posibilitan las interacciones en línea. Existen distintos tipos de clasificaciones, pero en términos generales se dividen entre aquellos que suministran la conexión o un servicio técnico relacionado, y aquellos que alojan contenidos o prestan un servicio.

Entre ellos se encuentran las plataformas digitales, las cuales tienen un rol dual: i) **pasivo** facilitando el proceso de transmisión y difusión de un contenido más no toman decisiones sobre la difusión, es decir, “dan acceso, alojamiento transmisión e indexación a contenidos, producto y servicios, que se originan en terceros”, escenario donde facilitan la libertad de expresión; y ii) **activo** en la medida que pueden adoptar un modelo de negocios basado en datos, lo que implica que “a partir de la recolección y análisis descriptivo y prescriptivo de los datos de sus usuarios, las compañías como Facebook y Google formulan ‘modelos de negocios que confían en los datos como un recurso clave’ para extraer valor económico social”.

- **Responsabilidad de intermediarios:** a pesar de que estas plataformas no son las llamadas a responder por el contenido que publican sus usuarios, en caso de que una autoridad judicial encuentre que un contenido atenta contra los derechos fundamentales de una persona, puede ordenar su remoción directamente a los intermediarios de Internet, en orden a generar una garantía efectiva de las prerrogativas de la persona afectada, porque el infractor no quiere o no puede cumplir con lo ordenado por un juez.¹⁰

A continuación, se exponen algunos casos en los cuales la Corte se ha pronunciado sobre el acceso a Internet en diversos escenarios.

¹⁰ Respecto a este tema se pueden consultar también las sentencias T-277 de 2015, T-243 de 2018, SU-420 de 2019, T-229 de 2020, T-445 de 2021 y T-289 de 2023.



2.1. Acceso a internet en el marco del ejercicio del derecho a la protesta social

En la sentencia [T-372 de 2023](#), la Corte estudió una acción de tutela interpuesta por varios líderes de organizaciones defensoras de la libertad de prensa, quienes alegaron que las entidades accionadas vulneraron los derechos a la libertad de expresión y de asociación durante las protestas en contra del Gobierno Nacional, realizadas en el año 2021. Los accionantes sostuvieron que el uso de inhibidores de señal para interrumpir el servicio de internet durante las manifestaciones impidió denunciar digitalmente los abusos de la fuerza pública.

En esta oportunidad, la Corte señaló que, el Estado debe garantizar el acceso a la información pública y la prestación del servicio de internet sin injerencias indebidas, con mayor atención en contextos de manifestación, al ser estos escenarios de alto interés público cuando la ciudadanía requiere estar más informada. En esta ocasión, se ampararon los derechos de los accionantes y se exhortó al Congreso de la República para que regule la adquisición y uso de los dispositivos inhibidores de señal.

Respecto al acceso al internet, la Corte hizo un recuento de algunos instrumentos internacionales¹¹ que, si bien no son vinculantes en estricto sentido, sí corresponden a criterios de interpretación sobre el acceso a internet que resultan de utilidad para abordar este tipo de casos. A partir de estos instrumentos, y de la normativa nacional la Corte extrajo las siguientes pautas:

¹¹ Resolución conjunta sobre la libertad de Expresión e Internet: El 1 de junio de 2021 las Relatorías de Libertad de Expresión Emitieron declaración conjunta acerca de internet. Compuesta por los siguientes: el Relator Especial de la ONU para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la OEA para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos. Consejo de Derechos Humanos de la ONU: Resolución 20/8 del 5 de julio de 2012 sobre la promoción, protección y disfrute de los derechos humanos en internet. Relatoría Especial para la Libertad de Expresión de la CIDH. 31 de diciembre de 2013. Párr. 157.



Pautas relacionadas con el acceso a internet

El acceso a internet es un derecho fundamental, que implica unos deberes de abstención y prestación a cargo del Estado.

El goce efectivo de la libertad de expresión, que se relaciona estrechamente con los derechos fundamentales a la reunión y de asociación, no admite, en principio, restricciones en el acceso al servicio de internet, incluso por motivos de orden público.

A nivel general no cabe ningún modo de control previo ni de censura en ese entorno digital. Ahora bien, cuando excepcionalmente se invoque la seguridad nacional como limitación al acceso a internet que repercute en el ejercicio de la libertad de expresión, la ley debe especificar el alcance de esa restricción.

En todo caso, para que una limitación sea conforme a la Constitución y al bloque de constitucionalidad, deberá corresponder a un fin imperioso, legítimo, necesario y proporcional.

La garantía a cargo del Estado sobre acceso al servicio de internet conlleva a evitar la perturbación intencional para acceder a información en línea por parte de toda la población o un segmento de ella y, además, un deber reforzado de pronunciarse oportunamente sobre las denuncias de bloqueos, a partir de información técnica, actualizada y accesible.

Gráfica 1. *Elaboración propia con base en la sentencia T-372 de 2023.*





2.2. Acceso a internet como parte de la faceta prestacional del derecho a la educación

En la sentencia [T-030 de 2020](#), la Corte amparó el derecho a la educación de algunos estudiantes de una institución educativa rural que se quedó sin acceso a internet. Esta vez la Corte señaló que el internet es una herramienta que puede ayudar a asegurar el goce efectivo del derecho fundamental a la educación, en especial, de personas que se encuentran en zonas apartadas. Así mismo, se destacó el papel del servicio de internet como una herramienta propia de nuestra actual sociedad de la información y, en particular, su importancia en el ámbito educativo.



Sentencia [T-030 de 2020](#)

El acceso que permite el internet y las nuevas tecnologías de la información a esos múltiples y variados recursos ayuda a cerrar las brechas entre los estudiantes, al dar a los profesores herramientas para garantizar el desarrollo armónico e integral de sus estudiantes, sin importar que tan apartada físicamente se encuentre la institución educativa.

Por su parte, en la sentencia [SU-032 de 2022](#) se conocieron tres acciones de tutela en donde se señaló que, con motivo de la pandemia generada por el COVID 19, las autoridades del sector educativo presuntamente vulneraron los derechos de dos niños y un adolescente, al adoptar e implementar medidas de educación no presencial, sin garantizar la conectividad y proveer los equipos de cómputo y de conexión a internet necesarios.



Aunque en este caso se declaró la carencia actual de objeto, la Corte ordenó al gobierno nacional: (i) formular, actualizar e implementar en 6 meses un plan nacional de evaluación de los impactos generados por la Covid19 en la comunidad educativa; (ii) conformar, en lo posible, una Comisión de Expertos para que en el mismo periodo de tiempo presente recomendaciones para reducir la brecha educativa profundizada por la emergencia; y (iii) formular, dentro del año siguiente, una política pública de prevención que permita reducir el impacto de situaciones de emergencia que alteren el funcionamiento normal del sistema educativo.

En esta oportunidad, también se destacó que el uso o no de la tecnología como mediadora de la educación, es uno de los elementos distintivos entre los modelos pedagógicos de educación presencia y no presencial, esta última incluye la educación en línea, la educación virtual y la educación a distancia.

En un caso similar abordado en la sentencia [T-042 de 2023](#), la Corte indicó que las reglas generales sobre accesibilidad a la educación en tiempo de pandemia deben asegurar que los niños y niñas puedan seguir estudiando, a pesar de la emergencia. Estas medidas adicionales deben tener en cuenta el nivel de riesgo sanitario, las desigualdades que se exacerban durante una emergencia pública y la necesidad de recurrir a las tecnologías como alternativa a la presencialidad. También se reiteraron las órdenes dadas en la sentencia [SU-032 de 2022](#), al evidenciarse la inexistencia de avances tangibles.

2.3. Acceso a internet para garantizar el derecho a la salud

En la sentencia [T-406 de 2019](#), la Corte protegió los derechos de un hombre trans en situación de discapacidad auditiva, a quien una EPS le negó la prestación del servicio de intérprete y no le permitió el acceso a la red de internet para conectarse al Centro de Relevó¹² como servicio de interpretación en línea SIEL,

¹² Proyecto que permite a las personas sordas acceder a un intérprete en línea y comunicarse con el mediante chat de texto o de video, transmitiendo la información al intérprete, que es quien, realiza la llamada a una persona oyente, a su trabajo, al médico, a un familiar entre otros. A su vez, toda la



para lograr una comunicación oportuna y eficaz con el personal médico de la entidad.

La Corte consideró que la solicitud para acceder a una de las redes de internet de la entidad accionada tenía por objeto la protección del derecho a la libertad de expresión del accionante, en tanto que, solo así, podría: (i) expresarse plenamente con el personal médico de la entidad, (ii) informarse acerca de los procedimientos médicos que necesita, (iii) prestar su consentimiento informado. Por lo anterior, la Corte estimó que la discapacidad auditiva del accionante no podía constituir una barrera que restrinja irrazonablemente su derecho a expresarse en el marco del acceso a los servicios de salud y que este derecho debe ser garantizado en condiciones de igualdad a través de un intérprete o con ayuda de las TIC.

información que el oyente exprese, el intérprete la transmitirá en lengua de señas o por chat de texto, permitiendo entender de manera clara la información, brindando una comunicación más efectiva. Citado en la sentencia T-406 de 2019. M.P Carlos Bernal Pulido.



DERECHOS en el escenario DIGITAL y de las TIC



3. DERECHO A LA LIBERTAD DE EXPRESIÓN EN EL CONTEXTO DIGITAL

“El derecho a la libre expresión se enmarca hoy en un contexto tecnológico en el que cualquier persona, desde cualquier lugar del mundo e incluso mediante el uso de un dispositivo electrónico personal, como un teléfono celular, puede difundir contenidos informativos o de opinión, con la potencialidad de alcanzar de manera inmediata a un amplísimo público.”

Sentencia T-145 de 2016



El derecho a la libertad de expresión, entendido como aquel que goza toda persona para poder informar y recibir información veraz e imparcial, como también, para buscar, recibir y difundir ideas de manera libre y sin censura previa por cualquier medio, se encuentra consagrado en el artículo 20 de la Constitución Política, así como en el artículo 13 de la Convención Americana sobre Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, normas que se integran al ordenamiento jurídico interno colombiano mediante el bloque de constitucionalidad consagrado en el artículo 93 de la Carta Política.

La Relatoría para la Libertad de Expresión de la CIDH ha reconocido que el derecho a la libertad de expresión encuentra en la Internet un instrumento único para desplegar, incrementalmente, su enorme potencial en amplios sectores de la población. En el mismo sentido, la Corte en las sentencias [T-634 de 2013](#), [T-145 de 2016](#), [T-243 de 2018](#) y [T-275 de 2021](#) han señalado que la información publicada a través de redes sociales tiene características diferenciadas a las que se divulga en otros medios: (i) cuenta con una amplia accesibilidad; (ii) los emisores de información por estos medios determinan el contenido de los mensajes que publican de forma autónoma; (iii) la información se difunde de manera inmediata a un número de destinatarios exponencialmente alto; y (iv) una vez los mensajes son publicados e incorporados a una red social, en muchas ocasiones la información es “indisponible” para el emisor y puede ser difundida de forma espontánea por otros usuarios.

A continuación, se destacan algunos aspectos procesales y sustanciales relacionados con la protección del derecho a la libertad de expresión en entornos digitales como garantía medular de la democracia, así como también los límites que la jurisprudencia ha identificado con el propósito de amparar otros derechos fundamentales que, dependiendo del caso analizado, se encuentran relacionados con el ejercicio del derecho a la libertad de expresión.



3.1. Procedencia de la tutela en casos donde se advierta un abuso del derecho a la libertad de expresión en redes sociales

Mediante la sentencia [SU-420 de 2019](#), la Corte en un pronunciamiento unificado conoció varias acciones de tutela en donde los actores señalaron que por medio de blogs, Facebook y YouTube se les acusó de ser “estafadores”, “ladrones” “rateros” y “mafiosos”, además, indicaron que estas manifestaciones les generaron graves perjuicios reputacionales y laborales.

Este Tribunal estableció criterios claros para determinar la procedencia de este mecanismo en conflictos entre particulares por publicaciones en internet. Al respecto, determinó que antes de acudir a la tutela por calificativos deshonrosos en redes sociales, el afectado debe agotar tres requisitos previos, adicionales a los establecidos en el Decreto 2591 de 1991:

1. **Solicitud directa al emisor:** exigir al autor de la publicación que la modifique, corrija o retire.
2. **Reclamación a la plataforma:** acudir a los mecanismos de reporte o denuncia que ofrezca la red social o el sitio web, si sus políticas comunitarias lo contemplan.
3. **Verificación de la relevancia constitucional:** el juez debe evaluar si el caso tiene el mérito suficiente para ser protegido por vía de tutela.

Para determinar esta “relevancia constitucional”, el fallo exigió un análisis del contexto de la publicación, valorando tres elementos: quién comunica, sobre quién se comunica y cómo se comunica (analizando el contenido, el medio utilizado y el impacto real del mensaje). Así mismo, esta Corporación resaltó que, si bien las expresiones utilizadas en las publicaciones están amparadas por la libertad de expresión, dicho derecho no es absoluto y pierde su protección constitucional e internacional cuando las publicaciones carecen de un fin legítimo, no aportan a debates de interés público o revelan una intención puramente injuriosa.



Sentencia *SU-420 de 2019*

Lo publicado en redes sociales está amparado por la libertad de expresión, pero también está sujeto a los límites por lo que algunas publicaciones no se encuentran bajo la protección señalada en el artículo 20 de la Carta, ni por los instrumentos internacionales que la consagran. Así, se activa un límite a la libertad de expresión cuando lo divulgado no se identifica con un fin constitucional legítimo, ni siquiera contribuye a un debate en específico, sino simplemente conlleva una intención dañina o insultante respecto del hecho que se quiere comunicar.

Cabe destacar que, según lo referido en la sentencia [T-256 de 2025](#), el requisito de acudir a los mecanismos previstos por el intermediario de la red social para solicitar la eliminación de la publicación no es directamente aplicable cuando el cuestionamiento se dirige contra el ejercicio de la facultad de moderación de contenidos por parte del operador de la plataforma, pues en este último caso la vulneración de los derechos fundamentales se le atribuye al intermediario mismo. Los mecanismos de reclamación previstos por los operadores de redes sociales no son judiciales ni su objetivo es resolver conflictos con la plataforma, de modo que, en principio, agotarlos no es indispensable para acudir a la acción de tutela.

A propósito de la procedencia de la acción de tutela, cuando se pretenda la rectificación de publicaciones realizadas por un particular en redes sociales, en la sentencia [T-190 de 2024](#) se estudió un caso relacionado por una tutela presentada por un ciudadano contra un programa de comedia y sus presentadores. El accionante señaló que los accionados difundían mediante sus plataformas digitales burlas relacionadas con noticias sobre violencia sexual



cometidas contra niños, niñas y adolescentes, y de esta manera, se fomentaba la comisión de este tipo de delitos.

La Corte determinó que el accionante no les solicitó a los accionados ni a las redes sociales la enmienda y/o retiro de las publicaciones que censura. Estos elementos, sumados a la falta de legitimación en la causa por activa, llevaron a declarar la improcedencia de la acción. Sin embargo, esta Corporación resaltó que las personas que ejercen labores en las redes sociales están llamados a adoptar y fortalecer mecanismos de autocontrol y buenas prácticas, en lo que respecta a la prevalencia de los derechos de los niños, niñas y adolescentes.

Un caso similar se estudió en la sentencia [T-320 de 2021](#). En esta oportunidad, la Corte examinó la procedencia de una acción de tutela interpuesta por un ciudadano contra una figura pública de redes sociales por un presunto abuso de su derecho a la libertad de expresión al realizar comentarios discriminatorios contra la comunidad LGBTIQ+. Esta Corporación determinó que, para que la acción de tutela sea procedente contra un particular por publicaciones en redes sociales, es indispensable que el afectado agote primero los mecanismos de autocomposición. Esto significa que, antes de acudir a la justicia, la persona que se siente afectada debe solicitar directamente a quien hizo la publicación que la retire o la enmiende. Conforme a lo expuesto, se declaró la improcedencia de la tutela por no cumplir con el requisito de subsidiariedad, dado que el actor no solicitó el retiro y enmienda ante la accionada. De igual forma, la “situación de indefensión” es un elemento analizado a la hora de decidir la procedencia de una acción de tutela contra particulares como ocurre con las redes sociales.

Al respecto, en la sentencia [T-050 de 2016](#) la Corte resolvió una colisión entre la libertad de expresión y los derechos a la honra y al buen nombre, originada por la publicación en Facebook de la foto de una persona señalada como deudora. En esta providencia se indicó que el estado de indefensión se define como una situación de naturaleza fáctica en la que la persona afectada carece de una defensa efectiva frente a la violación o amenaza de sus derechos, encontrándose



en una posición de impotencia o sometimiento. Esto se configura al divulgar información a través de medios de comunicación de alto impacto como las redes sociales, ya que esto crea una situación de inferioridad que trasciende la esfera privada.



Sentencia **T-050 de 2016**

En el caso de publicaciones en plataformas como Facebook, la indefensión surge porque la parte demandada tiene un amplio poder de disposición sobre el contenido y el control de los medios en que aparece, detentando el poder de acceso y manejo del sitio, mientras que el afectado carece de control sobre dicha publicación. En consecuencia, cuando se evidencia este estado de debilidad manifiesta, la acción de tutela se vuelve procedente, aunque el accionado sea un particular.

3.2. Límites a la libertad de expresión y discursos no protegidos

Este derecho, aunque es amplio no es absoluto. El artículo 13 de la Convención Americana sobre Derechos Humanos y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, establecen límites a este derecho, prohibiendo lo siguiente: (i) la propaganda a favor de la guerra; (ii) la incitación al terrorismo; (iii) la apología del odio nacional, racial, religioso o de otro tipo de odio que constituya incitación a la discriminación, la hostilidad, la violencia contra cualquier persona o grupo de personas por cualquier motivo (modo de expresión que cubija las categorías conocidas comúnmente como discurso del odio, discurso discriminatorio, apología del delito y apología de la violencia); (iv) la pornografía infantil; y (v) la incitación directa y pública a cometer genocidio. Estas prohibiciones se han reiterado, entre otras, en las sentencias [T-391 de 2007](#), [T-219 de 2009](#), [C-592 de 2012](#), [T-110 de 2015](#), [T-155 de 2019](#) y [SU-420 de 2019](#).



En la sentencia [T-087 de 2023](#) se estudió una tutela presentada por un grupo de nueve periodistas contra el CNE. Estas señalaron que eran víctimas de un patrón de violencia digital por razones de género en redes sociales, a menudo instigado o tolerado por actores y partidos políticos para desacreditar su trabajo periodístico. La Corte señaló que, si bien la libertad de expresión tiene plena vigencia en el entorno digital, esta no ampara discursos que inciten a la violencia o discriminación por razones de género. Preciso que existe un marcado patrón de violencia en línea contra las mujeres periodistas y un déficit normativo para prevenir, investigar y sancionar esta forma de agresión en el ámbito político. Estos elementos permiten evaluar la necesidad de crear mecanismos específicos, pues esperar un monitoreo constante de las redes sociales por parte de las autoridades podría constituir una forma de censura.

En lo que respecta a los discursos de odio en plataformas digitales, en la sentencia [T-061 de 2024](#), la Corte sentó un precedente sobre la responsabilidad de los creadores de contenido y los intermediarios de internet. Esta Corporación revisó una tutela interpuesta contra un influenciador que utilizó expresiones violentas y discriminatorias contra la población LGBTIQ+, a través de un video de YouTube. La Sala determinó que dichas expresiones constituirían un discurso de odio, el cual se encuentra explícitamente excluido del amparo constitucional a la libertad de expresión. Si bien se declaró la carencia actual de objeto por daño consumado, la Corte emitió un pronunciamiento de fondo con el fin de fijar algunas reglas y prevenir futuras violaciones de derechos.

Como resultado, se ordenaron las siguientes medidas:

1. **Para el influenciador:** se le impusieron medidas de reparación, como la obligación de publicar la sentencia en sus redes sociales y participar en un curso de formación sobre derechos humanos.
2. **Para la plataforma:** se emitió una prevención a YouTube por no haber gestionado de manera oportuna y eficaz la denuncia del accionante. La Corte reiteró el deber de los intermediarios de contar con mecanismos accesibles y eficientes para actuar contra la difusión de discursos prohibidos.



3.3. Alcance de la responsabilidad y de las facultades sancionatorias de los intermediarios y administradores de plataformas digitales

En lo referente a la responsabilidad, en la sentencia [SU-420 de 2019](#), la Corte señaló que, por regla general, las plataformas no tienen la obligación de responder por las publicaciones de los usuarios en redes sociales, dado que la responsabilidad recae en quien utiliza directamente expresiones ofensivas o calumniadoras. Sin embargo, determinó que, si una autoridad judicial considera que un contenido vulnera los derechos de una persona, puede ordenar la remoción de dicho contenido de manera directa a los intermediarios. En efecto, la plataforma que aloja las publicaciones puede participar en el trámite judicial como tercero, ya que es la única entidad con la capacidad de ejecutar una eventual orden emitida mediante la sentencia de amparo. Bajo este panorama, la Corte indicó lo siguiente:



Sentencia **SU-420 de 2019**

Si bien las páginas que proveen herramientas para facilitar las publicaciones electrónicas no son los responsables de la infracción de los derechos a la honra o al buen nombre de las personas, al tener la única posibilidad de retirar el contenido vejatorio difundido en sus portales y, por tanto, ser los únicos actores con capacidad de detener el hecho vulnerable mediante la eliminación de la publicación que perturbe los derechos fundamentales de una persona, en su calidad de administradores de la plataforma, son susceptibles de ser vinculados al proceso y destinatarios de una orden de amparo que pretenda la cesación del hecho constitutivo de transgresión invocada.



La Corte en la sentencia [T-229 de 2020](#) se pronunció frente las facultades sancionatorias de los intermediarios (proveedores de servicios de Internet, proveedores de alojamiento de sitios Web, plataformas de redes sociales y motores de búsqueda) quienes son los que permiten la circulación de ideas y contenidos. Al respecto se señaló que:



Sentencia **T-229 de 2020**

Para garantizar la libertad de expresión en línea e impedir la censura previa es necesario dotar a los intermediarios de Internet de inmunidad por los contenidos que terceros difunden a través de sus plataformas, pues, (...), dichos actores privados, además de que no redactan la información, no tienen los conocimientos jurídicos, el contexto o la capacidad técnica para evaluar adecuadamente qué debe ser censurado y qué puede circular en términos de veracidad y buen nombre. Por consiguiente, los intermediarios de Internet solo deben proceder a retirar cierto contenido cuando un juez imparcial y autónomo, luego de ponderar los derechos en discusión, decida que la información debe ser excluida de la esfera pública.

En la misma línea, en la sentencia [T-453 de 2024](#), esta Corporación resaltó que el debido proceso se rige como un límite para las facultades sancionatorias por parte de los intermediarios en redes sociales. En esta sentencia, la Corte examinó la potestad de las plataformas digitales para sancionar a sus usuarios, estableciendo que esta facultad no es absoluta y debe respetar garantías fundamentales. El caso se centró en la tutela de un abogado cuya cuenta de TikTok fue bloqueada y suspendida bajo el argumento erróneo de que era menor de 13 años. A pesar de que el usuario presentó su documento de identidad



DERECHOS en el escenario DIGITAL y de las TIC



para desvirtuar la acusación, la plataforma persistió en su decisión, afectando su libertad de expresión y su actividad económica.

En esa misma providencia, este Tribunal señaló que al momento de aceptar los términos y condiciones en una plataforma se origina una relación jurídica entre la red y el usuario. Así mismo, indicó que la moderación de contenido está regulada bajo ciertas obligaciones de debida diligencia y las plataformas son las encargadas de regular el contenido generado por los usuarios mediante los términos contractuales del servicio y las políticas de contenido.



Sentencia **T-453 de 2024**

Para que cualquier persona pueda acceder a los servicios que ofrece una red social necesariamente debe aceptar los términos y condiciones respectivos, o, en otras palabras, debe adherirse al clausulado normativo que la plataforma, de manera previa, diseñó para regular la relación jurídica que se crea entre la red social y el usuario. Adicionalmente, debe advertirse que los términos y condiciones al ser un contrato de adhesión pueden contener cláusulas que generan un desequilibrio entre los sujetos contractuales involucrados, debido a que no fueron producto de una negociación entre las partes contratantes y, por consiguiente, resulta razonable que tiendan a favorecer los intereses del sujeto que los elaboró

Por su parte, en la sentencia [T-256 de 2025](#), la Corte también abordó un caso de tensión entre la libertad de expresión y el derecho a la honra y al buen nombre por ideas e informaciones expresadas en redes sociales. A diferencia



de los dos casos referidos con anterioridad, en esta oportunidad se analizaron las tensiones que se presentan en los procesos de moderación de contenidos, en relación con los diferentes actores involucrados. De esa forma, se estudió una tutela formulada por una influencer y actriz de contenido para adultos cuyo perfil en Instagram (plataforma administrada por Meta Platforms, Inc.), fue cerrado al considerar que el contenido publicado violaba las políticas comunitarias sobre desnudez y promoción de servicios sexuales. Por su parte, la accionante resaltó que esta decisión se basaba en un estigma debido a su trayectoria en la industria del cine para adultos.

Esta Corporación señaló que la moderación de contenido en redes sociales es una práctica o proceso en donde se revisa el contenido publicado que generan los usuarios de las plataformas digitales con el fin de determinar si se cumple con las “normas comunitarias”. Esta revisión puede realizarse antes o después de la publicación del contenido.

Moderación ex ante (antes)	Moderación ex post (después)
Revisión de los contenidos antes de que el material sea publicado en las plataformas, para evitar la circulación de elementos violatorios con prohibiciones absolutas.	Revisión posterior a la publicación. Por lo general es reactivo, es decir en reacción a una denuncia realizada por otros usuarios.

Gráfica 2. Elaboración propia con base en la sentencia T-256 de 2025.

Al respecto, la Corte realizó un ejercicio de síntesis a los niveles de moderación y señaló que:



Niveles de moderación de contenido		
Nivel 1	Tipo de discurso	Discurso especialmente protegido: no puede ser removido. Discurso cubierto por la protección general y amplia: puede ser removido en cumplimiento de las garantías de los derechos humanos, como el debido proceso y la igualdad, de forma transparente y consistente Discurso prohibido: puede ser removido automáticamente.
Nivel 2	Formas y tono de lo que se comunica	La remoción del contenido no puede obedecer exclusivamente al tono de la publicación o que no corresponda con posiciones mayoritarias.
Nivel 3	Calidad del sujeto que comunica	La remoción de contenidos no puede obedecer a razones discriminatorias, especialmente cuando se trata de sujetos de especial protección constitucional.
Estudio concreto sobre restricción	Test tripartito de libertad de expresión	Las restricciones sobre los discursos que gozan de protección general de la libertad de expresión deben cumplir con los requisitos de legalidad, fin legítimo y necesidad al amparo del principio de estricta proporcionalidad.

Gráfica 3. Elaborada por la Sala Primera de Revisión en la sentencia T-256 de 2025.



Sentencia T-256 de 2025

La Corte reconoce que la moderación de contenidos no sólo es una práctica habitual de las compañías que administran redes sociales digitales como Instagram o Facebook. Es, sobre todo, una necesidad para asegurar una Internet confiable, en el que puedan circular libremente las ideas, la información, el conocimiento y las opiniones, donde se limiten los contenidos que constituyan discursos no protegidos, como la pornografía infantil, la incitación a la violencia y al genocidio o el discurso de odio. En todo caso, esos procedimientos deben, igual que las reglas comunitarias, ajustarse a unos estándares mínimos compatibles con el marco nacional e internacional sobre el derecho a la libertad de expresión.

Frente a este tema, este Tribunal destacó la relación que existe entre la moderación de contenido y el debido proceso. Subrayó que este proceso tiene un carácter sancionatorio, ya que busca identificar y restringir contenidos prohibidos o restringidos por las normas comunitarias de la plataforma. Por ello, resulta esencial que se cumpla con las garantías mínimas del debido proceso específicas para este procedimiento, entre las cuales se encuentran las siguientes:

Que haya consistencia y sensibilidad contextual en la aplicación de las reglas comunitarias, tanto de los equipos humanos como de IA.

Que no haya una aplicación discriminatoria o contraria al derecho a la igualdad de las reglas comunitarias.



Que las normas de la casa se apliquen maximizando el derecho a la libertad de expresión cuando se trate de contenido potencialmente objetable pero no prohibido.

Que haya transparencia sobre las reglas comunitarias infringidas, los procesos de reclamación e impugnación de las decisiones, así como una comunicación formal, sencilla y accesible que redunde en una respuesta de fondo sobre las reclamaciones elevadas a los operadores de las redes sociales.

Las sanciones deben ser advertidas de antemano a los usuarios, con detalle de las consecuencias que su aplicación puede acarrear.

Gráfica 4. Elaboración propia con base en la sentencia T-256 de 2025.

Conforme a lo expuesto, para el caso estudiado la Corte declaró la carencia actual del objeto por daño consumado debido a que no es posible reestablecer la cuenta principal de la actora que contaba con más de 5 millones de seguidores por la posibilidad de que esta haya sido eliminada de manera definitiva. No obstante, le ordenó a Meta (empresa operadora de Instagram) abstenerse de imponer restricciones arbitrarias en la nueva cuenta que posee la actora y en adelante deberá explicar sus reglas de forma transparente, clara y precisa, justificando cualquier restricción a la libertad de expresión.

Así mismo, le ordenó a la accionada lo siguiente:

1. Establecer un canal de comunicación electrónica accesible y visible que permita la notificación de procesos judiciales en su contra que se originen en Colombia.
2. Revisar y ajustar las Condiciones de uso de Instagram y su política de privacidad, de modo que los usuarios ubicados en Colombia y cuyas cuentas son eliminadas por infracciones a las condiciones de uso o las normas Comunitarias, conozcan con claridad las razones de la medida.



3. Unificar en un mismo sitio las condiciones de uso y normas comunitarias, expresadas con claridad y en idioma español las políticas sobre desnudos y actividad sexual de adultos, y sobre servicios sexuales entre adultos.



3.4. Libertad de opinión y de información en el entorno digital

En la sentencia [SU-355 de 2019](#), se examinó una acción de tutela presentada por una creadora de contenido en YouTube contra un canal de opinión de la misma plataforma. La controversia se desató por un video de respuesta que criticaba las afirmaciones de la accionante, quien, basándose en sus creencias cristianas, había expresado que las relaciones homosexuales “no está[n] bien”, aunque las “tolera”.

Al resolver el caso, la Sala Plena negó el amparo de los derechos de la accionante, al determinar que el video del canal de opinión era una expresión crítica sobre un asunto de manifiesto interés público y, por lo tanto, se encontraba amparado por la libertad de expresión.

El fallo estableció una distinción fundamental entre dos facetas de este derecho:



Libertad de Información	Libertad de Opinión
Exige que los hechos transmitidos sean veraces e imparciales.	Protege la manifestación de juicios de valor, pensamientos y posturas subjetivas, las cuales no están sujetas a un juicio de veracidad.

Gráfica 5. Elaboración propia con base en la sentencia SU-355 de 2019.

La Corte concluyó que el video correspondía a la categoría de “Libertad de Opinión”. De manera adicional, la sentencia destacó que el discurso sobre la orientación sexual goza de una protección constitucional reforzada y que las figuras públicas —categoría en la que se incluyó a la youtuber por su exposición e influencia— deben tener un umbral de tolerancia más alto frente a la crítica.

3.5. Difusión de acusaciones y expresiones difamatorias en redes sociales

En la sentencia T-050 de 2016, mencionada en el título sobre procedencia de la acción de tutela, la Corte señaló que, cuando se emplean expresiones “injuriosas”, “vejatorias”, “humillantes” o “desproporcionadas” que evidencian intención dañina y carecen de un fin legítimo, estas no gozan de la protección constitucional prevista. Tal es el caso de los mensajes difamatorios, parciales o erróneos.

Como remedio, la Corte ordenó a la accionada publicar en su perfil de Facebook una retractación dirigida a la actora. Dicha publicación debía tener el mismo alcance que el mensaje original.



Sentencia **T-050 de 2016**

Si bien redes sociales como Facebook implican un mayor riesgo de vulnerabilidad de derechos fundamentales al buen nombre, a la intimidad y a la imagen, no quiere decir que el uso de dichas plataformas implique una cesión de tales garantías y, en consecuencia, la libre y arbitraria utilización de los datos, ya sea videos, fotos y estados, entre otras, ni tampoco la publicación de cualquier tipo de mensaje, dado que, como se ha venido reiterando, la protección y límites de la libertad de expresión por medios de alto impacto también aplican a medios virtuales.

Por su parte, en la sentencia [T-145 de 2016](#) se ampararon los derechos de una mujer que presentó acción de tutela contra una persona que publicó en Facebook imágenes de ella junto con expresiones que le imputaban conductas delictivas, sin existir condena judicial alguna que respaldara dichas afirmaciones. La Corte mencionó que, en el ejercicio de la libertad de información exige cumplir con ciertos estándares mínimos de veracidad respecto al contenido difundido. En particular, esta Corporación enfatizó la importancia de este requisito de veracidad cuando se difunde información sobre presuntos hechos delictivos.



Sentencia *T-145 de 2016*

La libertad de expresión en cualquiera de sus manifestaciones encuentra entonces un límite claro cuando se trata de las afirmaciones referidas a la comisión de conductas delictivas, pues el requisito de veracidad que ampara el derecho fundamental al buen nombre y a la honra está condicionado por la garantía iusfundamental de la presunción de inocencia, garantía que exige que una afirmación de ese tipo en todo caso se sustente en una sentencia en firme o que al menos se refiera a un procedimiento en curso.

Así mismo, en la sentencia [T-117 de 2018](#), se protegieron los derechos de un hombre al cual en redes sociales se le acusó de ser culpable de un homicidio. La Corte reiteró que, las afirmaciones públicas sobre la responsabilidad penal de una persona deben atender a la garantía constitucional de la presunción de inocencia, por lo que para atribuirle a alguien un delito es un requisito ineludible contar con una sentencia judicial en firme que dé cuenta de ello.

En la sentencia [T-243 de 2018](#), la Corte analizó el caso de una mujer la cual consideró vulnerados sus derechos por una publicación realizada en redes sociales por su ex empleadora en donde la acusó de haber incurrido en conductas delictivas. La Corte reafirmó la prohibición de que los empleadores utilicen “listas negras” para difundir información desproporcionada sobre ex empleados, pues esto menoscaba sus oportunidades laborales futuras. Esta Corporación enfatizó el carácter esencial de la libertad de expresión como una garantía en una sociedad democrática, pero destacó que está sujeta a limitaciones legítimas. Estas restricciones deben cumplir el test tripartito: estar previstas en la ley, perseguir fines legítimos y ser necesarias y proporcionales.



3.6. La denuncia pública de violencia contra las mujeres como discurso especialmente protegido “Escrache”

En la sentencia [C-222 de 2022](#), al analizar la constitucionalidad de los eximentes de responsabilidad para los delitos de injuria y calumnia, la Corte se preguntó si una víctima de violencia sexual que denuncia tales hechos en redes sociales puede invocar esta circunstancia como eximente de responsabilidad cuando el presunto agresor la denuncia por injuria y calumnia. Al respecto, esta Corporación mencionó que las denuncias sobre casos de violencia de género contra la mujer constituyen un ejercicio legítimo del derecho a la libertad de expresión. En este sentido, las autoridades deben proteger este tipo de denuncias, dado que las víctimas utilizan las redes sociales como espacios seguros para expresar sus testimonios.

Al respecto, esta Corporación indicó que prohibir la *exceptio veritatis* en casos de imputaciones sobre la vida sexual o delitos contra la libertad sexual restringe los derechos a la igualdad, defensa y contradicción del sujeto procesado por injuria y calumnia, al permitir que el infractor se ampare en su intimidad para deslegitimar las denuncias como discurso protegido y de interés público, aunque existan pruebas de veracidad. De manera adicional, este Tribunal precisó que en casos en los que terceros o medios divulguen hechos de violencia sexual o de género, se requiere el consentimiento de la víctima para poder publicar.



Sentencia *C-222 de 2022*

La excepción de veracidad podrá ser aplicable como excluyente de responsabilidad cuando las imputaciones de conductas que se refieran a la vida sexual, conyugal, marital o de familia, o al sujeto pasivo de delitos contra la libertad, integridad y formación sexuales tengan interés público y cuenten con el consentimiento de la víctima, (...), particularmente cuando se trata de denuncias relacionadas con violencia sexual o de género contra la mujer.

Por su parte, en la sentencia [T-289 de 2021](#), se analizó una tutela presentada por un hombre contra una mujer que, a través de sus redes sociales, publicó acusaciones en donde afirmó que él la había abusado sexualmente. La Corte señaló que la libertad de expresión en las mujeres que han sido víctimas de violencia de género se convierte en un mecanismo de defensa y denuncia contra actos que atentan contra su dignidad, lo que se enmarca en un discurso de interés público y político.

Bajo este contexto, la Corte señaló que la libertad de expresión de la presunta víctima no puede evaluarse con los mismos estándares que la información ordinaria, pues representan testimonios personales sin mediación de fuentes y estos emergen de la experiencia subjetiva de quien se considera víctima. En este entendido, se negó el amparo solicitado.



Sentencia **T-289 de 2021**

Toda denuncia pública que haga una mujer de haber sido víctima de abuso sexual, además de ser una denuncia (en los términos de la legislación penal), se convierte en una forma de reivindicación política de los derechos de sus congéneres, la cual le permite hacer manifiesta su inconformidad con el contexto social en el que se desenvuelve. Por ello, este tipo de expresiones deben ser concebidas como propias de un discurso de contenido político que goza de una especial protección, en cuanto comporta una problemática cuya superación es de interés público.

En la sentencia [**T-356 de 2021**](#) se analizó la acción de tutela de un activista político contra varios colectivos feministas que difundieron en redes sociales dos denuncias en su contra por presunto acceso carnal violento. La Corte determinó que la acción de tutela era improcedente por no cumplir con el requisito de subsidiariedad. Sin embargo, precisó que la libertad de expresión de grupos históricamente discriminados, como las mujeres que denuncian violencia de género, tiene una protección especial. Además, señaló que el accionante, al ser una figura con proyección pública por su activismo político, debe soportar una mayor carga de escrutinio social, lo que limita sus derechos a la honra y al buen nombre.

En el mismo sentido, en la sentencia [**T-061 de 2022**](#), la Corte negó el amparo del derecho al buen nombre de un docente universitario acusado por informes digitales de incurrir en casos de acoso sexual en contra de estudiantes. Esta Corporación señaló que la difusión de dichos documentos constituyó en un ejercicio de la libertad de expresión, dado que su contenido se basó en denuncias de



violaciones de derechos humanos ocurridos en el contexto universitario. Este Tribunal indicó que este tipo de denuncias representan una herramienta de presión por parte de los movimientos sociales.



Sentencia **T-061 de 2022**

Los denominados escraches, especialmente aquellos que se refieren a la defensa de los derechos humanos de las mujeres, prima facie, gozan de protección constitucional debido a que: (i) se explican en virtud a que previamente, personas han presentado denuncias oficiales por hechos que, se relacionan con violaciones a los derechos humanos, y estas son desatendidas o son tramitadas sin la debida diligencia por parte de las autoridades estatales; (ii) ello motiva que, en un contexto de inacción, y en ejercicio de formas de protesta social que gozan de protección constitucional se hagan puestas en escena que implican una interpelación a las autoridades públicas y cuyo objetivo es el reclamo por la omisión de investigación o sanción de responsables de vulneraciones a los derechos humanos.

A su turno, en la sentencia [T-452 de 2022](#) se estudió una tutela interpuesta por un director de cine contra un medio periodístico feminista, que publicó en plataformas digitales una serie de denuncias anónimas por acoso y abuso sexual en su contra. La Corte determinó que las periodistas no desconocieron los derechos fundamentales del accionante porque el reportaje se ajustó a los estándares constitucionales del periodismo. En ese sentido, reiteró que la división entre el relato y la opinión de las periodistas estaba plenamente diferenciada, y concluyó que el reportaje reprodujo denuncias reservadas y



anónimas sobre violencia sexual que demostró un trabajo investigativo serio. En este caso, la Corte negó el amparo de los derechos solicitados.

De manera adicional, relató que:



Sentencia ***T-452 de 2022***

El escrache es una de las estrategias feministas para dar a conocer episodios de acoso y abuso sexual en contra de mujeres. Esta forma de denuncia permite amplificar las voces de las mujeres víctimas las cuales pueden optar por mantener anónimos sus nombres para evitar exponerse cara a cara frente a sus agresores, y encuentra en el periodismo feminista aliadas con capital social y político que contribuyen a que sus relatos lleguen a un público amplio, lo cual permite generar debates al tiempo que se genera un efecto preventivo para toda la sociedad.

Finalmente, la sentencia [T-241 de 2023](#) revisó una tutela interpuesta por un ciudadano contra un perfil anónimo en Facebook que lo acusaba de ser un “violador” y de cometer maltrato físico y psicológico. Durante el proceso, se identificó a la administradora del perfil, quien afirmó ser víctima directa de los hechos denunciados. La Corte determinó que la denuncia anónima de una víctima de violencia sexual es un ejercicio legítimo de la libertad de expresión y un discurso especialmente protegido. La sentencia estableció que cuando la denuncia es realizada directamente por la víctima, no son exigibles los criterios de veracidad e imparcialidad, ya que comunica una vivencia propia. Por estas razones, se negó el amparo solicitado por el accionante.



Casos similares se han estudiado en las sentencias [T-361 de 2019](#) y [T-275 de 2021](#).

3.7. Deberes de las y los funcionarios públicos que interactúan en redes sociales

En la sentencia [T-695 de 2017](#), se ampararon los derechos de una mujer a quien un concejal, mediante sus redes sociales y en sesiones del concejo, acusó de cometer delitos a través de comentarios difamatorios. La Corte estableció que la protección constitucional de los derechos a la honra, al buen nombre y a la intimidad se activa cuando se divulgan públicamente hechos falsos, erróneos, tergiversados sobre una persona, que afectan su imagen ante la sociedad. De manera adicional, resaltó que la *exceptio veritatis* exime de responsabilidad a quien realiza comentarios injuriosos, siempre que demuestre la verdad de sus afirmaciones.

Por su parte, en la sentencia [T-124 de 2021](#) se estudió una tutela presentada por un ciudadano contra la vicepresidenta del país. Este señaló que la accionada por medio de sus redes sociales publicó un mensaje acompañado por una imagen de la Virgen de Fátima y el logo del Gobierno nacional.

La Corte señaló que, si bien la libertad de expresión es universal, su ejercicio adquiere matices distintos cuando proviene de funcionarios públicos, pues sus comunicaciones conllevan simultáneamente un derecho fundamental y un deber de información ciudadana. Preciso que en estos casos resulta crucial determinar si las publicaciones en cuentas personales tienen carácter oficial o privado, para lo cual deben considerarse factores como el nivel de privacidad de la cuenta, su descripción y el uso habitual que se le da. Estos elementos, permiten evaluar el impacto y naturaleza específica de cada publicación. Se declaró la carencia actual del objeto por hecho superado y se ordenó al consejero Presidencial para las Comunicaciones que capacite a los funcionarios del Gobierno nacional sobre el adecuado manejo y uso de redes sociales.



Sentencia *T-124 de 2021*

Los funcionarios públicos tienen el deber de garantizar los derechos de todas las personas y asegurar la vigencia del ordenamiento jurídico, es necesario que el ejercicio de su derecho a la libertad de expresión se encuentre sometido a cargas especiales y a mayores restricciones que el resto las demás personas. Por tanto, las opiniones o informaciones que trasmitan a los ciudadanos, en especial si se trata de altos funcionarios del Estado, deben estar provistas de una especial diligencia y cuidado a fin de evitar que con éstas se lesionen o pongan en riesgo los derechos de las personas. Esta responsabilidad se acentúa cuando el mensaje se transmite a través de medios masivos de comunicación, como las redes sociales, dada su amplia capacidad de difusión y penetración en la sociedad.

La Corte en la sentencia [T-149 de 2025](#) estudió una acción de tutela interpuesta por un periodista contra una congresista por bloquear sus perfiles en redes sociales. La parlamentaria defendió su acción alegando que el demandante ejercía violencia de género contra ella tanto en redes como en páginas web de su propiedad.

Esta Corporación estableció que cuando autoridades utilizan redes sociales para comunicaciones relacionadas con sus funciones, estas actuaciones pueden configurar un cumplimiento del deber de divulgación proactiva de información. Al realizar un estricto juicio de proporcionalidad, el tribunal reconoció que la labor periodística del accionante en plataformas digitales representa un ejercicio legítimo de libertad de expresión y un mecanismo de control político en la



democracia digital. Precisó que esta protección constitucional no se extiende a expresiones que constituyan violencia política. Tras este análisis, la Corte decidió amparar los derechos del periodista.



Sentencia **T-149 de 2025**

Estas tecnologías [redes sociales] han permitido romper barreras sociales, económicas y geográficas de acceso a escenarios de manifestación, control ciudadano y participación. Lo anterior, al ser medios de gran alcance, gratuitos, inmediatos y desterritorializados, que resultan ser más efectivos para el ejercicio de derechos fundamentales, que los medios tradicionales de comunicación.

Casos similares se han estudiado en las sentencias [T-263 de 2010](#), [T-593 de 2017](#), [T-244 de 2018](#), [T-293 de 2018](#), [T-155 de 2019](#), [T-578 de 2019](#), [T-324 de 2020](#), [T-446 de 2020](#), [T-445 de 2021](#) y [T-475 de 2024](#).

3.8. Estándares de protección de derechos fundamentales en el ejercicio del periodismo digital

En la sentencia [T-242 de 2022](#), la Corte estudió el caso de un exfuncionario público y senador que formuló una acción de tutela contra un periodista por el contenido de una serie web y diversas publicaciones en redes sociales. En estas, el comunicador acusaba directamente al político de ser responsable de delitos graves como genocidio y de liderar una organización criminal, presentando estas afirmaciones como hechos verídicos. El accionante alegó que, al no existir



condenas judiciales, dichas publicaciones vulneraban sus derechos a la honra, al buen nombre y a la presunción de inocencia.

Esta Corporación amparó los derechos del exfuncionario al considerar que el periodista sobrepasó los límites de la libertad de información. El fallo determinó que el comunicador presentó inferencias subjetivas y opiniones como si fueran hechos corroborados, sin contar con un soporte fáctico serio y suficiente para acusaciones de tal gravedad. La Corte calificó este actuar como un “ejercicio periodístico irresponsable” que afectó injustificadamente la reputación del actor y el derecho de la sociedad a recibir información veraz. En consecuencia, se le ordenó al periodista rectificar las aseveraciones que no cumplieron con la carga de veracidad.

En esta oportunidad, la Corte reiteró la protección constitucional de las denuncias que se realizan a funcionarios públicos:

La protección constitucional de las denuncias sobre funcionarios públicos

Especial protección constitucional. La Constitución protege el derecho de los particulares, medios de comunicación y periodistas a denunciar –mediante opiniones o informaciones– que los funcionarios públicos están vinculados o han incurrido en conductas arbitrarias, abusivas o delictivas. Estas denuncias son discursos especialmente protegidos. La protección reforzada de estos discursos persigue tres finalidades: (i) reducir los riesgos de represión oficial de la disidencia política, (ii) garantizar que la ciudadanía vea la esfera pública como un escenario seguro para la deliberación política y, por último, (iii) proteger el pluralismo informativo.



Naturaleza del discurso. Los discursos mediante los cuales se emiten críticas o denuncias que vinculan a un funcionario público con conductas arbitrarias, abusivas o delictivas pueden constituir opiniones o informaciones. El juez debe determinar la naturaleza de los discursos a partir de los criterios desarrollados por la jurisprudencia constitucional.

(i) Denuncias que constituyen opinión. La Corte Constitucional ha considerado que constituyen opiniones aquellas críticas o protestas generales en contra de la gestión de los funcionarios públicos que (a) son publicadas en medios que en principio no tienen una finalidad informativa, tales como columnas de opinión, blogs o cuentas personales de redes sociales de personas que no ejercen el periodismo, (b) se dan en un contexto generalizado de controversia pública en relación con la gestión de los funcionarios, (c) están fundadas en argumentos emotivos en los que prevalece un tono subjetivo que expresa el reproche o los sentimientos de indignación del emisor y (d) no contienen imputaciones directas e inequívocas de responsabilidad penal.

(ii) Denuncias que constituyen información. La Corte Constitucional ha considerado que constituyen informaciones o versiones sobre hechos aquellas denuncias sobre los funcionarios públicos que (i) son publicadas en medios que comúnmente tienen una finalidad informativa, tales como noticieros o programas de periodismo investigativo y (ii) en las que el emisor (a) lleva a cabo una descripción detallada de las condiciones de tiempo, modo y lugar en las que habrían tenido lugar las conductas delictivas y (b) presenta argumentos legales de los cuales se derivan imputaciones directas de responsabilidad penal.

Contenido de la garantía constitucional de estos discursos. La especial protección constitucional implica que el derecho a discutir, publicar y divulgar expresiones sobre las conductas presuntamente arbitrarias, ilegales y delictivas de los funcionarios



públicos debe gozar del mayor nivel de apertura posible. De otro, que, correlativamente, las limitaciones y restricciones a estos discursos deben tener un margen reducido. Esta especial protección constitucional cubre tanto a las opiniones como a las informaciones, sin embargo, el alcance de los límites aplicables a cada tipo de discurso es distinto.

Gráfica 6. Elaborada por la Sala Quinta de Revisión en la sentencia T-242 de 2022.

Al aplicar estos estándares, la Corte encontró que los contenidos cuestionados no cumplían con la carga de veracidad, al presentar como hechos probados meras hipótesis basadas en testimonios no verificados. En consecuencia, amparó los derechos del accionante y ordenó las rectificaciones correspondientes.

Por su parte, en la sentencia [T-452 de 2022](#), la Corte destacó que el ejercicio periodístico y los medios de comunicación gozan de una protección especial. Esta se fundamenta en el carácter esencial de la prensa, a la que se ha atribuido las funciones de: (i) actuar como un educador; (ii) servir de mecanismo para la construcción del diálogo social y pacífico; y (iii) erigirse como guardián de la democracia. Sin embargo, esta Corporación alertó sobre un efecto contraproducente: el “efecto paralizador o silenciador”. Dicho efecto surge cuando, en el ejercicio de su labor, los periodistas deciden abstenerse de difundir información por miedo a ser objeto de sanciones civiles o penales desproporcionadas. La consecuencia inmediata es la autocensura, la cual vulnera el libre flujo de la información, pilar fundamental del sistema democrático.



Sentencia T-452 de 2022

La Corte Constitucional ha considerado que el ejercicio irresponsable de las acciones judiciales, es decir, aquel que no persigue la defensa de los derechos, sino la limitación de otros, y la congestión del aparato judicial o dilatar el ejercicio de sus funciones puede ser constitutivo de *abuso del derecho*.

A su turno, en la sentencia [T-394 de 2024](#), la Corte revisó una acción de tutela interpuesta por un periódico contra un alcalde. El medio de comunicación alegaba que una serie de publicaciones del mandatario en la red social X (antes Twitter), en las que cuestionaba su imparcialidad y le atribuía intereses políticos y económicos, configuraban un patrón de acoso que vulneraba la libertad de prensa.

La Corte resolvió declarar la improcedencia de la tutela. El fundamento principal de la decisión fue que el periódico omitió un requisito de procedibilidad indispensable en estos casos: no solicitó la rectificación de la información directamente al exalcalde antes de acudir a la vía judicial.

El razonamiento de la Sala se basó en dos puntos clave:

1. Naturaleza de la controversia: aunque no se pedía eliminar los trinos, el núcleo del conflicto residía en el contenido y la presunta falsedad de los mensajes, lo que hacía aplicable el mecanismo de la rectificación.
2. Igualdad de condiciones en el debate: la Corte destacó que la disputa se daba entre dos actores con un poder e influencia significativos en la opinión pública: un medio de comunicación de gran alcance y un funcionario de



alto perfil. Esta simetría de poder configura un debate en igualdad de condiciones, donde la autocomposición del conflicto, a través de la solicitud de rectificación, se erige como el mecanismo primario y preferente antes de la intervención de un juez constitucional.

En la sentencia [T-206 de 2024](#), se analizó una tutela presentada por un periodista que involucraba la actuación de una inspección de policía. El periodista afirmó que el demandado, como parte de un procedimiento policial, autorizó una sanción en su contra por los comentarios que había hecho en su perfil personal de Facebook criticando a ciertos servidores públicos de la administración municipal.

La Corte señaló que la libertad de expresión es un derecho común a todos; pero la libertad de prensa constituye una importante garantía dentro del Estado Social de Derecho en virtud de su contribución al diálogo social y salvaguarda de la democracia, por esta razón existe una protección de todos los sujetos que intervienen en el ejercicio periodístico. Así mismo, quienes desarrollan esta actividad, tienen una responsabilidad de acreditar una veracidad e imparcialidad. Bajo este escenario, esta Corporación señaló que la autoridad policial se extralimitó en sus funciones y tomó decisiones que vulneraron el derecho a la libertad de expresión.

En la sentencia [T-475 de 2024](#), se abordó un caso relacionado con la práctica del bloqueo de periodistas en redes sociales por parte de entidades estatales. El caso se originó a raíz de la acción de tutela de un periodista que, tras publicar denuncias sobre presunta corrupción en una Gobernación, fue bloqueado de la cuenta oficial de dicha entidad en la red social X (antes Twitter). El accionante argumentó que esta acción constituía un acto de censura que vulneraba sus derechos fundamentales.

La Corte le dio la razón y amparó los derechos del periodista. El fallo establece un precedente clave: cuando una entidad pública utiliza sus redes sociales como un foro público designado para informar e interactuar con la



DERECHOS en el escenario DIGITAL y de las TIC



ciudadanía, no puede restringir arbitrariamente la participación. En este contexto, el bloqueo de un periodista crítico se considera un acto de censura.

La sentencia subraya que el bloqueo generó un doble perjuicio:

1. Vulneró el acceso a la información: impidió al comunicador recibir información oficial de primera mano.
2. Obstaculizó la libertad de prensa: lo excluyó del debate público digital, menoscabando su capacidad de ejercer el control social, una función esencial del periodismo.

En consecuencia, la Corte ordenó a la Gobernación desbloquear de inmediato al periodista y le advirtió que, en el futuro, debe abstenerse de realizar bloqueos, salvo que se demuestre la violación de normas comunitarias que deben ser claras, preexistentes y de aplicación neutral.



DERECHOS en el escenario DIGITAL y de las TIC



4. DERECHO A LA IMAGEN EN ENTORNOS DIGITALES

“El derecho a la imagen como el derecho personalísimo que otorga a las personas la facultad de decidir en qué eventos y en qué condiciones otras personas tienen la posibilidad de captar, publicar, reproducir o comercializar su imagen”.

Sentencia T-275 de 2021



La Constitución Política no consagra el derecho a la imagen propiamente, sin embargo, la Corte desde su jurisprudencia temprana, reconoció dicha prerrogativa. De esa forma, en la sentencia [T-090 de 1996](#), se mencionó que, con las limitaciones legítimas deducibles de las exigencias de la sociabilidad humana, la búsqueda del conocimiento y demás intereses públicos superiores, se estima que toda persona tiene derecho a su propia imagen y que, sin su consentimiento, ésta no puede ser injustamente apropiada, publicada, expuesta, reproducida o comercializada por otro.



Sentencia **T-339 de 2020**

El derecho a la propia imagen hace referencia a la potestad que tiene cada persona para determinar el manejo de su representación externa, así como su utilización. Esta garantía tiene origen jurisprudencial, a partir de una lectura sistémica e integral de la Constitución junto con su artículo 94, y se concibe como un derecho fundamental, de carácter personalísimo y autónomo, relacionado con la personalidad jurídica y el libre desarrollo a la personalidad, así como una garantía concurrente con los derechos a la intimidad, al buen nombre y a la honra

Respecto a su protección jurídica, la jurisprudencia ha referido que la misma tiene lugar a partir de tres facetas:



-
- (i) la autonomía para definir desde lo estético su propia imagen (dimensión de autodefinición del ser en su aspecto físico).
 - (ii) la identificación de su imagen en la sociedad, la cual le permite identificarse plenamente frente a los demás.
 - (iii) la utilización de esa imagen en cuanto a cómo y qué parte puede ser difundida de manera libre o restringida y de forma gratuita u onerosa (dimensión positiva), y en la posibilidad de prohibir su obtención, utilización y reproducción (dimensión negativa)
-

Gráfica 7. Elaboración propia con base en la sentencia T-339 de 2020.

De igual forma, en la sentencia [T-275 de 2021](#), la Corte destacó que se trata de un derecho fundamental innominado y autónomo bajo el entendido de que la imagen personal es una expresión directa de la individualidad e identidad de la persona.

En este pronunciamiento se precisó que existe un grupo de representaciones que dan cuenta con claridad del aspecto físico, en general, y de los rasgos del rostro que permiten identificar a las personas como las fotografías, esculturas, videos y demás documentos que permitan identificar con precisión al individuo. En contraste, existen otras representaciones en las que no resulta claro si está involucrada la imagen, tal y como sucede con las siluetas, las caracterizaciones y algunas expresiones que reproducen el estilo de las personas y que pueden permitir su identificación. En estos últimos casos, la protección constitucional es altamente contextual y dependerá de las circunstancias específicas de cada caso.

En relación con la protección de este derecho en el entorno digital, en la sentencia [T-260 de 2012](#), la Corte se refirió a las potentes herramientas con que cuentan las redes sociales para el intercambio, procesamiento y análisis de la información facilitada por los usuarios, quienes en un primer momento pueden no prever este alcance. En este contexto, se consideró que, de manera



concomitante al aumento de estas posibilidades de interacción, se generan también riesgos para los derechos fundamentales, entre ellos, el de la imagen.

A continuación, se mencionará algunos pronunciamientos en los que la Corte ha estudiado casos en los que se ha visto comprometido este derecho en escenarios o plataformas digitales, puntualmente, respecto a la tercera faceta de protección relacionada con el uso y difusión de dicha imagen.

4.1 Difusión de videos y fotografías en páginas web o redes sociales

En la sentencia [T-379 de 2013](#), la Corte estudió el caso de un artista musical cuya trayectoria era utilizada en redes sociales para promocionar una orquesta sin su autorización. La Corte señaló que, si bien el usar la imagen de una persona sin autorización implica la vulneración de este derecho, existen situaciones excepcionales cuando se trata de: (i) actuaciones que son captadas en el ámbito público; o (ii) de una figura pública haciendo referencia a su historia laboral, trayectoria o información relacionada con el ejercicio de sus funciones, donde el ámbito de privacidad se ha reducido por razón del rol que cumple dentro de la sociedad.





Sentencia *T-379 de 2013*

No podría alegarse la violación del derecho a la imagen de una persona pública, en aquellos casos en que simplemente se menciona su historia laboral o se resaltan sus aportes a la sociedad, pues es claro que nadie puede desligarse de lo vivido. Este análisis es distinto, por obvias razones, cuando de lo que se trata es de proteger su vida privada, ya que, en dichos casos, su intimidad personal o familiar, *prima facie*, no tiene por qué ser afectada, tocada o referida por terceros, ni utilizada para alegar algún vínculo con ella.



En la sentencia [T-339 de 2020](#), la Corte estudió el caso de un ciudadano que reprochó el hecho de que un medio de comunicación publicara en su página web oficial un video del accidente automovilístico del que fue víctima. La Corte mencionó que cuando se trate de información brindada respecto de accidentes de tránsito ocurridos en espacio público, la imagen puede ser utilizada sin requerir autorización de su titular, por más de que en los videos o fotografías se puedan observar rasgos característicos de una persona, pues el centro de lo que se publica corresponde a una noticia, que busca informar a la comunidad sobre un suceso. En consecuencia, se negó el amparo.



DERECHOS en el escenario DIGITAL y de las TIC



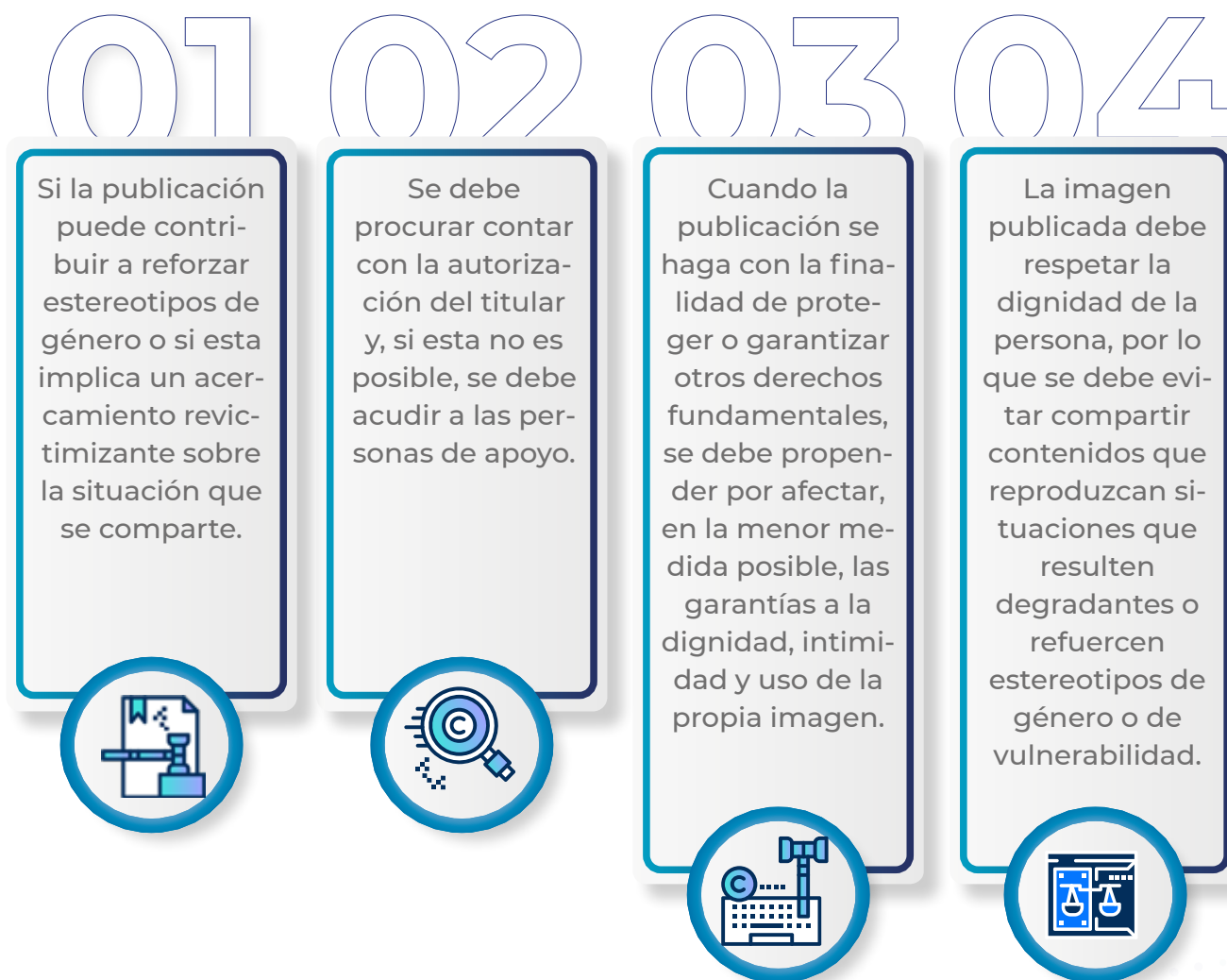
En la sentencia [T-275 de 2021](#), la Corte amparó los derechos de un hombre que, en medio de un “trastorno psicológico agudo” irrumpió desnudo en una vivienda. Los videos e imágenes fueron publicados en redes sociales. La Corte señaló que la libertad de información protege la publicación de denuncias de acoso por redes sociales, pero no otorga un derecho irrestricto a publicar datos privados o semiprivados del presunto acusado, cuando el conocimiento de dicha información por terceros no cumple ningún propósito legítimo y no tiene una conexión directa con un asunto de interés público.



Por su parte, en la sentencia [T-339 de 2022](#) se amparó el derecho a la imagen de una mujer que fue víctima de divulgación de fotografías de contenido sensible, por cuanto aparece en ropa interior o sin ropa en redes sociales. La Corte mencionó que, el exhibir fotografías íntimas de otra persona, de las cuales alguien se ha apropiado indebidamente, es una conducta que tiene la capacidad de afectar de manera evidente y manifiesta varios derechos fundamentales de la persona que aparece en las fotografías. En esta oportunidad se amparó el derecho a la intimidad e imagen y se ordenó la eliminación de las fotografías.



De igual forma, en la sentencia [T-152 de 2025](#), se amparó el derecho a la imagen de una mujer que se encontraba en situación de calle. La madre de la agenciada señaló que un noticiero por medio de su página de Facebook publicó una foto de su hija en ropa interior y desorientada. La Corte señaló que, para garantizar la efectiva materialización de los derechos de las personas en situación de discapacidad y limitar el ejercicio de violencia contra la mujer en redes sociales, el emisor de publicaciones con fotografías de contenido sensible debería tener en cuenta lo siguiente:



Gráfica 8. Elaboración propia con base en la sentencia T-152 de 2025.

4.2 Alcance constitucional de la autorización para el uso de la propia imagen

En la sentencia **T-634 de 2013**, la Corte amparó los derechos de una mujer que autorizó a la empresa para la que trabajaba como masajista, el uso de imágenes suyas con fines publicitarios. La accionante solicitó de manera posterior el retiro de ese contenido de una red social, sin embargo, la empresa se negó a hacerlo.



En este caso, la Corte identificó que las imágenes fueron tomadas y divulgadas con base en una autorización general para ser usadas con fines publicitarios no específicos y, en esa medida, la accionante nunca consintió de manera expresa que fueran divulgadas en un contexto en el cual aparece proyectada en un rol que puede ser asociado a la prestación de servicios sexuales. Bajo estas consideraciones, se indicó que en estas situaciones existe la posibilidad de exigir el retiro de imágenes en redes sociales.



Sentencia **T-634 de 2013**

De no reconocer la existencia de ciertos límites que pueden emerger en cada caso como consecuencia de la vulneración de derechos fundamentales en el marco de ciertas autorizaciones para el uso de la propia imagen (autorizaciones indeterminadas y ambiguas), el uso de la misma estaría no sólo de manera indefinida a merced de terceros al tiempo que la protección del derecho a manejar la propia imagen, sino que además afectaría la posibilidad de las personas para auto determinarse con relación a ella; ésta perdería toda eficacia y podría violar de forma definitiva otros derechos fundamentales.

En esa línea, la Corte expresó que los jueces constitucionales deben estudiar cada caso concreto para determinar si existe una afectación o vulneración de un derecho fundamental incluso cuando media una autorización para el uso de la propia imagen. Frente a este punto, se precisaron las siguientes delimitaciones del alcance de la mencionada autorización:



DERECHOS en el escenario DIGITAL y de las TIC



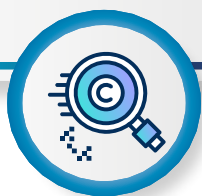
01

La autorización para el uso de la propia imagen no puede implicar la renuncia definitiva del mismo.



02

La autorización comprende el consentimiento informado no solo acerca del uso de la propia imagen sino sobre las finalidades de éste.



03

La autorización de uso de la propia imagen no puede constituir un límite absoluto al carácter necesariamente dinámico y cambiante de la autodeterminación de las personas o a su libre desarrollo de la personalidad.



04

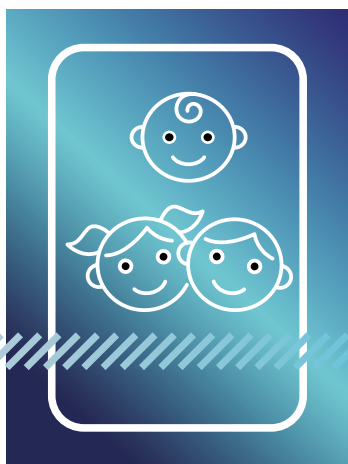
La imagen publicada debe respetar la dignidad de la persona, por lo que se debe evitar compartir contenidos que reproduzcan situaciones que resulten degradantes o refuercen estereotipos de género o de vulnerabilidad.



Gráfica 9. Elaboración propia con base en la sentencia T-634 de 2013.



4.3. Protección del derecho a la imagen de los niños, niñas y adolescentes en entornos digitales



Padres que crean cuentas en redes sociales con la imagen de sus hijos. En la sentencia [T-260 de 2012](#), la Corte amparó los derechos de una niña cuyo padre creó a su nombre un perfil de Facebook del que ella no era consciente y que se utilizaba para ventilar una disputa familiar. En este caso se precisó que, si bien la patria potestad implica la posibilidad de que los padres tomen ciertas decisiones en nombre de sus hijos, tales decisiones no pueden poner en riesgo a los mismos, ni afectar sus derechos fundamentales. Bajo ese análisis, se ordenó cancelar la cuenta a nombre de la niña.



Sentencia *T-260 de 2012*

En el caso específico de los menores de edad, en especial niños y niñas, el acceso a las redes sociales debe darse con el acompañamiento de los padre o personales responsables de su cuidado, a fin de que éstos sean conscientes de que si bien el mundo de la información y la tecnología implica un sinnúmero de beneficios para su desarrollo, al mismo tiempo genera una serie de riesgos que se pueden evitar con un correcto manejo de la información y con una adecuada interacción con los demás miembros de la red.



Divulgación de imágenes de menores de edad sin autorización. En la sentencia [T-904 de 2013](#), la Corte protegió el derecho de un grupo de menores de edad. La vulneración tuvo lugar por cuanto un noticiero, en el marco de un reportaje, divulgó sin autorización un video en el que se captan imágenes de los niños mientras jugaban en la cancha de fútbol al interior de un conjunto residencial. La Corte resaltó que la actividad tuvo lugar en un espacio que hace parte de la esfera privada. Aunque se trataba de un espacio descubierto, esto no lo convertía en un escenario público. Esta Corporación consideró

que los videos publicados en el medio de comunicación al haber sido grabados sin la autorización de los padres y de los niños excedió el ámbito constitucionalmente protegido por la libertad de información al difundir imágenes en las que se aprecian rasgos de la fisonomía de los niños, por esta razón ordenó retirar los videos en donde se aprecie la imagen de los menores.

Por su parte, en la sentencia [T-610 de 2019](#), la Corte amparó el derecho a la imagen de una niña grabada por sus familiares durante su rescate efectuado en el marco de un proceso administrativo de restablecimiento de derechos. Luego, dichos videos fueron entregados a un medio de comunicación que se encargó de divulgarlos por redes sociales. La Corte mencionó que en el evento que terceros realicen grabaciones o tomen fotografías de menores de edad deben hacerlo con el consentimiento del titular y deben cerciorarse de que tal material no sea usado de manera indebida o en transgresión de su interés superior. Se precisó que hay situaciones en que las filmaciones o las fotografías tienen fines relacionados con la protección de los derechos de los menores de edad, en cuyo caso, el material debe ser entregado a la autoridad competente.



4.4. Uso de imágenes para fines distintos a los concertados con la persona titular

En la sentencia [T-090 de 1996](#), la Corte amparó el derecho a la imagen de una mujer que accedió a ser grabada en el momento del parto con el propósito de reproducir el video en un programa de televisión. Sin embargo, el médico siguió utilizando el video para fines académicos y otros programas de televisión. La Corte señaló que, la utilización de material fílmico, por fuera de la finalidad convenida, vulnera la intimidad, pues en esas condiciones no opera el consentimiento de la persona que se ve expuesta a la mirada y al escrutinio público respecto de un hecho íntimo.



Por su parte, en la sentencia [T-407A de 2018](#), la Corte amparó los derechos de una mujer quien accedió a grabar un video pornográfico a modo de casting. Sin embargo, este video fue publicado en varias páginas de internet. La Corte mencionó que, la libertad contractual es amplia y permite autorizar a terceros el uso, difusión y comercialización de su propia imagen, en virtud del derecho que se tiene a disponer de esta. Sin embargo, señaló que en los contratos que suscriben las empresas productoras de material audiovisual pornográfico es necesario precisar algunos parámetros mínimos constitucionales, con el fin de asegurar la manifestación de la voluntad de las personas cuyas imágenes van a ser publicadas:



Gráfica 10. Elaboración propia con base en la sentencia T-407A de 2018.

A su turno, en la sentencia [T-289 de 2023](#), la Corte amparó el derecho a la imagen de una adolescente transgénero y migrante que accedió a grabar una entrevista para ser reproducida en un entorno académico. Sin embargo, la entrevista fue publicada en redes sociales, en donde se daba información del contexto personal de la adolescente como su identidad sexual, su edad, su ubicación geográfica, además de haber hecho mención pública sobre sus condiciones particulares de migrante irregular y trabajadora sexual. La Corte señaló que, las personas que publiquen contenidos en medios de comunicación o redes sociales tienen la obligación de proteger la imagen y la identidad de los niños y niñas, y evitar los posibles riesgos que pueda entrañar su mención en tales publicaciones.



4.5. Imágenes captadas por cámaras de video de seguridad

A continuación, se exponen algunas reseñas de casos analizados por la Corte relacionados con imágenes captadas a través de cámaras en distintos ámbitos.

En el servicio de transporte público. En la sentencia [C-094 de 2020](#), la Corte estudió una demanda en contra de algunos artículos del Código Nacional de Seguridad y Convivencia Ciudadana. En esta oportunidad, la Corte señaló que el implementar cámaras de vigilancia en los vehículos de transporte público genera una restricción al derecho a la intimidad, que encuentra justificación en la prevalencia del interés general y el orden público. Sin embargo, resaltó que el almacenamiento de imágenes debe estar sujeto al régimen de habeas data.



En el ámbito laboral. En la sentencia [T-768 de 2008](#), la Corte estudió el caso de un empleado de un banco que fue despedido con fundamento en las imágenes captadas por una cámara instalada en la oficina donde aquel trabajaba. En esta oportunidad, se concluyó que no se vulneraron los derechos del accionante, pues la instalación de las cámaras buscaba un fin legítimo: controlar las conductas irregulares de quienes obstruían los sistemas de vigilancia del banco.

En las consideraciones se indicó que 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, de ahí que, en cada caso, se deba ponderar las circunstancias específicas y evaluar la razonabilidad de las medidas de vigilancia. Dentro de las situaciones a considerar están las siguientes:



- El objeto social que desarrolla la empresa.
- El lugar donde la medida es implementada, pues es razonable que recaiga en lugares donde se desarrolle la actividad laboral que, por ejemplo, se encuentren abiertos al público, pero no lo sería en aquellos donde el trabajador ejerce una esfera privada como lugares de descanso, tales como baños o vestuarios.
- Que la medida guarde una relación directa con la seguridad necesaria de las instalaciones de trabajo o el control del cumplimiento de los deberes y funciones de los trabajadores.
- Que pueda tomarse otras medidas menos invasivas para lograr los propósitos legítimos
- Que los perjuicios derivados de la medida, en lo posible, sean mínimos.
- Que la medida sea conocida, pues de manera excepcional puede legitimarse medidas subrepticias (ocultas).
- Que la medida no implique someter a la persona a tratos crueles, inhumanos o degradantes, los cuales se encuentran proscritos de manera absoluta.



Establecimientos privados abiertos al público. En la sentencia [T-487 de 2017](#), la Corte analizó un caso donde el accionante solicitó copia de los videos registrados por las cámaras de un casino, instaladas en la salida del parqueadero del establecimiento, pues su hijo fue atropellado en dicho punto y requería aportar la prueba al proceso penal. Esta Corporación señaló que la información obtenida a través de las grabaciones de video de la calle o el espacio público es privada, ya que la entrega de este material fílmico a particulares puede vulnerar el derecho a la intimidad de las terceras personas al quedar su



imagen registrada en la grabación solicitada por el ciudadano. Sin embargo, la Corte decidió que la solicitud de la grabación tiene relación con el derecho al acceso a la administración de justicia, por esta razón ordenó la entrega a la autoridad competente para que sirva como prueba en el proceso.

Por su parte, en la sentencia [T-114 de 2018](#), la Corte conoció el caso de una persona que fue hospitalizada después de sufrir un accidente en unas termas. Al respecto, se cuestionó que el establecimiento público se negara a remitir la copia de los videos requeridos por los médicos para determinar el tiempo de inmersión. La Corte indicó que los registros audiovisuales contenidos en las cámaras de seguridad de un establecimiento público que incluyen imágenes privadas de los niños, las niñas y los adolescentes constituyen información privada. Por esta razón, se negó el amparo invocado.

A su turno, en la sentencia [T-280 de 2022](#), se ampararon los derechos de una mujer grabada dentro de un baño ubicado en las instalaciones de una escuela de equitación mientras ella realizaba actividades fisiológicas. La grabación fue difundida sin su consentimiento en WhatsApp. La Corte señaló que la captación y la divulgación no consentida del video constituyó una violación de los derechos a la intimidad y a la imagen y un acto violencia de género digital.



Sentencia **T-280 de 2022**

Incluso en espacios abiertos al público, los baños son sitios íntimos y privados. Esas áreas privadas son inalienables, inviolables y reservadas. Cuando se ubica una cámara escondida en un baño solo es posible inferir que el propósito de esa acción es vulnerar la intimidad y captar imágenes de los usuarios de esos servicios sin su consentimiento.



VIDEO

Video sobre
grabación no
consentida en baño
público y divulgación
en red social

En el ámbito de salud. En la sentencia [T-144 de 2024](#), se analizó una acción de tutela formulada por la madre de un niño diagnosticado con Trastorno del Espectro Autista TEA. La accionante mencionó que la IPS accionada negó la solicitud de entrega de los videos grabados por las cámaras de videovigilancia instaladas en los salones de terapia a donde asiste su hijo. La Corte señaló que la videovigilancia puede estar justificada en algún propósito asociado con el bienestar y/o tratamiento del paciente, pero, debe procurarse que el desarrollo tecnológico esté al servicio de preservar su derecho a la intimidad, por ejemplo, disponiendo de un sistema que registre movimientos y no imágenes. En esta oportunidad, se concedió el amparo y se ordenó a la accionada para que adopte un protocolo detallado y específico para la recolección, tratamiento, almacenamiento y consulta de datos visuales con fines de seguimiento terapéutico y seguridad.



En el ámbito educativo. En la sentencia [T-170 de 2025](#), la Corte estudió una acción de tutela interpuesta por un sindicato contra el SENA, un centro académico y una empresa de seguridad, por la negativa de estas entidades de retirar unas cámaras de videovigilancia instaladas al interior de los salones de clase. La Corte determinó que la instalación de cámaras de seguridad en las aulas educativas resulta lesiva para los derechos, ya que, si bien la información obtenida mediante las cámaras de videovigilancia no ha sido utilizada en procesos administrativos, internos o externos, o judiciales, la medida representa una amenaza. En esta ocasión, se concedió el amparo y se ordenó el retiro de las cámaras de videovigilancia instaladas en las aulas educativas. Un caso similar se estudió en la sentencia [T-407 de 2012](#).



DERECHOS en el escenario DIGITAL y de las TIC



5. LA ADMINISTRACIÓN DE JUSTICIA EN EL MARCO DEL USO DE NUEVAS TECNOLOGÍAS Y DE LA INTELIGENCIA ARTIFICIAL

“El uso de las tecnologías con fines judiciales no se puede entender como un capricho. Es indudable la capacidad transformadora que su implementación, uso y masificación puede traer a la eficiencia de la administración de justicia y al acceso de los ciudadanos a ella.”

Sentencia C-134 de 2023



El artículo 229 de la Constitución Política consagra el derecho al acceso a la administración de justicia. La Corte ha señalado que este derecho se sustenta en tres pilares: i) la posibilidad de acudir y plantear un problema ante el juez competente, ii) la resolución de dicho problema y iii) el cumplimiento efectivo de la decisión adoptada.¹³

En Colombia, el uso de tecnologías de la información y las comunicaciones en el sector público ha impulsado un proceso de modernización del sistema judicial para implementar una justicia digital. Este proceso busca optimizar la práctica de pruebas, la formación, conservación y reproducción de expedientes, así como la comunicación entre despachos y garantizar un funcionamiento razonable del sistema de información. La administración de justicia, como servicio público esencial, está llamada a aprovechar estas tecnologías para cumplir sus funciones con calidad, eficiencia y seguridad.¹⁴

En la sentencia [C-037 de 1996](#), la Corte declaró exequible, entre otras disposiciones, el artículo 95 del entonces proyecto de ley estatutaria de administración de justicia¹⁵, según el cual, el Consejo Superior de la Judicatura (Cons.S. Jud.) debía incorporar “tecnología de avanzada al servicio de la administración de justicia”. Dicho artículo, se encaminó a garantizar que el uso de medios técnicos, electrónicos, informáticos y telemáticos sirviera para mejorar aspectos relevantes en el ejercicio de administrar justicia. Al respecto, la Corte señaló:

¹³ Sentencias T-295 de 2007 M.P Alvaro Tafur Galvis y T-665 de 2012 M.P Adriana María Guillén Arango.

¹⁴ Sentencias T-203 de 2025 M.P Jorge Enrique Ibáñez Najar, T-398 de 2023 M.P Antonio José Lizarazo Ocampo y SU-355 de 2022 M.P Cristina Pardo Schlesinger.

¹⁵ Proyecto de Ley Estatutaria 58/94 Senado y 264/95 Cámara



Sentencia C-037 de 1996

Esta disposición busca que la administración de justicia cuente con la infraestructura técnica y la logística informática necesaria para el recto cumplimiento de las atribuciones y responsabilidades que la Constitución le asigna.

En el mismo sentido, en la sentencia [C-134 de 2023](#), en un ejercicio similar de control automático de constitucionalidad sobre la disposición que modificó el referido artículo 95, la Corte declaró exequibles varias adiciones relacionadas con el uso de las TIC en la administración de justicia. A su vez, declaró constitucional la incorporación de un Plan de Transformación Digital para la Rama Judicial el cual debe ser expedido cada cuatro años por el Consejo Superior de la Judicatura junto con un plan anual de acción y otro operativo.

En este pronunciamiento, la Corte señaló que el uso de las TIC ofrece una posibilidad real de mejorar la experiencia de acceso judicial lo cual redundará en una mayor protección y exigibilidad de los derechos de los ciudadanos. Así mismo, resaltó que el Plan de Transformación Digital es sin duda un aporte importante en tanto busca proteger el núcleo básico del derecho al acceso a la administración de justicia, con la habilitación de canales en línea. El plan además busca un fin importante como lo es la estandarización de los procesos de digitalización en los despachos judiciales, algo indispensable si se quiere cerrar las brechas de acceso y diseñar servicios de justicia centrados en el usuario final, que no es otro que el mismo ciudadano.

En esta misma providencia se destacó que, para poder garantizar la seguridad y promover una conectividad eficiente, los juzgados, tribunales y entidades judiciales deberán emplear herramientas tecnológicas aprobadas por el Cons.



S. Jud. en cumplimiento del Plan de Transformación Digital. Sin embargo, esta Corporación aclaró que dichas herramientas no deben desconocer la autonomía de los jueces y de las altas cortes para determinar los canales de acción adecuados. Por ello, el Cons. S. Jud. al promover la incorporación de tecnologías de la información, debe respetar un margen de acción para que los órganos judiciales, en especial las altas cortes, puedan adoptar las herramientas tecnológicas acorde a sus necesidades y capacidades específicas.

En cuanto a la presencialidad en las audiencias, la Corte estableció que esta constituye una manifestación de la autonomía del juez. No obstante, precisó que, en materia penal, la audiencia de juicio oral debe ser presencial porque en este proceso se tiene la particularidad de que la libertad de una persona puede verse comprometida. La realización de esta audiencia de forma virtual puede generar riesgos en una adecuada construcción de la verdad.

A lo anterior se le suma, el marco normativo adoptado con el fin de regular el servicio de administración de justicia durante el estado de emergencia por la pandemia de COVID-19, la Corte realizó el control de constitucionalidad del Decreto Legislativo 806 de 2020, por medio del cual se adoptaron medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia. [C-420 de 2020](#), la Corte realizó el control de constitucionalidad del Decreto Legislativo 806 de 2020, por medio del cual se adoptaron medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia.

En este pronunciamiento, la Corte señaló que al hacer uso de herramientas y canales digitales con el fin de adelantar las actuaciones judiciales y suministrar la información y documentación necesaria para el desarrollo del proceso, no se entorpece el acceso al servicio público de administración de justicia. Por el contrario, facilita el ejercicio de ese derecho fundamental y contribuye a que el servicio se preste de manera ágil y eficiente.



Cabe destacar que los avances tecnológicos emergentes han permitido incorporar herramientas cada vez más diversas al servicio de la administración de justicia. Por ejemplo, de manera reciente, se han analizado casos relacionados con el uso de Inteligencia Artificial (IA) en este ámbito, así como su impacto en la garantía de derechos fundamentales, situación que ha significado un verdadero desafío para la Rama Judicial.



Sentencia **T-323 de 2024**

La IA tiene el potencial de mejorar el bienestar de las personas y, en general, de la sociedad. Su contribución en la evolución de la sociedad se ha visto reflejada en la realización y armonización de actividades relacionadas con la economía, la innovación, la productividad global, entre otras. De esta forma, la implementación de esta herramienta tecnológica se ha dado en diversos sectores, los cuales van desde la producción, las finanzas y el transporte, hasta la atención médica, la seguridad y, por su puesto, el derecho y la administración pública.

En ese contexto, la Corte se ha pronunciado en diferentes momentos sobre el alcance del uso de dichas herramientas en el marco de la administración de justicia, a continuación, se presentan algunos casos agrupados según las temáticas abordadas en cada uno.

5.1. Competencia de los jueces constitucionales colombianos para dirimir asuntos que involucran intermediarios con sede extranjera

En la sentencia [T-256 de 2025](#), esta Corporación se pronunció sobre la competencia de los jueces nacionales cuando una controversia involucra a una



red social cuya casa matriz se encuentra en el extranjero. La Corte destacó dos extremos problemáticos; por un lado, la aplicación estricta del principio de territorialidad que dejaría en impunidad conductas que no suceden en algún lugar físico; por otro, una jurisdicción universal en donde se generaría una inseguridad jurídica al no saber que normas se deben acoger.

De esta manera, la Corte concluyó que el Estado no puede renunciar a ejercer su jurisdicción sobre la internet, aplicando criterios sobre la jurisdicción que se limitan solo a un entendimiento estricto de la territorialidad. En materia de tutela, indicó que se puede utilizar un enfoque de territorialidad mixto, en el cual la competencia se determine por el lugar donde se presenta la amenaza de los derechos fundamentales. De manera subsidiaria, se considera competente el juez del lugar donde dichos eventos generan sus efectos.



Sentencia **T-256 de 2025**

El hecho de que una disputa se relacione con Internet no quiere decir que los jueces nacionales carezcan de competencia para conocerla. Por el contrario, aunque Internet pone a prueba los criterios tradicionales para asignar la jurisdicción, es posible establecer reglas que permitan regular lo que sucede en el ciberespacio sin que se convierta en una intervención ilimitada en el mundo virtual. (...). De igual forma, en línea con la jurisprudencia de esta Corte en materia de acción de tutela, el juez constitucional puede ser competente para conocer una disputa cuando la vulneración o amenaza de los derechos fundamentales ocurre en Colombia o, en subsidio, cuando de forma clara produce efectos en el país.



5.2. Publicación de información y administración de los sistemas de consulta de la página web de la Rama Judicial

En la sentencia [SU-355 de 2022](#), la Corte conoció una acción de tutela formulada por una mujer quien consideró que un juzgado vulneró su derecho a la intimidad al publicar en internet el expediente del proceso del que era parte. Al respecto, la Corte señaló que en los procesos judiciales se aplica el principio de publicidad, lo que hace que los sujetos procesales tengan conocimiento de las actuaciones dentro del proceso. Sin embargo, este principio no significa hacer público todas las actuaciones, dado que, la información contenida en algunas ocasiones puede transgredir el derecho a la intimidad.

En esta oportunidad, se amparó los derechos de la actora y se le ordenó al Consejo Superior de la Judicatura que reglamente de manera específica, clara y completa las condiciones en que se deben realizar las publicaciones en el portal web de la Rama Judicial y actualice la normativa existente a las nuevas necesidades de publicación en la página, a raíz de la priorización de las tecnologías de la información y de las comunicaciones en la administración de justicia.



Sentencia ***SU-355 de 2022***

El juzgado, como creador del contenido del micrositio web que tiene a su cargo, es el responsable de la información y de los documentos que incrusta en ese micrositio. Por lo tanto, el principal llamado a valorar el contenido de la información que publicaba en este caso era el despacho judicial.

En la sentencia [T-398 de 2023](#), la Corte estudió una acción de tutela presentada por un hombre que indicó que, en la página de consulta de procesos de la



Rama Judicial, aparece vinculado a dos procesos penales, motivo por el cual solicitó la anonimización de dichos procesos. La Corte señaló que, en los procesos penales, durante las actuaciones iniciales existe una reserva y un manejo más estricto de la información, ya que de esta puede depender la eficacia de la investigación y la protección de bienes jurídicos superiores.

Asimismo, la Corte mencionó que no existe una regla especial de competencia establecida por el Cons.S.Jud que determine quién debe ocultar la información una vez que el dato ha caducado, lo que ocasiona que la información pueda vulnerar los derechos a la intimidad personal y familiar de las personas. En consecuencia, la Corte amparó los derechos del actor y reiteró la orden de la sentencia [SU-355 de 2022](#), que insta a reglamentar de manera completa los lineamientos para el tratamiento de los datos personales publicados en la página web de la Rama Judicial, en particular, aquellos relacionados con anotaciones penales.



Sentencia **T-398 de 2023**

La información producto de las diligencias previas a la formulación de la imputación, incluyendo la de entrega provisional de los bienes de que trata el artículo 100 del Código de procedimiento penal, en tanto hacen parte de la etapa de indagación, no reviste la característica de ser pública y en consecuencia exige la aplicación de las limitaciones derivadas del habeas data y del derecho al buen nombre.

Por último, en la sentencia [T-203 de 2025](#), la Corte analizó una acción de tutela interpuesta por un hombre quien advirtió sobre la indebida permanencia del registro de un proceso penal iniciado en su contra en la base de datos de



la Rama Judicial. La Corte afirmó que la conservación de datos personales en la página de la Rama Judicial, cuando la pena ya se ha extinguido, contraviene los principios de legalidad, finalidad y veracidad. Además, indicó que la persistencia de esa información afecta a las personas, pues las etiqueta como delincuentes sin que lo sean. En consecuencia, instó al Cons.S.Jud para que comunique las condiciones en las que deben anonimizarse o suprimirse los datos personales de quienes son procesados penalmente y cumplen con su pena, con el fin de proteger los derechos a la intimidad y *habeas data*.



Sentencia T-203 de 2025

Mantener el registro de datos personales relacionados con un antecedente penal que ya no existe implica el tratamiento de información desactualizada e inexacta, que eventualmente puede ser consultada por usuarios que no tienen ningún interés legítimo en aquellos datos. Como consecuencia, el titular se puede ver afectado por consultas no autorizadas.

5.3. Valoración probatoria de los mensajes de datos y las capturas de pantalla

La Corte en la sentencia [C-662 de 2000](#)¹⁶ señaló que los mensajes de datos deben recibir el mismo tratamiento jurídico que los documentos en papel, dado que cumplen con los mismos criterios que un documento tradicional.

¹⁶ Acción pública de inconstitucionalidad contra la Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.



Por su parte, en la sentencia [C-604 de 2016](#)¹⁷, la Corte mencionó que los mensajes de datos son admitidos como medios de prueba y deben ser tenidos en cuenta las reglas de la sana crítica para la apreciación de estos.

Por ejemplo, en la sentencia [T-043 de 2020](#), se conoció una acción de tutela presentada por una mujer a quien no se le renovó el contrato laboral, pese a que informó a sus superiores, mediante WhatsApp, sobre su estado de gestación. La Corte señaló que el avance tecnológico ha propiciado la aparición de pruebas electrónicas. Indicó que, debido a su informalidad y la posibilidad de edición o alteración, estas pruebas tienen carácter indiciario, por lo que deben evaluarse junto con otros medios probatorios. En este caso, se protegió el derecho fundamental al trabajo y se ordenó a las accionadas ofrecer disculpas y contratar nuevamente a la accionante.



Sentencia *T-043 de 2020*

Los avances tecnológicos que a nivel global se han dado en distintos campos (...), también han influido en el entendimiento y el ejercicio del derecho. Al efecto, en el ámbito probatorio, los operadores judiciales diariamente deben analizar elementos extraídos de aplicaciones de mensajería instantánea, ya sea que se cuente con metadatos que permitan realizar un mayor rastreo de la información o solo capturas de pantallas respecto de ciertas afirmaciones o negaciones realizadas por una de las partes en el litigio.

¹⁷ Acción pública de inconstitucionalidad contra la Ley 527 de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.



Un caso similar relacionado con la no renovación de un contrato de prestación de servicios se estudió en la sentencia [T-467 de 2022](#). En esta oportunidad, la Corte se pronunció respecto al valor probatorio de las copias impresas de los mensajes de datos, sobre las cuales precisó lo siguiente:



Sentencia **T-467 de 2022**

Las copias impresas de los mensajes de datos son medios de convicción que deberán ser valorados según las reglas generales de los documentos y las reglas de la sana crítica, y su fuerza probatoria dependerá del grado de confiabilidad que le pueda asignar el juez atendiendo a las particularidades de cada caso. La confiabilidad se determina por la (i) autenticidad, entendida como la identificación plena del creador del documento, es decir, la certeza que debe tener el juzgador respecto de la persona a quien se le atribuye la autoría del documento; y por (ii) la veracidad de la prueba, esto es, la correspondencia con la verdad de la declaración o representación del hecho allí expresados. En particular, la valoración de este último atributo de la prueba demanda del juez la aplicación de las reglas de la sana crítica, la presunción de buena fe, los principios del debido proceso, de defensa, de igualdad, y de lealtad procesal.

Por su parte, en la sentencia [T-238 de 2022](#), la Corte amparó los derechos de un hombre a quien se le declaró la caducidad de la acción en un proceso de impugnación de paternidad. El juzgado consideró que el laboratorio encargado de la prueba de paternidad envió los resultados por correo electrónico un año antes, según una captura de pantalla incluida en el proceso, lo que implicó que el plazo para impugnar había vencido. Sin embargo, el actor afirmó



DERECHOS en el escenario DIGITAL y de las TIC



que conoció los resultados un mes antes de iniciar el proceso. La Corte determinó que el juzgado erró al decidir con base únicamente en la captura de pantalla, prueba indiciaria, sin considerar los demás elementos probatorios ni verificar si el actor había acusado recibo del correo. Por último, consideró que:

01

Los mensajes de datos son pruebas válidas en el ordenamiento colombiano.



02

Es deseable que se plasmen firmas digitales y, en general, que se acuda a los medios de prueba que permitan autenticar el contenido de los mensajes de datos, su envío y recepción.



03

Las copias impresas y las capturas de pantalla tienen fuerza probatoria, las cuales deberán ser analizadas bajo el principio de la sana crítica y partiendo de la lealtad procesal y la buena fe.



04

Su fuerza probatoria es la de los indicios, lo que supone la necesidad de valoración conjunta con todos los medios de prueba debidamente incorporados al plenario.



05

Cuando se notifica o comunica por medio de un mensaje de datos, los términos procesales no pueden empezar a contar sino hasta el momento en el que el iniciador recepcione “acuse de recibo” o, en su defecto, cuando se pueda constatar, por cualquier medio, el acceso del destinatario al mensaje de datos.



Gráfica 12. Elaboración propia con base en la sentencia T-238 de 2022.



DERECHOS en el escenario DIGITAL y de las TIC



VIDEO

Video sobre valoración
probatoria de los
mensajes de datos

Respecto a este tema, también pueden consultarse las sentencias [T-420 de 2023](#), [T-186 de 2023](#), [T-347 de 2024](#), [T-189 de 2024](#), [T-293 de 2023](#), [T-045 de 2025](#), [T-132 de 2025](#), [T-164 de 2025](#), [T-272 de 2025](#) y [T-291 de 2025](#).

VIDEO

Video sobre notificación
del estado de gestación
por WhatsApp



5.4 Acceso a la información privada enviada por correo electrónico para servir como medio de prueba en procesos judiciales

En la sentencia [T-916 de 2008](#) se amparó los derechos de un ciudadano quien afirmó que, durante un proceso de divorcio, el juez consideró como prueba unos correos electrónicos que fueron obtenidos sin su consentimiento. La Corte señaló que la interferencia en las comunicaciones, sin el consentimiento de la persona afectada y con fines de divulgación, puede vulnerar este derecho a la intimidad.



Sentencia *T-916 de 2008*

La correspondencia y demás formas de comunicación privada son inviolables y sólo podrán ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Cabe recordar, que una cosa es compartir una cuenta de correo electrónico y otra muy distinta registrar el correo del otro, sustraerlo, y presentarlo como prueba en proceso judicial, todo ello sin el consentimiento de la parte a quien se encontraba dirigido el mismo.

En la sentencia [T-044 de 2013](#), se estudió una tutela presentada por una mujer que, durante un proceso de divorcio, solicitó al juzgado accionado que decretara pruebas relacionadas con una grabación magnetofónica y una inspección judicial a la cuenta electrónica de su cónyuge. El juzgado negó esta solicitud. La Corte indicó que el derecho a la intimidad puede restringirse cuando la integridad y seguridad de una familia están en juego, dado que los medios de prueba solicitados resultan pertinentes, ya que los hechos que se buscan demostrar son difíciles de acreditar con otros elementos distintos a los



solicitados. En consecuencia, la Corte amparó los derechos de la actora y ordenó que se decretaran las pruebas.

5.5. Notificación personal para la presentación y sustentación de recursos judiciales por medios electrónicos

En la sentencia [SU-387 de 2022](#), la Corte conoció una tutela presentada por varios accionantes contra el Consejo de Estado. Los actores afirmaron que la Corporación judicial vulneró su derecho al debido proceso al rechazar la impugnación presentada por considerarla extemporánea, sin tener en cuenta que el Decreto 806 de 2020 estableció que la notificación personal se entendería realizada una vez transcurrieran dos días hábiles al envío del mensaje. La Corte estimó que el régimen de notificaciones personales previsto en dicha norma aplica en los trámites de tutela. Por ello, determinó que se presentó una vulneración al no tener en cuenta los términos de notificación personal. En consecuencia, amparó los derechos de los actores y ordenó dar curso a la impugnación.



Sentencia [SU-387 de 2022](#)

La aplicación de las reglas de notificaciones del artículo 8 del Decreto Legislativo 806 de 2020 a la notificación personal de la sentencia de tutela no compromete la protección efectiva de los derechos fundamentales.

En el mismo sentido, en la sentencia [T-298 de 2023](#), la Corte conoció una tutela en la que un juzgado rechazó un recurso por considerarlo extemporáneo. El accionante afirmó que no se respetó el término establecido en el Decreto 806 sobre la notificación personal. La Corte precisó que, el término para entender que se dio el envío de la notificación empieza a contarse desde que se acuse



el recibo de la comunicación o se pueda constatar el acceso del destinatario al mensaje. Bajo este entendido, reiteró lo dicho por la [SU-387 de 2022](#), amparó los derechos del actor y ordenó dar trámite a la impugnación.

A su vez, en la sentencia [T-261 de 2025](#) se protegieron los derechos al debido proceso y a la defensa de la Rama Judicial, al señalar que en un proceso ejecutivo no se notificó el mandamiento ejecutivo, lo que impidió ejercer su derecho de defensa. Además, señalaron que en el aplicativo SAMAI no se encontraba el expediente electrónico completo. La Corte mencionó que la notificación personal requiere el envío de la comunicación por correo electrónico y, en el caso de ser una entidad pública, esta debe dirigirse al buzón de notificaciones judiciales. Se evidenció que la notificación se envió a un correo distinto al que la parte accionante publicó como exclusivo para recibir notificaciones judiciales de demandas y decisiones judiciales y extrajudiciales en procesos donde la Nación - Rama Judicial sea parte. En consecuencia, se ordenó rehacer la actuación e incorporar todas las piezas del expediente electrónico.

5.6. Uso de la inteligencia artificial en la administración de justicia

La jurisprudencia constitucional ha reconocido que los avances tecnológicos en materia de IA han irradiado cada ámbito de la vida humana, incluido el sistema judicial. En efecto, la proliferación de sistemas de IA y su aplicación en escenarios judiciales, tanto en el trámite como en lo sustancial, dan paso progresivo a un nuevo paradigma en el servicio público de administración de justicia. De allí la necesidad de evaluar las condiciones para que la implementación de estas nuevas tecnologías en la Rama Judicial pueda llevarse a cabo con respeto de los derechos fundamentales, entre ellos el debido proceso.

Lo anterior se desarrolló en la sentencia [T-323 de 2024](#), en la cual la Corte revisó el caso de un niño con TEA a quien se le amparó el derecho a la salud. En esta oportunidad, el juez de segunda instancia empleó ChatGPT 3.5 (IA) para formular preguntas jurídicas sobre el asunto bajo estudio e incorporó las respuestas en la sentencia.



En el caso en concreto, la Corte confirmó parcialmente las decisiones de instancia y amplió la protección del derecho a la salud del menor de edad. Por otra parte, advirtió que, aunque hubo un uso indebido de la herramienta de IA, al no cumplirse con los principios de transparencia y responsabilidad en su totalidad, la decisión del juez es válida, en la medida en que la IA no reemplazó el razonamiento lógico y humano que le correspondía al operador judicial para estudiar y solucionar la controversia, de esa forma, no tuvo lugar una usurpación de la función de administración de justicia a cargo de la autoridad judicial competente.

Dada la novedad del asunto, la Corte se ocupó de realizar algunas aproximaciones frente al alcance del uso de la IA a la hora de adoptar decisiones judiciales. Al respecto señaló que el juez, cuando encuentre necesario y pertinente recurrir a sistemas de IA, puede emplearlos razonada y ponderadamente. Esto supone un enfoque de protección de derechos fundamentales que valore y considere las mejores prácticas, así como la aplicación de criterios éticos y de respeto a los mandatos superiores.

De esta forma, las limitaciones al uso de IA en la administración de justicia tienen como fin último garantizar el debido proceso de los administrados. Respecto a esta relación la Corte estableció que:

- *Frente a la garantía de juez natural:* el juez natural tiene que ser un humano, no una máquina, por lo que la IA no puede reemplazar al juez en la toma de decisiones judiciales. Si una IA toma la decisión sin la valoración y determinación del juez, la decisión sería inválida y esto afecta el derecho al debido proceso.
- La garantía del juez natural se viola cuando el juez utiliza IA para reemplazar el razonamiento lógico y humano necesario para de interpretar los hechos, las pruebas, motivar la decisión o adoptarla. Esto implica una sustitución del poder jurisdiccional.



- *Frente a la garantía de la motivación de las decisiones judiciales:* la administración de justicia exige una alta diligencia para verificar la veracidad y la fiabilidad consultada por el juez y su equipo. No se permite incorporar textos generados con IA en las decisiones judiciales. El juez que incluya estas decisiones incumple con su deber de motivar la decisión, al incluir argumentos que pueden ser contrarios a la realidad.
- El uso de IA generativa en la administración de justicia, sin medidas de protección, puede comprometer la decisión imparcial e independiente del juez, lo que a su vez vulnera el derecho de defensa al producir una desconfianza sobre la fiabilidad de las decisiones.
- *Frente a la garantía del debido proceso probatorio:* los jueces deben garantizar el derecho a la intimidad y privacidad que obran en la prueba judicial. El marco de la protección debe dirigirse a la transparencia sobre el uso que el operador judicial hace de los datos y establecer salvaguardas para la información sensible. En particular, debe evitarse que el uso de algoritmos no licenciados procese los datos personales y los reutilicen haciéndolos accesibles.



Sentencia T-323 de 2024

El uso de IA generativa en la administración de justicia, sin salvaguardas, puede afectar el deber de motivar las decisiones judiciales, las garantías del juez natural independiente e imparcial y el derecho a la defensa al producirse desconfianza sobre la fiabilidad de las decisiones y, por tanto, promoverse que fácticamente se dé un reemplazo del juez por parte de la herramienta y la adopción de los fallos dentro del sistema judicial.



En esa línea, expuso los siguientes criterios orientadores en cuanto al uso de IA por parte de las autoridades judiciales:

Criterios orientadores

1. **Transparencia:** entendida como la obligación de evidenciar con claridad y precisión el uso, alcances y ubicación en las actuaciones o decisiones de los resultados obtenidos por la utilización de tales herramientas, que permita a los usuarios e interesados su pleno conocimiento y la posibilidad efectiva de contradicción.
2. **Responsabilidad:** comprendida como aquella obligación que existe de que el usuario de la herramienta de IA se encuentre capacitado y comprenda los impactos del uso de estas tecnologías, para a su vez dar cuenta del origen, idoneidad y necesidad del uso de la IA y la información suministrada por la misma, la cual debe ser verificada.
3. **Privacidad:** es aquel deber de custodiar y proteger la reserva de los datos personales y sensibles que se ponen en conocimiento de la administración de justicia para cumplir con los fines propios de la Rama Judicial.
4. **No sustitución** de la racionalidad humana: como expresión de la imposibilidad ética y jurídica de sustituir la acción y la responsabilidad del individuo de la especie humana en la gestión de las actuaciones y decisiones judiciales.
5. **Seriedad y verificación:** implica la obligación de realizar un estricto escrutinio sobre las fuentes, alcances, restricciones, posibilidades, falencias y riesgos que presente la herramienta de cara a la actuación en curso o a la solución del problema jurídico correspondiente.



6. **Prevención de riesgos:** como mandato en cuanto aplicar los estándares adecuados de control sobre situaciones que generen riesgo por la aplicación de tecnologías tales, en aspectos como imprecisiones, desactualizaciones, alucinaciones, sesgos, inconsistencias y demás.

7. **Igualdad y equidad:** en cuanto se erradiquen todas las formas de discriminación relacionadas con la aplicación de sesgos derivada del uso de tales tecnologías y su impacto negativo en la eficacia de los derechos humanos.

8. **Control humano:** en tanto siempre se permita la realización efectiva de escrutinios sobre las actuaciones y decisiones en que se usen herramientas de IA, mediante el acceso a la debida información y el uso de recursos que deban ser resueltos por autoridades humanas.

9. **Regulación ética:** implica el desarrollo de estándares de comportamiento individual que se adecúen a los mandatos superiores y legales y a las pautas razonables para el uso de tales tecnologías por parte de los funcionarios y servidores de la Rama Judicial.

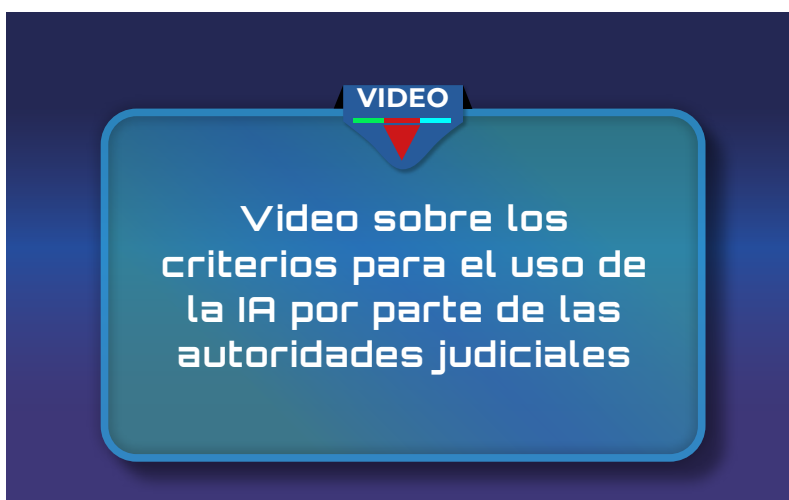
10. **Adecuación a buenas prácticas y estándares colectivos:** en tanto se apliquen los esquemas razonables que se definan para el funcionamiento de la Rama Judicial, desde su autonomía e independencia, a partir de las definiciones que adopten sus autoridades, tanto en sede de administración como de orientación jurisprudencial.

11. **Seguimiento continuo y adaptación:** a efecto que el uso de tales tecnologías consulte los avances jurídicos, sociológicos y tecnológicos que se vayan implementando, así como los esquemas de mejora y control que se construyan en forma progresiva.



12.Idoneidad: el uso de las tecnologías de la información y de las comunicaciones en la gestión y trámite de los procesos judiciales y asuntos en curso debe ser adecuado para facilitar y agilizar el acceso a la justicia.

Gráfica 13. Elaboración propia con base en la sentencia T-323 de 2024.



La Corte exhortó a los jueces para que evalúen el uso correcto de la IA y apliquen los principios antes mencionados y criterios éticos con el fin de garantizar los derechos fundamentales, en especial el del debido proceso.

Además, le ordenó al Cons. S. Jud. divulgar una guía o manual relacionado con la implementación de la IA generativa en la Rama Judicial, esta regulación deberá seguir los lineamientos dados en la sentencia. A su vez, se ordenó la divulgación de la providencia y el fomento de espacios de aprendizaje sobre el uso de la IA en el contexto judicial.

En respuesta a estas órdenes, el Cons. S. Jud. expidió el Acuerdo PCSJA24-12243 del 16 de diciembre de 2024 por medio del cual se adoptaron los lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial.



DERECHOS en el escenario DIGITAL y de las TIC



VIDEO

Video sobre uso de la IA
en el ámbito judicial
(minuto 6:39)



DERECHOS en el escenario DIGITAL y de las TIC



6. DERECHOS DE ACCESO A LA INFORMACIÓN PÚBLICA Y DE PETICIÓN EN CONTEXTOS DIGITALES.

“El uso de las herramientas tecnológicas, incluyendo las redes sociales, ha impactado la forma en la que se desarrolla la comunicación entre los servidores públicos y los ciudadanos, generando la necesidad de normativas que permitan afrontar los nuevos retos que van apareciendo en el entorno digital”

Sentencia T-475 de 2024



El artículo 74 de la Constitución Política establece que, por regla general, todas las personas tienen derecho al acceso a los documentos públicos. Este derecho representa un aspecto cardinal en una democracia constitucional, ya que constituye un derecho fundamental autónomo destinado a garantizar la máxima publicidad y transparencia en las actuaciones del Estado.¹⁸

Cabe destacar que la ley y la jurisprudencia prevén que el ejercicio y la protección de este derecho se rigen, principalmente, por tres principios interrelacionados:

Principios para el ejercicio y la protección del derecho al acceso a la información pública

Principio de máxima publicidad de la información. Según el cual toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la propia ley.

Principio de transparencia. Establece que toda la información en poder de los sujetos obligados definidos en la ley se presume pública y, en consecuencia, ellos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, con exclusión solo de aquello que esté sujeto a las excepciones constitucionales y legales.

Principio de divulgación proactiva de la información. Los sujetos obligados tienen el deber de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública.

Gráfica 14. *Elaboración propia con base en la sentencia T-149 de 2025 y la Ley 1712 de 2014.*

¹⁸ Sentencias T-473 de 1992, T-695 de 1996, T-074 de 1997, C-491 de 2007, C-274 de 2013 y T-067 de 2025.



En cuanto a las restricciones de este derecho, la jurisprudencia ha resaltado que las mismas son excepcionales y su interpretación es restrictiva. Al respecto se ha señalado que:



Sentencia **T-149 de 2025**

El acceso a la información pública es la regla general y que solo en algunos casos y frente a cierto tipo de información es legítima su restricción. Sin embargo, esos límites al derecho al acceso a la información pública deben sustentarse en un motivo preciso, previamente definido en la Constitución o en la ley, y debe ser una restricción razonable y proporcional. Lo anterior, en consideración a las importantes finalidades que persigue el acceso a la información pública.

En esa línea, en la sentencia [C-274 de 2013](#), la Corte realizó el control previo, automático e integral de constitucionalidad del proyecto de ley estatutaria que regula este derecho (Ley 1712 de 2014). En esa providencia, se recogieron las reglas jurisprudenciales que definen tanto el alcance como las limitaciones constitucionalmente admisibles al derecho fundamental al acceso a la información pública.

En el siguiente cuadro elaborado en la sentencia [T-067 de 2025](#) se resumen estas subreglas.



Reglas jurisprudenciales para la protección del derecho fundamental de acceso a la información pública ¹⁹

Ante la inexistencia de reserva legal expresa, el derecho fundamental al acceso a la información se aplica sin restricción.

La limitación o reserva debe estar debidamente sustentada en la ley o la Constitución.

La ley que limite el derecho fundamental de acceso a la libertad de información debe ser precisa y clara.

La reserva opera sobre el contenido mas no sobre la información de la existencia de documentos.

En los escenarios en que es posible escindir la información sobre la cual no recae reserva de aquella protegida, es deber de las autoridades la divulgación parcial de la información.

Deber de motivación de la decisión de invocar la reserva.

Aplicación e interpretación restrictiva de la reserva.

La reserva legal no cobija información que por decisión constitucional debe ser pública.

La reserva debe ser temporal.

Deben existir sistemas adecuados de custodia de la información en reserva.

La reserva obliga a los servidores públicos, pero no a los periodistas.

¹⁹ El contenido de cada una de estas reglas puede consultarse en el cuadro completo elaborado en la sentencia T-067 de 2025. M.P Natalia Ángel Cabo



La reserva no puede impedir el control intra o inter orgánico, jurídico y político de las actuaciones públicas respecto de la información.

Las limitaciones al derecho al acceso a la información pública deben cumplir con los estándares constitucionales de razonabilidad y proporcionalidad.

Procede el control administrativo y judicial a la decisión que alega la reserva.

La reserva en asuntos relacionados con defensa y seguridad nacional debe cumplir con los estándares generales de las limitaciones admisibles del derecho.

Gráfica 15. Síntesis elaborada con base en la sentencia T-067 de 2025.

También la Ley 1712 de 2014 en su artículo 28 desarrolla lo que se conoce como el test del daño al interés público que, tal como se mencionó en la sentencia [T-067 de 2025](#), busca equilibrar el derecho de acceso a la información pública y la protección de ciertos intereses que se pueden ver afectados por la publicación de determinada información. Para ello, la norma establece que el sujeto obligado que niegue el acceso a determinada información pública alegando un daño a un interés particular o público debe demostrar que: (i) la información está relacionada con un objetivo constitucional y legalmente legítimo; (ii) se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014; (iii) la información causaría un daño presente, probable y específico sobre un bien o interés constitucional; (iv) dicho daño excede el interés público que representa el acceso a la información.

Ahora bien, en la actualidad, el Estado opera no solo mediante formatos de información tradicionales, sino también a través de sistemas digitales; por ello, el acceso a la información que maneja el Estado debe adaptarse a estas nuevas y dinámicas fronteras tecnológicas, con el fin de que las personas conozcan la existencia de los datos que estén bajo el poder o custodia de autoridades estatales y puedan acceder a ellos.



En ese contexto, el uso de redes sociales por parte de servidores públicos para el desempeño de sus funciones tiene un impacto directo en la garantía de este y otros derechos, de ahí la importancia de reconocer la idoneidad de este tipo de medios y de establecer la naturaleza de la información que comparten los servidores en sus redes. Al respecto, la Corte resaltó lo siguiente:

Espacios deliberativos, de control y de participación	Transparencia y divulgación proactiva	Uso de perfiles y naturaleza de la información
Las redes sociales son un medio efectivo para la deliberación pública, así como para el control de la gestión pública y la participación ciudadana.	El uso de estos medios digitales es un mecanismo idóneo y efectivo para el cumplimiento del deber de transparencia, e s p e c i a l m e n t e del principio de divulgación proactiva de la información.	La valoración del uso de que los funcionarios públicos le dan a sus perfiles personales en redes sociales y de la naturaleza de la información allí publicada, debe efectuarse conforme con los siguientes criterios: (i) nivel de privacidad de la cuenta; (ii) características de la cuenta; (iii) uso de la cuenta; (iv) cómo se comunica la información y (v) el contenido del mensaje publicado por el servidor público.

Gráfica 16. Elaboración propia con base en la sentencia T-149 de 2025.

A continuación, se mencionan algunos casos en los que la Corte ha protegido este derecho frente a restricciones desproporcionadas en el escenario digital.

6.1. Derecho al acceso a la información pública a través de redes sociales

En la sentencia [T-475 de 2024](#) se protegieron los derechos de una persona que fue bloqueada en la red social X por un ente territorial, con lo cual se le



restringió la posibilidad de interactuar en un canal oficial dispuesto para tratar asuntos de interés general. En esta oportunidad, la Sala constató que dicho bloqueo desconoció el derecho de acceso a la información pública, en particular, aquélla publicada por la entidad en esta red social, así como al desarrollo mismo de esas publicaciones en la cronología del organismo gubernamental.

La Corte destacó que el derecho a recibir información no puede darse por satisfecho cuando se le exige a un usuario acudir a un canal determinado a la vez que se le impide el acceso a otro, pues parte de la información a la que se tiene derecho, incluye el tono, el estilo, la oportunidad y la forma en la que se comunica el mensaje, atributos que pueden estar moldeados por el canal comunicativo al que se acuda.



Sentencia **T-475 de 2024**

A diferencia de lo que ocurre con las páginas web, la comunicación en redes sociales no es vertical ni unidireccional, sino que implica la construcción de una comunidad deliberativa. Así pues, ante las publicaciones del administrador, los usuarios pueden comentar dichas publicaciones y entablar una comunicación directa con el administrador. En este último caso, el administrador puede, por la vía de las respuestas a los comentarios, sentar una postura frente a un cuestionamiento, o en general, suministrar información de interés público. Esta información queda alojada en la red social en la que ocurre la interacción, por lo que el bloqueo también representa la imposibilidad de conocer la forma como el administrador interactúa con la población y suministra información relevante.



Por otra parte, se reiteró la jurisprudencia sobre la prohibición de censura. Al respecto, se refirió que el bloqueo en una red social como X constituye un acto de censura cuando concurren, en principio, ciertos elementos no taxativos a saber:

- Que la cuenta de X sea de una entidad pública y se emplee con fines públicos.
- Que la cuenta haya sido creada con la finalidad clara de interactuar con la población sobre asuntos de interés público.
- Que la exclusión de publicaciones o de participantes en las cuentas de opinión no responda a una finalidad legítima, ni a un criterio neutral frente a la opinión que estos contengan o expresen.
- Que la exclusión de contenidos o actores no sea el resultado de un proceso previsto en las reglas de la comunidad para los supuestos de incumplimiento.

En el mismo sentido, en la mencionada sentencia [T-149 de 2025](#), la Corte ordenó desbloquear a un periodista de algunas redes sociales de una congresista indígena. Si bien en la sentencia se analizaron y se sancionaron las conductas del periodista constitutivas de VCMP, la Corte amparó su derecho a acceder a la información pública contenida en dichas cuentas.



Sentencia **T-149 de 2025**

Las excepciones y restricciones al acceso a información pública se refieren exclusivamente a la calidad de la información, su naturaleza y el tipo de datos que la componen. No a la calidad de las personas o solicitantes que pretenden acceder a la misma.



6.2. Derecho de acceso a la información pública relacionada con sistemas de toma de decisiones automatizadas

En la sentencia [T-067 de 2025](#), la Corte protegió los derechos de un ciudadano a quien se le negó el acceso al código fuente de la aplicación digital CoronaApp, la cual incluye información de los ciudadanos en el marco de la contención del virus Covid 19, bajo el argumento de que dicho código es de carácter reservado y que su publicación puede poner en riesgo la integridad y reserva de los datos personales administrados por esa plataforma. Al resolver el caso, la Corte determinó que las autoridades accionadas no justificaron en debida forma la negativa frente al acceso a la información pública solicitada, por ende, se ordenó que dicho código fuera entregado al accionante.

Al respecto, se señaló que, en los eventos en los cuales un sujeto obligado niegue el acceso a información pública por considerar que tiene carácter de clasificada o reservada se debe demostrar que: (i) la información se relaciona con un objetivo legítimo establecido legal o constitucionalmente; (ii) se trata de una de las excepciones expresamente establecidas en los artículos 18 y 19 de la Ley 1712 de 2014 ; y (iii) al revelar la información se causaría un daño presente, probable y específico sobre un bien o interés constitucional y (iv) el daño es sustancial, es decir, mayor al beneficio de dar acceso a la información.

Respecto al tercer punto, se resaltó lo estipulado en el artículo 28 de la referida Ley, el cual establece una carga probatoria para quien niegue el acceso a la información bajo argumentos de reserva, esta se conoce como el Test del Daño. Este es un mecanismo legal que evalúa si la restricción a la información tiene justificación, de esa forma, se busca equilibrar el derecho de acceso a la información pública con la protección de ciertos intereses que podrían afectarse por la divulgación de determinada información. En virtud de este juicio argumentativo, el sujeto obligado que niegue la entrega de la información pública alegando un daño a un interés particular o público, debe demostrar lo siguiente:

1. Que se trate de un daño real y presente.



2. Que se trate de un daño probable.
3. Que se trate de un daño específico.

Si la autoridad cumple con esta carga probatoria, puede mantener la reserva de la información, si no cumple, debe suministrar lo solicitado.

En el caso mencionado, la Corte estimó que la falta de transparencia y acceso al código fuente de la aplicación no solo disminuyó la extensión, obligatoriedad y funcionalidad del derecho fundamental al acceso a la información pública, sino que también impidió que los ciudadanos pudieran verificar la precisión, seguridad y uso correcto de sus datos personales, limitando así su capacidad para proteger sus derechos a la privacidad, a la protección de datos y a la participación informada en los procesos de toma de decisiones públicas.



Sentencia **T-067 de 2025**

En un sistema constitucional y democrático, los ciudadanos deben conocer la forma, el fundamento y el proceso a través del cual se toman las decisiones de política pública que los afectan. Cuando los ciudadanos no conocen la forma en la que las aplicaciones o sistemas de toma de decisiones están construidas, no pueden llegar a entender a cabalidad cuál es la finalidad con la que el Estado usa los datos de las personas. Tampoco pueden saber si existen defectos en el diseño que lleguen a generar o reproducir graves discriminaciones o sesgos. Por ello, el derecho de los ciudadanos a acceder, en la medida de lo posible, a información sobre los sistemas algorítmicos que utiliza el Estado para la toma de decisiones, y el uso que se le da a los mismos, es una garantía fundamental para evitar que estas tecnologías lleven a la vulneración de otros derechos fundamentales.



DERECHOS en el escenario DIGITAL y de las TIC



En esta oportunidad, teniendo en cuenta las particularidades del tipo de información solicitada, la Corte se pronunció sobre el derecho de acceso a la información pública en el marco del uso de **sistemas de tomas de decisiones automatizadas**, como herramientas tecnológicas que puede hacer que las decisiones de política pública sean más eficientes, confiables y precisas, pero que no están exentas de generar riesgos y vulneraciones de derechos fundamentales. A continuación, se hace referencia a algunos conceptos que permiten comprender mejor el funcionamiento de estos sistemas.

Sistemas de tomas de decisiones automatizadas (SDA): son herramientas que utilizan un proceso algorítmico para llegar a una decisión, ya sea un ranking, calificación o asociación, que puede llevar luego a otra acción o comportamiento. Se dice que estos sistemas actúan en el marco de la inteligencia artificial, o que son sistemas de inteligencia artificial, porque contribuyen a procesos de toma de decisiones que normalmente serían llevados a cabo por humanos.

Son este tipo de sistemas que, con base en el algoritmo, o su traducción al código fuente, se procesa determinada información o datos (como el estado del tráfico, o las calificaciones y estatus socioeconómico de un potencial estudiante) para llegar a una decisión (la ruta más rápida o el cupo en determinada universidad), o, por lo menos, para informar o apoyar a un individuo en la toma de decisiones.

Algoritmo: conjunto de reglas y procedimientos que se siguen para resolver un problema determinado de manera lógica y eficiente. En palabras más sencillas, un algoritmo es una serie de pasos ordenados que hacen que una información de entrada - “input”- se convierta en un resultado -“output”-, y puede ser implementado en forma de un programa de computación que resuelve el problema de forma automatizada y mucho más veloz.

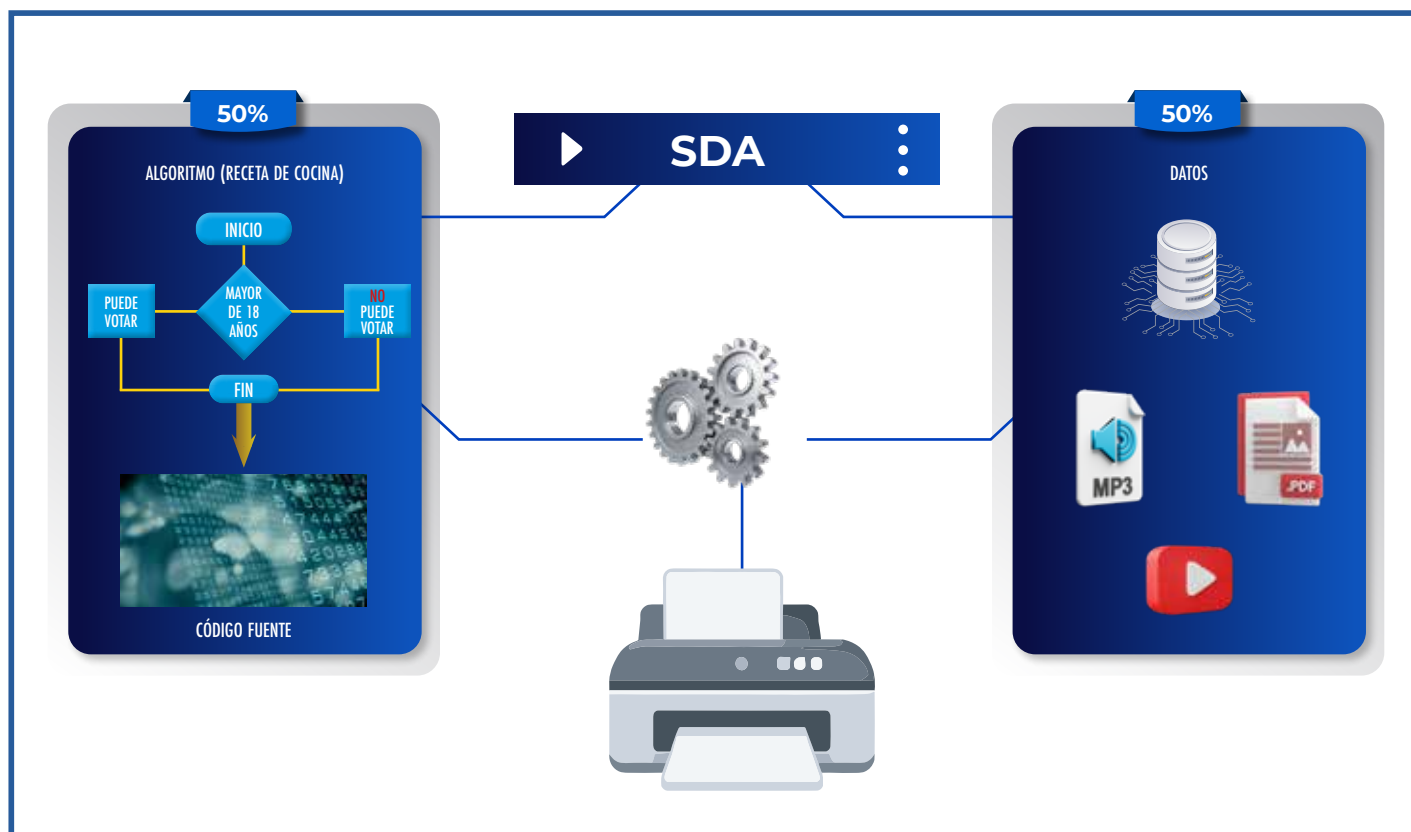
Código fuente: para que un computador tenga la capacidad de entender y procesar un algoritmo, este debe ser traducido a un lenguaje computacional. Esa traducción del algoritmo es lo que se conoce como el código fuente. Es la columna vertebral del software o la aplicación, y es lo que proporciona la estructura y las directrices necesarias para que se ejecuten las instrucciones o pasos previstos en el algoritmo. Estos pasos pueden consistir en procesar datos, tomar decisiones y producir resultados. Sin esta base, el algoritmo carecería de la dirección y la lógica necesarias para operar. Este puede ser abierto o cerrado:

Abierto: se pone a disposición del público para que cualquier persona pueda modificarlo y construir sobre él.

Cerrado: Protegidos bajo la figura de derechos de autor.



Gráfica 17. Elaboración propia con base en la sentencia T-067 de 2025.



Gráfica 18- Elaboración propia con base en la sentencia T-067 de 2025.

En ese contexto cobra relevancia la garantía de **transparencia algorítmica**, a través de la cual se busca que los ciudadanos puedan conocer y comprender cómo los sistemas de toma de decisiones automatizadas (SDA) procesan los datos que capturan y cómo toman decisiones que afectan la vida de las personas. Según lo dicho en esta sentencia, se trata de un principio con un fin constitucional: democratizar el funcionamiento interno de un sistema de toma de decisión automatizado, para que sea entendible por quienes se ven afectados por su puesta en marcha y operación.



Sentencia T-067 de 2025

Se trata de una garantía fundamental en una sociedad democrática, pues si un sistema de toma de decisiones automatizadas (SDA) opera y toma decisiones de manera opaca, es imposible que la sociedad evalúe su capacidad de actuar con justicia y equidad, o su impacto en la autonomía y la dignidad de las personas. Como su propia definición lo revela, la transparencia algorítmica es un concepto que se deriva de un elemento que hace parte sustancial e inescindible de la naturaleza del derecho fundamental al acceso a la información pública: la disponibilidad de información.

La Corte destacó que la transparencia algorítmica no se garantiza de una sola manera, en ese sentido, debe ser vista como un espectro en el que, a través de diferentes mecanismos, se le permite a la ciudadanía conocer y entender la forma en la que los sistemas utilizados por las entidades públicas toman las decisiones, algunos de estos mecanismos se muestran a continuación:



DERECHOS en el escenario DIGITAL y de las TIC



Formas de transparencia algorítmica

Perfecta o completa: el receptor de la información tiene un conocimiento completo de las reglas de funcionamiento del sistema y de su proceso de creación.

Significativa: se tiene un conocimiento suficiente para valorar el algoritmo. En ese sentido, se conoce lo necesario para que las personas puedan entender y valorar el sistema algorítmico detrás de las decisiones públicas. Esta tiene dos elementos:

Accesible: auditorías o inspecciones externas que analicen y expliquen sus impactos.

Explicabilidad: las personas deben poder entender, en lenguaje sencillo y concreto, cómo el sistema llegó a un determinado resultado.

Activa: el Estado, de manera abierta y permanente, ofrece información sobre sus sistemas de operación a través de la publicación periódica en portales de datos abiertos o en repositorios de licencias públicas de desarrollo de aplicaciones.

Pasiva: se da a raíz de solicitudes de acceso a la información. En estos casos, el Estado publica información sobre el algoritmo o sobre el SDA que utiliza en sus procesos, como respuesta a solicitudes específicas elevadas por cualquier ciudadano en ejercicio de su derecho de acceso a la información pública.

Gráfica 19. Elaboración propia con base en la sentencia T-067 de 2025.

La Corte resaltó que, si bien una de las formas de garantizar la transparencia algorítmica es a través de la publicidad total o condicionada del código fuente, esta práctica tiene algunos riesgos relacionados con la manipulación de código, la precisión de la información frente a la actualización de los algoritmos o la protección de la privacidad de la información.



Frente a este contexto, se advirtió que habrá situaciones en que una explicación significativa sobre el funcionamiento del sistema sea más apropiada que la publicidad total del código fuente, ya que esta puede crear riesgos desproporcionados para la seguridad nacional o desconocer secretos empresariales. No obstante, es fundamental tener en cuenta que cuando se trata de SDA a cargo de entidades públicas, la transparencia algorítmica activa y pasiva debe guiarse bajo un principio de divulgación máxima. Según este principio, es importante que la información revelada al público para vigilar la acción digital del Estado permita examinar el desempeño de la aplicación informática o herramienta tecnológica utilizada. Por ello, en cada caso, habrá que analizarse cuál es la medida que maximiza el acceso a la información, sin afectar de manera desproporcionada otros derechos e intereses.

En este punto, la Corte también destacó el papel de los jueces constitucionales como garantes del derecho fundamental al acceso a la información pública y los deberes que tienen respecto a la valoración de las excepciones de acceso a una información pública.



Sentencia **T-067 de 2025**

Ante solicitudes de información, las autoridades y los jueces constitucionales deberán analizar los riesgos y beneficios de dar acceso a determinado código fuente, así como encontrar alternativas que balanceen entre el interés público de acceder a la información y los riesgos (reales, probables y específicos) que están implícitos en esa publicidad. Priorizarán siempre la transparencia significativa y el acceso a la información.



Por último, en este pronunciamiento, se dictaron una serie de órdenes generales entre las cuales se destaca que la AND, junto con las oficinas designadas por la PGN y a la Defensoría del Pueblo, deberán expedir una serie de lineamientos relacionados con la transparencia algorítmica en los sistemas algorítmicos utilizados por el Estado. Dichos lineamientos deberán propender por la maximización de los estándares de transparencia, confianza y acceso a la información pública.

6.3. Derecho de petición por medios tecnológicos

En la sentencia [T-230 de 2020](#), la Corte amparó los derechos de un ciudadano que presentó una petición a través de una red social de una entidad pública. Sin embargo, la accionada no le brindó respuesta y señaló que la red social Facebook no es un canal de comunicación oficial de la entidad, en la medida en que no es administrada por el área de atención al usuario.

La Corte señaló que, las peticiones formuladas por medios electrónicos habilitados por la autoridad pública deben tramitarse como si se tratara de un medio físico, siempre y cuando se cumplan los siguientes requisitos: (i) determinar quién es el solicitante; (ii) que esa persona apruebe lo enviado y (iii) verificar que el medio electrónico cumpla con características de integridad y confiabilidad, es decir, que el canal permite constatar el trayecto del mensaje desde que fue enviado por el originador hasta que fue recibido por su destinatario. Así mismo, refirió que las redes sociales han fomentado en la sociedad la expectativa de recibir información inmediata sobre las acciones del Estado, así como la obligación de las entidades públicas de ofrecer dicha información sin demora.



Sentencia *T-230 de 2020*

Cualquier tipo de medio tecnológico habilitado por la entidad y que funcione como un puente de comunicación entre las personas y las entidades, podrá ser utilizado para el ejercicio del derecho fundamental de petición. De ahí que, siempre deberá ser atendido por los funcionarios correspondientes para dar respuesta a las solicitudes, quejas, denuncias y reclamos que se canalicen por dicho medio.



DERECHOS en el escenario DIGITAL y de las TIC



7. DERECHO A LA PARTICIPACIÓN POLÍTICA EN EL PLANO DE LA DEMOCRACIA DIGITAL

“Es indudable que los escenarios digitales han facilitado y democratizado el ejercicio de la libertad de expresión, de modo que el debate público dejó de estar concentrado en los medios tradicionales de comunicación y, en cambio, abrió el espacio para que la población se exprese directamente en dicho ámbito”.

Sentencia T-475 de 2024



De acuerdo con el artículo 40 superior, entre otras disposiciones normativas, el derecho a la participación política se garantiza a través de los siguientes mecanismos: (i) elegir y ser elegido; (ii) participar en elecciones, plebiscitos, referendos, consultas populares y otras formas de participación democrática; (iii) constituir partidos, movimientos y agrupaciones políticas sin ninguna limitación; (iv) interponer acciones públicas en defensa de la Constitución y la ley; (v) difundir ideas y programas políticos; (vi) revocar el mandato de funcionarios electos y (vii) acceder al desempeño de funciones y cargos públicos, entre otros.²⁰ Algunas de estas formas de materializar el derecho a la participación política encuentran en el entono digital un escenario propicio que, de cierta forma ha facilitado la interacción en materia política pero también ha suscitado algunas tensiones entre los derechos de quienes trasladan el debate público a las redes sociales.

Tal como se refirió en la sentencia [T-149 de 2025](#), nos encontramos en un contexto de ciudadanía y democracia altamente digitalizado. Esto se evidencia, especialmente, en el uso de plataformas tecnológicas como medios de comunicación, manifestación, interacción, difusión de información, organización, consolidación de comunidades y participación política. En efecto, estas tecnologías han permitido romper barreras sociales, económicas y geográficas de acceso a escenarios de manifestación, control ciudadano y participación. Lo anterior se debe a que constituyen medios de gran alcance, gratuitos, inmediatos y desterritorializados, que incluso resultan más efectivos para el ejercicio de derechos fundamentales que los medios tradicionales de comunicación.

A continuación, se mencionan algunos casos en los cuales la Corte analizó el derecho a la participación política a través de herramientas digitales.

²⁰ Sentencia T-149 de 2025.



7.1. Encuestas electorales realizadas a través de internet

En la sentencia [C-1153 de 2005](#), la Corte estudió la constitucionalidad del proyecto de ley que reglamentó la elección del presidente de la República, en el cual se incluía la posibilidad de publicar encuestas electorales en Internet. La Corte reconoció que las encuestas realizadas a través de Internet no están al alcance de toda la población, pero esto no significa que se prohíba recurrir a otras metodologías que sí permiten medir con mayor amplitud y en otros estratos sociales la intención electoral. La Sala Plena consideró que quienes sí tienen la posibilidad de manifestar su opinión por esa vía no deberían perderla. En consecuencia, declaró exequible esta disposición.

7.2. Derecho a la participación política a través de redes sociales y protección a las mujeres ante todo tipo de violencia

En la mencionada sentencia [T-149 de 2025](#), además de proteger los derechos a la libertad de expresión y al acceso a la información del periodista que fue bloqueado de algunas redes sociales por parte de una congresista, la Corte protegió su derecho a la participación política. Al respecto, la Corte señaló que las redes sociales de funcionarios y entidades públicas, al usarse para fines oficiales, se convierten en “foros públicos digitales”, estos son espacios abiertos al público en donde se puede producir un debate, opinión, control o rendición de cuentas, por lo que bloquear a un ciudadano —especialmente a un periodista por sus críticas— constituye un acto de censura desproporcionado.

Por otra parte, la Corte reconoció en este caso la ocurrencia de actos de VCMPP en redes sociales en contra de la congresista por parte del accionante que también afectaron su derecho a la participación política en un escenario libre de violencias. Frente a este punto, la Corte destacó:



Sentencia T-149 de 2025

Se acentuaría el silenciamiento de las mujeres y se desincentivaría la participación de estas en el ámbito político, al avalar actos tendientes a desacreditarlas por sus capacidades y calidades personales. De hecho, los efectos producidos por este tipo de agresiones no se circunscriben solamente a la vulneración de los derechos de la accionada a una vida libre de violencias, a la dignidad humana y a la integridad personal. Por el contrario, tienen un alcance expansivo que desconoce el rol esencial de la mujer en la promoción y defensa de sus propios intereses y los de su colectividad y, a su vez, permitir que la arena política digital o presencial se configure como un espacio hostil para las mujeres incrementa la autocensura, el temor a participar en la vida política y, además, transmite un mensaje equivocado al dar a entender que para evitar ser víctima es necesario no ejercer los derechos políticos de los que son titulares las mujeres.

7.3. Transmisión por parte de la ciudadanía de sesiones de los órganos colegiados del Estado a través de redes sociales

En la sentencia [T-230 de 2025](#), la Corte protegió los derechos de un ciudadano a quien no se le permitió grabar y transmitir las sesiones de un concejo municipal por no tener acreditación como periodista, no contar con el consentimiento de los miembros del órgano para el tratamiento de datos personales y por ser señalado de emitir información parcializada.



En este caso, la Corte encontró vulnerado, entre otros, el derecho a realizar control político debido a que ninguna de las tres razones por las cuales se le negó grabar y transmitir tiene respaldo constitucional. Al respecto, se adujo lo siguiente:



Sentencia **T-230 de 2025**

Primero, por regla general, las sesiones de los órganos colegiados políticos son públicas y pueden ser transmitidas por los periodistas profesionales o ciudadanos. En efecto, la transmisión de las sesiones de corporaciones públicas no se puede limitar de forma general, y transmitir las sesiones de las corporaciones públicas es vital para el control político. Segundo, las corporaciones colegiadas públicas pueden tener sus propios mecanismos de difusión, pero esto no limita la posibilidad de que los periodistas profesionales o ciudadanos transmitan las sesiones. Tercero, la transmisión de las sesiones de órganos colegiados no requiere autorización para el tratamiento de datos personales.



DERECHOS en el escenario DIGITAL y de las TIC



8. DERECHO AL HABEAS DATA EN EL MARCO DEL USO DE NUEVAS TECNOLOGÍAS

“En Internet, la intimidad de los usuarios y la garantía del habeas data, son dos derechos que resultan plenamente eficaces. (...) En todo caso, es necesario asegurar ciertas garantías mínimas a todos los usuarios que acceden a este sistema de información. (...) debe asegurarse –en virtud del derecho de habeas data- que tal información no va a ser inapropiadamente utilizada, lo cual supone que su almacenamiento y destinación, necesariamente temporales, se limitará a la recolección de datos precisos, veraces y completos que resulten relevantes para los fines de información e inspección para los que se solicitan”

Sentencia C-1147 de 2001



El artículo 15 de la Constitución Política consagra tres derechos fundamentales interdependientes: (i) el derecho a la intimidad personal, (ii) el derecho al buen nombre, y (iii) el derecho a conocer, actualizar y rectificar información personal. Este último se conoce como derecho al *habeas data* y busca proteger los datos personales. Este derecho, regulado por la Ley Estatutaria 1581 de 2012⁵, adquiere una particular relevancia en las sociedades contemporáneas en las que hay una acelerada trasmisión de la información través de medios tecnológicos y una vasta masa de datos.



Sentencia **T-443 de 1994**

El derecho al *habeas data* es un derecho fundamental concebido para contrarrestar los peligros del desarrollo de la informática que, junto con la electrónica y las telecomunicaciones, hace posible la difusión ilimitada de datos de la persona. Su finalidad principal consiste en preservar la información individual ante su utilización incontrolada. Este derecho otorga a la persona la posibilidad jurídica de impedir que terceras personas usen datos falsos, erróneos o reservados y desvirtúen así su identidad o abusen del derecho a informar.

Según lo dicho en la sentencia [T-729 de 2002](#), el derecho al *habeas data* otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de estos, de conformidad con los principios que regulan el proceso de administración de datos personales. Cabe destacar que



este derecho no siempre se consideró un derecho autónomo²¹. A continuación, se muestra parte del recorrido jurisprudencial hasta llegar a dicho reconocimiento:



T-414 de 1992: Primera sentencia sobre habeas data. Asoció el concepto de “libertad informática”.



T-340 de 1993: El derecho al habeas data como parte del derecho a la intimidad.



SU- 082 de 1995: Reconoce que el núcleo esencial de este derecho está compuesto por la “autodeterminación informática”, entendida como la facultad de la persona a la cual se refieren los datos para autorizar su conservación, uso y circulación.



T-552 de 1997 - T-307 de 1999: Se reconoce el derecho al habeas data como derecho autónomo. Línea que se mantiene hasta la actualidad.

²¹ Sentencia **T-585 de 2012** M.P Jorge Ignacio Pretelt Chaljub: La jurisprudencia constitucional, en un principio interpretó el derecho al habeas data como una garantía del derecho a la intimidad, sin embargo, desde los primeros años de la nueva Carta, también surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad. Según esta línea, el habeas data tiene su fundamento último “(...) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad”. A partir de 1995, surge una tercera línea interpretativa que apunta al habeas data como un derecho autónomo y que es la que ha prevalecido desde entonces. Así, según la sentencia SU-082 de 1995, el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad. Además, este derecho comprende al menos Las siguientes prerrogativas: “a) El derecho a conocer las informaciones que a ella se refieren; || b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; || c) El derecho a rectificar las informaciones que no correspondan a la verdad.”, e incluye el derecho a la caducidad del dato negativo. En esta misma dirección, en la sentencia **T-176 de 1995**, la Corte indicó que el derecho al habeas data es vulnerado cuando se desconoce alguna de las prerrogativas enunciadas en la sentencia **SU-082 de 1995**, es decir, cuando la información contenida en el archivo o base de datos es “(...) recogida de manera ilegal, sin el consentimiento del titular del dato”, es errónea o recae “(...) sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente”.

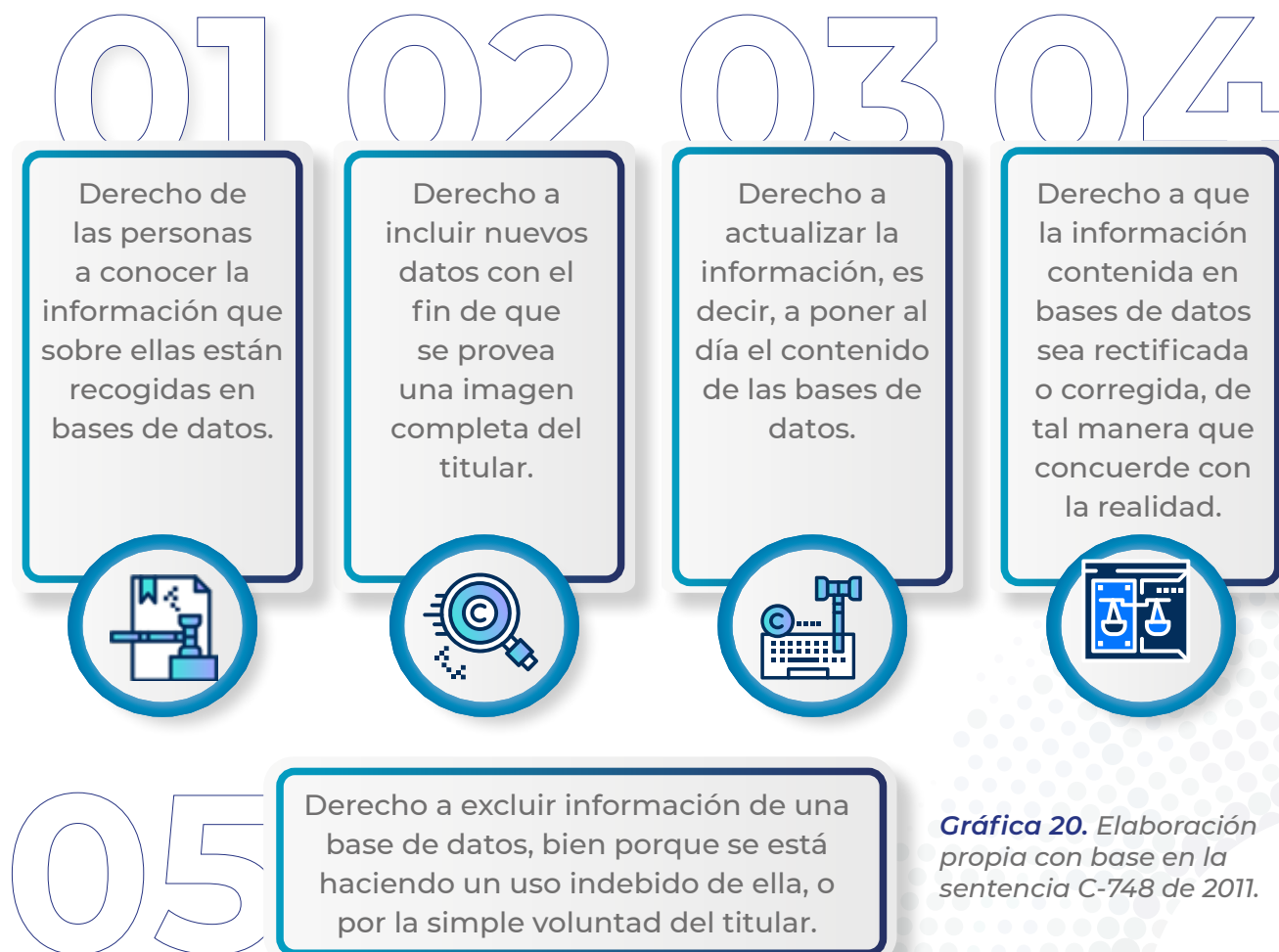


DERECHOS en el escenario DIGITAL y de las TIC



En la sentencia [T-307 de 1999](#), la Corte refirió que este derecho, también denominado como “derecho - garantía a la libertad o autodeterminación informática”, tiene dos dimensiones distintas pero complementarias. De una parte, les confiere a las personas el poder jurídico para conocer e incidir sobre el contenido y la difusión de la información personal que les concierne y que se encuentra archivada en un banco de datos. Por otra parte, establece un conjunto de principios en torno a los cuales debe girar todo el proceso de acopio, uso y transmisión de datos personales.

Al respecto, la Corte ha destacado los siguientes contenidos mínimos de este derecho:



Gráfica 20. Elaboración propia con base en la sentencia C-748 de 2011.



En cuanto a los principios, en la sentencia [T-294 de 2023](#), la Corte mencionó que tanto la legislación estatutaria como la jurisprudencia constitucional han determinado el contenido y alcance de esa garantía superior a partir de la identificación de los principios de administración de datos personales, de los cuales se derivan diferentes prerrogativas para el titular del dato personal, así como deberes correlativos para los responsables y encargados del tratamiento al igual que para los usuarios de esa información. A continuación, se muestra una tabla con una síntesis del contenido de estos principios.

Principios de administración de datos personales	
Principio	Contenido
Principio de libertad	El tratamiento del dato personal solo puede ejercerse ante el consentimiento cualificado de su titular, esto es, previo, expreso e informado. Esto salvo que concurra un mandato legal o judicial que releve esa autorización.
Principio de finalidad	Impone el deber de que el tratamiento de los datos personales cumpla un objetivo constitucionalmente legítimo y que sea conocido por el titular al momento de extender su autorización, precisamente con el fin de que consienta sobre la recopilación del dato para tales fines. Ese objetivo, en consecuencia, debe estar necesariamente vinculado con el ámbito delimitado por la autorización del titular o la prescripción legal que la releva.
Principio de calidad o veracidad	Impone la necesidad de que la información personal contenida en bases de datos sea cierta, completa y actualizada. Por ende, se vulnera el derecho al habeas data cuando los registros no responden a la realidad, están fraccionados o no concuerdan con las actuales condiciones del sujeto concernido.



Principio de necesidad	Actividad de recopilación y tratamiento de datos personales debe restringirse a aquella información indispensable para el cumplimiento de la finalidad para la cual se ha constituido la base de datos y que está cobijada por la respectiva autorización o mandato legal supletorio.
Principio de transparencia o de libertad de acceso al titular	Exige que el sujeto concernido tenga la posibilidad de conocer en cualquier momento y sin restricción alguna la ubicación y uso de sus datos personales objeto de tratamiento en una base de datos.
Principio de acceso o circulación restringida	Confiere al titular del dato la garantía de que el tratamiento de su información personal y la transmisión de datos a los usuarios solo se realizará para los propósitos de la base de datos y que han sido objeto de autorización o mandato legal o judicial excepcional.
Principio de incorporación	Impone al responsable del tratamiento la obligación de registrar en una base de datos toda aquella información del sujeto concernido que involucre una consecuencia favorable para él.
Principio de temporalidad	Obliga a que el tratamiento de los datos personales permanezca únicamente por el tiempo necesario para el cumplimiento de los fines de la base de datos. De lo contrario, se configura una administración abusiva de esa información.
Principio de integridad	Obliga a tratar los datos personales en forma completa, es decir, que se incluya toda la información relevante para el cumplimiento de los fines de la administración del dato personal.



DERECHOS en el escenario DIGITAL y de las TIC



Principio de seguridad	Impone al encargado, al responsable y al usuario del dato personal objeto de tratamiento, la adopción de medidas técnicas y tecnológicas para evitar su acceso o circulación indiscriminada o diferente a las finalidades para las cuales se recopiló la información, así como su adulteración o pérdida.
Principio de confidencialidad	Deber de todas las personas involucradas en el tratamiento del dato personal de garantizar la reserva de la información (que no sea pública), incluso después de cumplido el objetivo para el cual se recopiló.
Principio de legalidad	Impone el deber de que el tratamiento de datos personales se realice con sujeción a las disposiciones constitucionales y legales y, en particular, con apego y respeto de los derechos fundamentales.
Principio de responsabilidad demostrada	Consiste en el deber que le asiste al responsable del tratamiento de datos de demostrar ante la autoridad de datos que cuenta con la institucionalidad adecuada y los respectivos procedimientos internos para garantizar el efectivo goce del derecho al habeas data. Específicamente, debe evidenciar la vigencia del principio de libertad, las facultades de conocimiento, actualización y la rectificación del dato personal. En plena correspondencia con la Superintendencia de Industria y Comercio, este principio implica que las medidas adoptadas para cumplir con el referido derecho son útiles, pertinentes y eficientes.

Gráfica 21. Elaboración propia con base en las sentencias T-360 de 2022 y T-294 de 2023.



La Corte ha estudiado el alcance de este derecho en varias oportunidades, tanto en sede de constitucionalidad como de tutela. A continuación, se hará referencia a algunos de estos pronunciamientos.

En las sentencias [C-1011 de 2008](#), [C-748 de 2011](#), [C-032 de 2021](#) y [C-282 de 2021](#), la Corte realizó un control automático de constitucionalidad sobre proyectos de ley estatutaria relacionados con la protección de datos personales.

Por su parte, en la sentencia [C-1066 de 2002](#) la Corte analizó la demanda de inconstitucionalidad contra el artículo 174 (parcial) de la Ley 734 de 2002. En esta oportunidad se declaró la exequibilidad condicionada del Código Disciplinario Único en el sentido que las certificaciones sobre antecedentes disciplinarios sólo incluirán las providencias ejecutoriadas dentro de los cinco años anteriores a su expedición y, en todo caso, aquellas que se refieren a sanciones o inhabilidades que se encuentren vigentes en dicho momento.

Por otro lado, en la sentencia [C-276 de 2019](#) la Corte estudió la demanda de inconstitucionalidad contra el artículo 298 (parcial) de la Ley 906 de 2004 el cual faculta a la Policía Judicial para difundir órdenes de captura a través de medios de comunicación. Esta corporación declaró exequible el inciso 3° del artículo y señaló que la información contenida en la orden de captura es pública y no está clasificada. Si bien contiene datos personales, se trata de información incluida en una providencia judicial que no afecta el núcleo esencial de los derechos a la vida, la intimidad, la salud y la seguridad del titular. Por último, se precisó que esta facultad de divulgación, no vulnera el derecho a la presunción de inocencia, siempre que la difusión de la información esté precedida por autorización judicial. En lo referente a los casos de tutela, en la siguiente tabla se presentan algunas consideraciones extraídas de casos analizados por la Corte, los cuales se clasifican según la temática abordada en cada pronunciamiento.



Sentencias de tutela relacionadas con la protección del derecho al *habeas data*

Asunto	Sentencia y consideración destacada
8.1. Tratamiento de información sobre transacciones económicas realizadas en Internet	
Recolección de información con fines tributarios sobre transacciones económicas realizadas en Internet	C-1147/01: la información que puede ser objeto del registro o de la solicitud que hace la administración tributaria, corresponde a datos de los que tiene pleno conocimiento la persona requerida que se generan como consecuencia del giro normal de sus actividades. Esto resulta razonable, pues son los agentes materiales de la actividad económica que se desarrolla a través de las páginas web o sitios de Internet quienes poseen, de primera mano, la información precisa sobre la cuantía y modalidad de las transacciones que realizan por Internet. No obstante, tales personas también pueden tener información reveladora sobre la identidad y las preferencias de los usuarios, circunstancia que impone la necesidad de establecer ciertos límites al tipo de datos que se comparte. Así, la exigencia de cierta información por parte de las autoridades no puede reñir con la existencia del derecho a la intimidad y el reconocimiento del derecho de <i>habeas data</i> que, en materias de inspección tributaria, sustrae del conocimiento de terceros -trátase de la Administración o de los particulares-, asuntos que por sus connotaciones y características interesan exclusivamente al ámbito de reserva del individuo.



8.2. Administración de datos personales relacionados con anotaciones, requerimientos, antecedentes y procesos judiciales o administrativos ²²

Anotaciones o registros penales en base de datos

[T-398/23](#): el derecho al olvido que se protege ampliamente respecto de los incumplimientos de obligaciones financieras debe predicarse con mayor razón respecto de las anotaciones judiciales que se formulen en los procesos penales que no alcanzan a constituir antecedentes penales y que cumplen una función instrumental al proceso. Como se ha dicho, tales anotaciones constituyen un dato negativo en tanto vinculan a un sujeto como un posible infractor del pacto social de la forma más grave posible, que es la violación a la ley penal. Más grave aún puede resultar este último caso en el que, dado que el proceso penal no está llamado a concluir, el sujeto no podrá esperar a su favor una sentencia absolutoria que lo posicione nuevamente ante la sociedad como un no infractor de la ley penal.

[T-125/25](#): la conservación de la información en las bases de datos internas de la Fiscalía puede prolongarse mientras que no involucre la información personal. Lo anterior significa que los datos que deben mantenerse son aquellos que resulten relevantes para la elaboración de estadísticas, lo que excluye, por supuesto, la identidad.

²² Al respecto se pueden consultar también las siguientes sentencias: T-120 de 1998, T-058 de 2015, T-036 de 2016, T-995 de 2012, T-648 de 2012, SU-458 de 2012, T-058 de 2015, T-509 de 2020 y T-203 de 2025.



Consulta, acceso y divulgación de antecedentes penales

T-512/16: existen fines constitucionales legítimos que impiden que el antecedente penal pueda eliminarse, como si el mismo nunca hubiera existido. Si bien la supresión como el no almacenamiento ni circulación de datos personales es posible en materia de obligaciones de carácter crediticio, lo mismo no se predica para asuntos penales, ya que no son equiparables.

SU-139/21: las autoridades no pueden limitar al titular del dato ni a los terceros legitimados para ello el acceso al mismo, en especial cuando se trata de una información de contenido negativo, como es el caso de los antecedentes penales y los requerimientos judiciales, toda vez que ello contraviene los principios de acceso, libertad, transparencia y veracidad que gobiernan la administración de los datos personales.

Rectificación y actualización de información sobre órdenes de captura

T-310/03: cuando la autoridad judicial no comunica la cancelación de una orden de captura o la autoridad encargada de cancelar ese registro no lo hace, la persona afectada en su derecho fundamental puede conocer, solicitar la rectificación y actualizar dicha información en desarrollo al derecho fundamental al habeas data y a fin de impedir una amenaza a su derecho fundamental a la libertad. En materia penal, el dato sobre la cancelación de una orden de captura debe desaparecer tan pronto la autoridad judicial competente así lo haya ordenado o haya certificado que ha operado la prescripción.

T-531/16: las autoridades judiciales tienen el deber de llevar un registro actualizado en el que aparezcan las órdenes de captura, así como la



	información sobre su cancelación, lo anterior, por cuanto constituye una de las formas de garantizar el ejercicio del derecho al <i>habeas data</i> .
Información contenida en sentencias o expedientes judiciales disponibles en páginas web	<u>T-020/14</u>: aun cuando se entiende que las sentencias son públicas, y así deben seguir siéndolo, la información personal contenida en ellas está sometida a los principios de la administración de datos, por lo que eventualmente pueden incluir datos sensibles o semiprivados, en cuya circulación y acceso deben cumplirse los principios de finalidad, necesidad y circulación restringida que rigen el derecho al <i>habeas data</i>. <u>SU-355/22</u>: el Consejo Superior de la Judicatura deberá especificar los lineamientos para garantizar que con las publicaciones que realizan tanto el administrador principal como los administradores secundarios en el portal web de la Rama Judicial no se vulnere el derecho la intimidad personal y familiar de las personas.
Antecedentes disciplinarios	<u>T-212/16</u>: el registro de una sanción disciplinaria en un certificado sometido a circulación no puede permanecer indefinidamente, ello equivaldría a un reproche disciplinario permanente.

8.3. Administración de información relacionada con programas sociales del Estado e inscripciones a pruebas académicas

Actualización en la información del SISBEN	<u>T-476/10</u>: como quiera que el aludido sistema tiene por objeto focalizar el gasto social para que beneficie a la población más necesitada, y que de estar desactualizado contrariaría el derecho fundamental al <i>habeas data</i> de las personas, pues las bases de datos recogida para alcanzar el fin señalado no
--	--



	estarían actualizadas, la Corte ha insistido en la existencia de un derecho fundamental a solicitar la reclasificación y el consecuente deber – por parte del Estado – de determinar oportunamente si la persona corresponde o no a un nivel diferente en el SISBEN.
	<u>T-627/14</u>: las personas tienen derecho a que la información de las bases de datos con que cuenta el SISBEN sea actualizada, de acuerdo con el derecho fundamental al habeas data.
Administración de bases de datos sobre víctimas de desplazamiento forzado	<u>T-167/16</u>: cuando la inclusión de datos que puedan generar situaciones provechosas para el titular, como es la posibilidad de adquirir un subsidio de vivienda o ser acreedor de beneficios asistenciales de reparación y atención, la omisión de registrar información actual del titular conlleva a una negación injustificada de la incorporación del dato que reporta el beneficio, con lo cual se vulnera el derecho al habeas data. Teniendo en cuenta los principios de circulación restringida de datos y de libertad, es necesario que las entidades que administran la información tengan especial cuidado con la información sensible que incorporan y sólo la circulen entre las entidades públicas que tengan relación con las políticas de asistencia y reparación a las víctimas.
	<u>T-009/21</u>: la Corte ha señalado que, para las víctimas de desplazamiento forzado, el derecho al habeas data envuelve una dimensión positiva relativa al deber de las entidades correspondientes de esforzar-



se de manera razonable con el objetivo de superar la trabas que se prevean o detecten (...). También ha señalado que el derecho al habeas data, en relación con esta población, implica que las bases de datos (i) especifiquen su identidad clara, no sólo en el Registro Único de Población Desplazada (RUPD), sino en las demás bases de datos manejadas por entidades públicas con responsabilidades respecto de la protección de sus derechos; (ii) contengan los datos indispensables para que los servicios y beneficios a que tienen derecho sean efectivamente provistos, y estén debidamente focalizados a sus necesidades y capacidades, y (iii) sean accesibles a diferentes entidades y organismos responsables de la ejecución de programas dirigidos a la población desplazada.

En procura de cumplir con los anteriores parámetros, las normas que regulan las bases de datos con información sobre víctimas de desplazamiento forzado (...), deben ser interpretadas y aplicadas de conformidad con los principios de legalidad, buena fe, favorabilidad y pro homine.

Rectificación y actualización de información

T-413/24: para el manejo de las bases de datos que utiliza el Estado en el desarrollo de los programas de atención social, las autoridades encargadas tienen un deber reforzado de realizar un debido uso de la información. En esa medida, deben tramitar de manera oportuna los reclamos que los usuarios realicen para actualizar o corregir información, a efectos de que ello no constituya una barrera administrativa para la garantía de otros derechos fundamentales como el mínimo vital y la vida digna.



Obligación de suministrar información relacionada con los datos reportados en el proceso de inscripción a pruebas Saber 11.

T-039/19: obligación de suministrar a los estudiantes y a sus familias la información relacionada con los datos reportados en el proceso de inscripción adquiere una especial importancia, en atención a que: (i) son los titulares de los datos; (ii) los datos no son suministrados por ellos, sino por un tercero, respecto del cual los estudiantes se encuentran en situación de subordinación; y (iii) los datos reportados pueden incidir en las condiciones particulares de presentación del examen.

8.4. Administración de datos personales contenidos en historias clínicas²³

Deber de custodia y el cuidado de las historias clínicas

T-153/24: los prestadores de los servicios de salud deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo mediante la adopción de los lineamientos para la administración de la seguridad de la información y la seguridad digital. En cuanto a las medidas de seguridad relacionadas en la Ley 1581 de 2012, el principio de seguridad establece que la información sujeta a tratamiento por el encargado del tratamiento a que se refiere dicha ley se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, de tal forma que se evite su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento (literal g del artículo 4 de la Ley 1581 de 2012).

²³ Al respecto se pueden consultar también las siguientes sentencias: T-443 de 1994, T-275 de 2005, T-158A de 2008, T-505 de 2015, T-058 de 2018, T-265 de 2020, T-402 de 2024.



T-376/19: existe una relación directa entre el derecho a la salud y el derecho de habeas data, pues es con base a la información que allí reposa que es posible diagnosticar y formular los medicamentos y demás prestaciones requeridas por el paciente para sobre-llevar y/o superar su enfermedad.

Siendo el paciente dueño de la información que es consignada en la historia clínica y el hospital el custodio de la misma, no se encuentra ninguna justificación para que dichos datos estén visibles en una plataforma que tiene fines administrativos.

8.5. Derecho al habeas data financiero ²⁴

Reporte negativo ante operadores de información financiera o crediticia

T-360/22: los requisitos para que proceda el reporte de un dato desfavorable son los siguientes: por un lado, (i) la veracidad acerca de la existencia de una obligación crediticia y, por otro, (ii) la autorización previa, escrita y expresa del titular para que se reporte el dato negativo.

²⁴ Al respecto se pueden consultar también las siguientes sentencias: Otras sentencias: T-414 de 1992, T-486 de 1992, T-022 de 1993, T-110 de 1993, T-220 de 1993, T-296 de 1993, T-303 de 1993, T-354 de 1993, T-389 de 1993, SU-528 de 1993, T-164 de 1994, SU-082 de 1995, T-096A de 1995, T-097 de 1995, T-176 de 1995, T-189A de 1995, T-199 de 1995, T-580 de 1995, T-462 de 1997, T-303 de 1998, T-856 de 2000, T-527 de 2000, T-1085 de 2001 T-589 de 2002, T-814 de 2002, T-592 de 2003, T-060 de 2003, T-1154 de 2003, T-204 de 2004, T-487 de 2004, T-846 de 2004, T-018 de 2005, T-565 de 2005, T-657 de 2005, T-1319 de 2005, T-204 de 2006, T-684 de 2006, T-943 de 2006, T-067 de 2007, T-272 de 2007, T-798 de 2007, T-248 de 2008, T-547 de 2008, T-002 de 2009, T-421 de 2009, T-1061 de 2010, T-964 de 2010, T-164 de 2010, T-129 de 2010, T-847 de 2010, T-811 de 2010, T-803 de 2010, T-017 de 2011, T-658 de 2011, T-246 de 2014.



Inclusión de suspensión de los derechos políticos como información en base de datos financiera

T-167/15: no le es dable a un ente en el desarrollo de funciones de carácter público “estigmatizar” a aquellas personas a quienes, a pesar de presentar un buen comportamiento crediticio hayan sido condenadas por conductas consideradas punibles por la legislación colombiana, salvo cuando con ellas se afecten bienes jurídicos de carácter económico con las cuales pueda ponerse en peligro el patrimonio de una persona natural o jurídica.

Protección por parte de las autoridades que administran datos cuando se demuestre que ha acontecido una situación de suplantación de identidad

T-360/22: cuando las entidades bancarias, crediticias o financieras reciban una queja en la que se advierta que existe un posible caso de suplantación de identidad deben llevar a cabo una investigación interna, con la finalidad de establecer si los productos fueron adquiridos mediante fraude. El deber de llevar a cabo esta investigación se justifica en el principio de responsabilidad demostrada.

Permanencia de los reportes negativos y derecho al olvido

T-883/13: la permanencia del dato negativo más allá del término previsto en el ordenamiento jurídico para la prescripción de la obligación configuraría un ejercicio abusivo del poder informático, la Corte determinó que en esos casos también debía aplicarse el plazo de permanencia de cuatro años previsto por el legislador en el artículo 13 de la Ley 1266 de 2008, esta vez, contados a partir del momento en que la obligación deja de existir cualquiera sea la causa.

T-294/23: el derecho a la supresión o al olvido supone una extensión de los principios superiores de privacidad, autodeterminación y libertad. En consecuencia, la información de un sujeto no debe



	mantenerse a perpetuidad en una base datos, sin que medie, o la autorización del titular de los datos, o un mandato legal explícito.
Autorización para el reporte negativo en bases de datos	<u>SU-089/95</u>: la facultad de reportar a quienes incumplan las obligaciones por ellos contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues, al fin y al cabo, los datos que se van a suministrar conciernen a él y, por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar.
Soporte de la obligación reportada en base de datos	<u>T-419/13</u>: los principios de finalidad y veracidad de la administración de datos personales, llevados al caso del habeas data financiero, obligan a que las fuentes estén en capacidad de sustentar los reportes sobre comportamiento crediticio en obligaciones existentes y comprobables. Así mismo, en caso de que el reporte verse sobre el incumplimiento de dichas obligaciones, la fuente está obligada a demostrar la existencia de la mora respectiva como condición de validez del reporte. <u>T-168/10</u>: no basta con que las entidades que realicen el reporte tengan los registros contables que soporten la existencia de la obligación, sino que, además, como condición para hacer el reporte y como medio para hacer efectivo el derecho de las personas a conocer las circunstancias del mismo, deben contar con los documentos de soporte, en los que conste la respectiva obligación.



Tensión entre el derecho al habeas data financiero y el debido proceso

T-184/23: en el contexto de un proceso judicial o administrativo, el habeas data no puede prevalecer, ni usarse como justificación para negar el acceso total a piezas procesales contenidas en el expediente, pues ello, puede representar una conculcación del derecho fundamental al debido proceso. En concreto, porque elimina la posibilidad de que el respectivo sujeto procesal conozca la actuación y diseñe su estrategia de defensa.

8.6. Administración de datos contenidos en la historia laboral

Cambios en la historia laboral²⁵

T-379/17: las administradoras deben velar por la salvaguarda de la historia laboral colocando todas las herramientas tecnológicas, legales y humanas para garantizar que la información ahí plasmada corresponda con la realidad. En todo caso de inconsistencia, ésta deberá ser solucionada por la administradora, pues es la entidad quien cuenta con la custodia de la información, pero siempre atendiendo al deber de decidir de buena fe y con el respeto del debido proceso. En el mismo sentido, se advirtió que los afiliados de las administradoras pueden hacer ejercicio del derecho al habeas data y que, en esa medida, tiene la posibilidad de solicitar la corrección y actualización de la información que reposa en la historia laboral, pues en todo caso corresponde a sus datos personales.

²⁵ Al respecto se pueden consultar también las siguientes sentencias: T-264 de 2022, T-247 de 2021, T-470 de 2019, T-207A de 2018, T-058 de 2017, T-399 de 2016, T-463 de 2016, T-079 de 2016, T-398 de 2015, T-706 de 2014, T-926 de 2013, T-592 de 2013, T-144 de 2013.



	<u>SU-182/19</u>: hay una obligación, tanto en el empleador como en las administradoras de pensiones, de velar por la correcta custodia, almacenamiento y disposición de los medios documentales que contengan información relevante sobre la trayectoria laboral de una persona, sea en el sector público o privado.
Inconsistencias en el cómputo de semanas cotizadas ²⁶	<u>T-482/12</u>: las entidades públicas y privadas que administran las bases de datos contentivas de la historia laboral de los afiliados al sistema general de seguridad social, por manejar datos que tienen el carácter de personal, deben reportar información cierta, precisa, fidedigna y actualizada de los titulares del derecho, para no vulnerar el derecho al habeas data que les asiste a éstos y, de paso, afectar el goce efectivo de otros derechos de naturaleza constitucional.
Actualización de historia laboral	<u>T-013/20</u>: los deberes de las administradoras de pensiones implican que ellas están obligadas a responder por el tratamiento de la información pensional, así que no les es posible endilgar sus responsabilidades a los afiliados. El alcance de las reglas dispuestas en la ley y la jurisprudencia establece que son las entidades que construyen, guardan y vigilan las historias laborales, las llamadas a responder por los inconvenientes que puedan presentar los documentos y su información.

²⁶ Al respecto se pueden consultar también las siguientes sentencias: T-855 de 2011 y T-599 de 2007.



8.7. Uso de datos personales recopilados en el marco de medidas de protección

Uso de información personal recabada por los sistemas de monitoreo instalados en vehículo asignado a periodista	<u>T-294/23</u>: la UNP tiene vedado adelantar actividades de inteligencia a partir de la información personal que recaba para el ejercicio de las funciones de protección que la ley le confió. Ello, debido a que tales actividades no hacen parte de sus objetivos legales. Así adelantar acciones de esa naturaleza desconocería el carácter reservado que el ordenamiento jurídico impone a los datos personales acopiados y tratados para fines, se insiste exclusivos, de diseño y ejecución de las medidas de protección. La UNP debe conservar, en cumplimiento del mandato legal y constitucional de preservación de la información –estrictamente– aquellos datos necesarios para mantener un acervo cultural, histórico, estadístico o científico del ejercicio de sus funciones, así como aquellos datos indispensables para que la misma administración, la justicia, o los entes de control puedan ejercer sus deberes constitucionales de vigilancia y fiscalización respecto de la destinación y ejecución de recursos públicos.
---	---

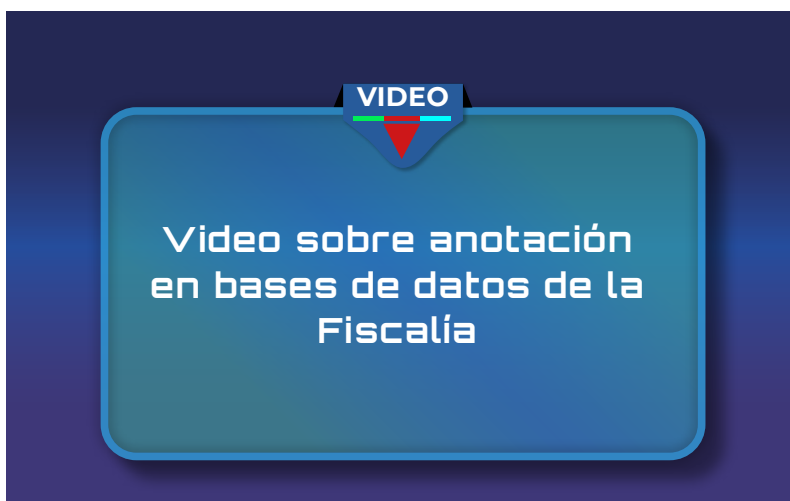
8.8. Bases de datos que solo contienen datos negativos

Registro de información desfavorable	<u>T-987/12</u>: es admisible que el prestador registre, si ha tenido la autorización previa, expresa e informado para ello, información personal del usuario que le conlleve consecuencias desfavorables y favorables. En este escenario se estaría ante una recopilación objetiva del dato personal. Contrario sucede cuando la
--------------------------------------	--



finalidad del registro es exclusivamente determinar la exclusión del sujeto concernido del acceso a determinado servicio público, puesto que en ese caso se está ante un ejercicio desproporcionado de la habilitación legal para la administración de datos personales.

Gráfica 22. *Elaboración propia con base en las providencias señaladas en la columna denominada “sentencia y consideración destacada”.*





DERECHOS en el escenario DIGITAL y de las TIC



9. DERECHO AL TRABAJO A TRAVÉS DEL USO DE MEDIOS TECNOLÓGICOS Y DIGITALES

“El derecho al trabajo es un pilar fundamental de nuestra sociedad, que abarca diferentes derechos de las personas para su desarrollo armónico. Además, tiene diferentes matices frente a su realización, como lo es el teletrabajo, lo cual va acorde con la integración social y pretende eliminar barreras de acceso de la población más vulnerable, con el objeto de que puedan tener un trabajo en condiciones dignas y alineado con sus condiciones particulares”

Sentencia T-233 de 2025



La Constitución Política consagra el trabajo como un fin en su preámbulo, un pilar fundamental del Estado según el artículo 1º y un derecho y una obligación social conforme al artículo 25. En ese contexto, las TIC han facilitado nuevas modalidades laborales que han trascendido la presencialidad y que permiten a los trabajadores desempeñar sus funciones desde diferentes lugares. Esta transformación tecnológica no solo ha redefinido las formas y espacios laborales, sino que ha hecho posible conciliar el trabajo con otros ámbitos de la vida de las personas. En consecuencia, se ha fortalecido la protección frente a derechos como la salud, la unidad familiar y la integridad personal, a partir de un enfoque laboral más inclusivo.



Sentencia **T-233 de 2025**

El teletrabajo no solo responde a transformaciones tecnológicas o a necesidades de eficiencia administrativa, sino que se inscribe en una evolución del derecho al trabajo hacia formas más inclusivas, flexibles y adaptadas a las condiciones reales de los trabajadores. En ese marco, el teletrabajo ha sido concebido como una herramienta que puede facilitar el acceso, la permanencia y el ejercicio del trabajo en condiciones dignas, especialmente para personas en situación de vulnerabilidad.

A continuación, se muestran algunas modalidades de trabajo facilitadas por el uso de las tecnologías de la información y las comunicaciones.



DERECHOS en el escenario DIGITAL y de las TIC



Modalidad	Naturaleza jurídica	Tipo de tecnologías utilizadas
Trabajo en casa	<i>Habilitación temporal de carácter legal</i> para desempeñar las funciones o actividades laborales por fuera del sitio donde habitualmente se efectúan, primordialmente desde la casa o domicilio del trabajador, sin variar las condiciones pactadas o establecidas al inicio de la relación laboral.	(i) Las TIC o también denominadas Tecnologías de la información y las comunicaciones o cualquier medio análogo. (ii) Se puede extender a cualquier trabajo que no requiera la presencia física del trabajador en las instalaciones de la empresa o entidad.
Trabajo a domicilio	<i>Habilitación permanente de origen contractual</i> para que el trabajador, solo o con la ayuda de su familia, preste sus servicios habitualmente desde su propio domicilio.	Ninguna en particular, sin perjuicio de que suele utilizarse para efectuar esquemas de trabajo por unidades de obra (como ocurre, por ejemplo, con los textiles, la zapatería o las artes gráficas).
Teletrabajo	<i>Forma de organización laboral de origen contractual</i> que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros, utilizando como soporte las TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.	Solo aquel que pueda ser prestado mediante las TIC.



DERECHOS en el escenario DIGITAL y de las TIC



Trabajo remoto

Forma de ejecución del contrato de trabajo de origen contractual, en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de las TIC u otro medio o mecanismo, donde el empleador y trabajador no interactúan físicamente a lo largo de la vinculación contractual.

Tecnologías existentes o nuevas, entendidas estas como cualquier medio, plataforma, software, programa, equipo, dispositivo y/o equipo que permita la comunicación, interacción y/o ejecución del contrato de trabajo de manera remota mediante una conexión a Internet o a cualquier otra red que permita ejecutar dichas acciones.

Gráfica 23. Elaboración propia con base en las sentencias C-212 de 2022 y T-099 de 2024.

En la siguiente tabla se mencionan algunas sentencias en las que la Corte se ha pronunciado sobre la constitucionalidad de normas relacionadas con estas modalidades laborales. Se destacan algunos pronunciamientos en los que la Corte ha sentado precedentes de tratamiento igualitario a los trabajadores que usan estas tecnologías.

Sentencias de constitucionalidad sobre la implementación de las TIC en el ámbito laboral

Sentencia	Asunto
Teletrabajo	
<u>C-337/11</u>	La Corte declaró exequible de manera condicionada el artículo de la Ley 1221 de 2008 ²⁷ el cual omitía a los teletrabajadores como beneficiarios del subsidio familiar. La Corte señaló que, en efecto, existió una omi-

²⁷ Ley 1221 de 2008 “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.” Art. 6 Numeral 6 C.



	sión legislativa relativa y, por ende, era válida la aplicación de esta disposición siempre y cuando se entienda que la protección en materia de seguridad social incluye a los teletrabajadores. Argumentó que, los trabajadores convencionales como los teletrabajadores realizan un trabajo subordinado, y, al encontrarse en igual condición, debe reconocérseles iguales derechos, sin que pueda considerarse que la forma de prestación incida en el reconocimiento de sus garantías.
<u>C-103/21</u>	La Corte declaró exequible la disposición de la Ley 1221 de 2008 que excluyó a los teletrabajadores de las disposiciones sobre jornada laboral, horas extra y trabajo nocturno. La Sala Plena estableció que esta norma no implica un aumento de la jornada laboral semanal definida en la ley ni desmejora los derechos sociales de los trabajadores, pues la jornada máxima permanece igual. Mencionó que este modelo es de doble beneficio, pues mientras el empleador accede a los frutos o réditos de la labor ejecutada, el trabajador dispone y maneja su tiempo y con ello goza de los espacios necesarios para atender su situación personal.

Trabajo en casa

<u>C-242/20</u>	La Corte declaró exequible el artículo que permitió la prestación de los servicios a cargo de las autoridades mediante la modalidad de trabajo en casa ocasionado por la Pandemia del Covid-19. Señaló que, la habilitación de trabajo en casa lleva implícito para las autoridades el deber de garantizar el acceso a la administración pública de los usuarios, incluso cuando la totalidad de las actuaciones se desarrollen por medio de las tecnologías.
---------------------------------	--



C-212/22

La Corte declaró exequible la ley que regula el trabajo en casa. Señaló que esta ley no regula de forma integral, estructural ni completa el derecho al trabajo, sino que otorga al legislador una habilitación permanente para que, en circunstancias excepcionales que impidan desempeñar las funciones en el lugar de trabajo, los empleados del sector público o privado puedan realizar sus labores desde su casa. Esta modalidad puede acordarse mutuamente o derivarse de la autoridad del empleador, sin modificar las condiciones laborales establecidas.

Trabajo remoto

C-400/24

La Corte declaró inexecutable la expresión “en primer grado de consanguinidad” utilizada en la ley de trabajo remoto que permite a los trabajadores que hacen uso de esta modalidad tener flexibilidad en sus horarios, para realizar tareas de cuidado, únicamente cuando las personas a su cargo se encuentren dentro del primer grado de consanguinidad. La Corte resaltó que el trabajo remoto responde a la necesidad de adaptar la virtualidad a las actividades productivas creando una conciliación de la vida familiar con el trabajo, por lo que las responsabilidades familiares de los trabajadores remotos no se predicen únicamente de aquellos sujetos de especial protección a su cargo con quienes comparten parentesco en primer grado de consanguinidad, sino de todos los familiares que, encontrándose en tales supuestos, implican la realización de las labores de cuidado.



Auxilio de conectividad

C-311/20

La Corte declaró exequible el decreto que, debido a la pandemia por Covid-19, destinó el auxilio de transporte como auxilio de conectividad para garantizar el acceso a los servicios tecnológicos. Señaló que, aunque los trabajadores realizan un traslado físico a sus lugares de trabajo, desempeñan sus actividades laborales de forma virtual. Este desempeño genera un costo de conectividad que el trabajador no está obligado a asumir.

Gráfica 24. Elaboración propia en base a las sentencias de constitucionalidad referidas en la columna denominada “sentencias”.

En materia de tutela, la Corte ha revisado diversos temas que se relacionan con el uso de las tecnologías para proteger diferentes derechos.

9.1. Teletrabajo como medida de inclusión laboral a personas con afectaciones de salud

En la sentencia T-254 de 2016, la Corte amparó los derechos de un ciudadano con lesión medular, desprendimiento de retina y desplazamiento del cóccix, a quien se le negó una solicitud de teletrabajo por su condición de salud. Señaló este tribunal que el teletrabajo facilita la inclusión laboral de personas en situación de discapacidad al flexibilizar las relaciones laborales mediante el uso de la tecnología. Así mismo, mencionó que cuando las funciones son intelectuales y no se requiere presencia física estas se pueden realizar en otro lugar por medio de la tecnología.



Sentencia *T-254 de 2016*

En casos en los que la discapacidad de un trabajador le genere barreras relacionadas con la movilización hasta el lugar de trabajo o su acceso al puesto destinado para tal fin, el empleador se encuentra en la obligación de otorgar el beneficio del teletrabajo, siempre que corresponda a una solicitud expresa del empleado o que sea el propio el empleador quien lo proponga, como una medida para mejorar no solo el servicio, sino también para realizar los ajustes razonables que permitan la realización plena del derecho al trabajo y al empleo.

Por su parte, en la sentencia [T-099 de 2024](#), la Corte amparó los derechos de un hombre, el cual se encontraba en situación de debilidad manifiesta por su condición de salud y la entidad accionada se negó otorgar la opción de teletrabajo por encontrarse en un cargo de libre nombramiento y remoción. Esta Corporación señaló que el teletrabajo se enmarca en una política pública que debe formularse para la incorporación de la población vulnerable y es por el uso de la tecnología que se puede garantizar el derecho al trabajo aun cuando existen afecciones por salud.

VIDEO

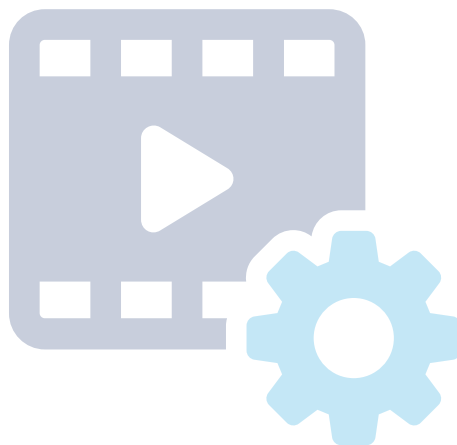
Video relacionado con el teletrabajo y la inclusión laboral de persona en situación de debilidad manifiesta



9.2. Teletrabajo como opción de protección a la unidad familiar

En la sentencia [T-233 de 2025](#), la Corte protegió los derechos de un servidor público de la Procuraduría General de la Nación, miembro de una comunidad indígena y víctima de desplazamiento forzado, quien solicitó traslado y teletrabajo para residir con su familia, pero la entidad negó ambas solicitudes sin tener en cuenta sus condiciones personales y la de los miembros de su núcleo familiar.

Al respecto, la Corte señaló que para implementar el teletrabajo en el sector público y en particular respecto de servidores de carrera, se debe considerar no solo los criterios de conveniencia institucional, sino también los principios constitucionales de igualdad material, dignidad humana y protección reforzada de ciertos sectores de la población, todo ello con miras a garantizar relaciones laborales justas y el efectivo goce de los derechos fundamentales asociados al trabajo. En consecuencia, amparó los derechos y ordenó el beneficio del teletrabajo.





Sentencia *T-233 de 2025*

El teletrabajo no puede entenderse, de ninguna manera, como una modalidad que exonere al trabajador de sus responsabilidades ni que implique una disminución en la exigibilidad de sus funciones. Por el contrario, se trata de una forma de organización del trabajo que debe garantizar los mismos niveles de compromiso, calidad y cumplimiento de objetivos, bajo esquemas adecuados de control, seguimiento y evaluación. Sólo así se ha considerado que el teletrabajo, en sus distintas modalidades, constituye una alternativa legítima para asegurar condiciones laborales dignas y compatibles con realidades personales o familiares complejas, sin que ello implique alterar el principio de eficiencia en el ejercicio de la función pública.

Un caso similar fue estudiado en la sentencia [T-265 de 2024](#).

9.3. Trabajo en casa como medida de protección a las víctimas del desplazamiento forzado

En la sentencia [T-486 de 2023](#), la Corte protegió los derechos de una servidora pública de carrera, madre cabeza de familia, víctima de amenazas y de desplazamiento forzado, quien solicitó a la entidad para la cual trabajaba un traslado o trabajo en casa. La Corte destacó que, en situaciones ocasionales, excepcionales o especiales, es posible modificar las condiciones iniciales del contrato para desempeñar funciones fuera del lugar del trabajo. Por ello, determinó que la actora, debido a las amenazas recibidas, puede trabajar desde un lugar distinto al asignado, sin que le desmejoren las condiciones ni la carga laboral, hasta que se le brinde respuesta a su solicitud de traslado.



Un caso similar se estudió en la sentencia [T-354 de 2024](#).

9.4. Trabajo sexual por medio de plataformas digitales (modelaje webcam)

En la sentencia [T-109 de 2021](#), la Corte conoció el caso de una mujer en estado de gestación que fue despedida del estudio webcam en donde laboraba. Pese a tratarse de un asunto cuya competencia le correspondería en un inicio a otro juez, la Sala estimó que sería desproporcionado imponerle la carga de iniciar un nuevo proceso judicial para que se determine si se configuró un contrato realidad; máxime si, como se señaló en el análisis de procedencia, las características atípicas del caso y la falta de una regulación específica podrían exceder los márgenes formales de un proceso ordinario.

En ese sentido, la Corte verificó el cumplimiento de cada uno de los requisitos para la existencia de un contrato realidad y halló configurada una verdadera relación laboral. Lo anterior sumado a que el empleador conocía sobre el estado de embarazo de la accionante durante la vigencia de la relación laboral, llevó al tribunal a concluir que la desvinculación se produjo mientras era titular del derecho a la estabilidad laboral reforzada. Respecto a este tipo de vinculaciones la Corte destacó que:



Sentencia T-109 de 2021

Más allá de las estipulaciones y la apariencia formal de los contratos celebrados entre empresarios y modelos webcam, por mandato constitucional derivado del artículo 53 superior -que consagra el principio de primacía de la realidad sobre formalidades establecidas por los sujetos de las relaciones laborales-, es menester verificar en cada caso concreto si, a partir de la manera en que se desarrolla en la práctica la actividad, es posible encontrar reunidos los elementos que caracterizan una relación laboral, esto es, si se presentan (i) la prestación personal del servicio por cuenta ajena, (ii) la subordinación, y (iii) la remuneración, de acuerdo con el artículo 22 del Código Sustantivo del Trabajo, pues, de ser así, habrá lugar a reconocer judicialmente la existencia de un contrato de trabajo soterrado, con los consecuentes derechos y deberes inherentes de esta relación.

Esta corporación señaló que, si bien el uso de nuevas tecnologías ha incrementado la industria del entretenimiento para adultos, incluido el modelo webcam, esta actividad debe analizarse teniendo en cuenta el contexto de muchas mujeres vulnerables que se dedican a esta actividad.



Sentencia *T-109 de 2021*

La industria del sexo, asentada de por sí sobre una cultura ligada a una particular visión sobre las mujeres y sus cuerpos, con la feminización de la pobreza, la precarización y con las dinámicas de explosión del consumo, apertura económica, desregulación, digitalización y repunte de las tecnologías informáticas e internet -distintivas de la globalización-, encuentra en el cibersexo posibilidades de expansión y el nicho propicio para ensancharse y obtener una nueva fuente de lucro, a expensas del sacrificio de algunas mujeres que ingresan al negocio como una opción de supervivencia, o como una salida para lograr independencia económica y mejorar su nivel de vida.

De acuerdo con este panorama, la Corte amparó los derechos de la mujer, declaró la existencia de un contrato de trabajo y la garantía de todos los derechos derivados de este reconocimiento. En este caso puntual, y teniendo en cuenta que la accionante se dedicaba al modelaje webcam ante la imposibilidad de acceder a otras formas de empleo, no se ordenó el reintegro sino un acompañamiento para que la accionante pueda optar por otras fuentes de trabajo. Por último, la Corte exhortó al Congreso de la República y al Ministerio del Trabajo para que regule la actividad del modelaje webcam.

9.5. Protección constitucional de las actividades desarrolladas por los y las influenciadoras digitales

La sentencia [T-256 de 2025](#) también se refirió a la protección de la actividad de los influenciadores digitales como personas que generan contenido para plataformas digitales lo que, a su vez, les permite alcanzar notoriedad y generar



ingresos económicos que pueden constituir todo o parte de su sustento vital. De esta forma, la Corte reconoció este oficio como una actividad propia del mundo digital que ha ganado relevancia gracias al crecimiento de las redes sociales y que tiene diversas modalidades como fuentes de ingresos monetarios, entre ellas las siguientes:

Contratos de publicidad con marcas y agencias cazatalentos en las que se acuerda la promoción de bienes o servicios específicos.

Monetización directa de cuentas frente a las plataformas mediante la entrega de dinero por autorizar la presentación de pauta publicitaria a los seguidores de la cuenta.

Ingresos directos por aportes de seguidores a través de estrategias de *crowdfunding* o recolección de dinero para un fin particular.

Venta directa de bienes y servicios producidos por el o la influenciadora.

Gráfica 25. *Elaboración propia con base en la sentencia T-256 de 2025.*

Este Tribunal refirió que la actividad de influenciador(a) puede ser catalogado como trabajo, si se tiene en cuenta la definición de la OIT²⁸, pues permite la circulación de bienes y servicios, al tiempo que proporciona medios de sustento a quien lo ejerce. De igual manera, se trata de una actividad que desarrolla otros derechos, como la libertad de expresión y la libertad de escoger profesión y oficio. Por todo ello, es una actividad que goza de protección constitucional. Sin

²⁸ Organización Internacional del Trabajo, Centro Interamericano para el Desarrollo del Conocimiento en la Formación Profesional (OIT/CINTERFOR). “Trabajo”. Texto citado en la sentencia T-256 de 2025. M.P. Natalia Ángel Cabo.



embargo, se destacó que las particularidades de este oficio suponen desafíos jurídicos que las categorías tradicionales del derecho no logran resolver con facilidad. De esa manera le corresponde al juez, en cada caso concreto, determinar si se trata de un trabajo independiente o existe subordinación laboral, para lo cual deberá considerar: (i) si la plataforma dicta reglas estrictas de comportamiento, (ii) si existe una dependencia económica o exclusiva con la plataforma, y (iii) si existe poder de dirección (órdenes, horarios y sanciones).

En caso de que se presenten estos elementos, se puede entender que existe subordinación y, por lo tanto, una relación laboral. Por el contrario, si se evidencia que el influenciador actúa de manera autónoma, se debe reconocer que se trata de un trabajo independiente. Conforme a lo expuesto, enfatizó que resulta necesario garantizar las protecciones mínimas relativas al derecho al trabajo.

Así mismo, este Tribunal resaltó la interdependencia estructural que existe entre los influenciadores y las plataformas digitales. Por un lado, los influenciadores dependen de las redes sociales para desplegar su modelo de negocio; por el otro, las plataformas requieren del contenido generado por estos actores para atraer usuarios. En este sentido, ninguna de las partes podría sostenerse sin la otra.

No obstante, la Corte enfatizó que, si bien las plataformas digitales operan como empresas privadas con autonomía para establecer sus reglas internas, a su vez, funcionan como espacios públicos, en donde los influenciadores comparten su contenido. Por ello, resulta necesario equilibrar esa autonomía con la protección de los derechos de los influenciadores, en donde el Estado debe proteger a la parte vulnerable, ya que las decisiones de dichas plataformas pueden generar la vulneración de otros derechos.



Sentencia T-256 de 2025

Ser influenciador en redes sociales es un oficio de creciente trascendencia y que, por lo mismo, siempre que no desconozca los límites propios del Estado social de derecho y los derechos fundamentales, goza de la protección constitucional a la que se refieren los artículos 25 y 26 de la Constitución Política. En otras palabras, los influenciadores digitales pueden ser considerados como trabajadores independientes que desarrollan un oficio en principio protegido por la Constitución. En tal sentido, frente al uso potencialmente arbitrario de la facultad amplia de moderación de contenidos y en virtud de la relación negocial desigual en la que se encuentran respecto de los operadores de las plataformas, pueden buscar la protección de los derechos señalados por vía de la acción de tutela.

Frente a este tema, en las órdenes dadas en la sentencia, la Corte instó al Ministerio del Trabajo, a la Superintendencia de Industria y Comercio y al Ministerio de Tecnologías de la Información y las Comunicaciones para que avancen en regulaciones sobre la actividad de influenciadores en redes sociales, en las que se definan claramente sus derechos y deberes frente a las audiencias, así como las reglas de su relación con las plataformas digitales.



DERECHOS en el escenario DIGITAL y de las TIC



10. DERECHO A LA PERSONALIDAD JURÍDICA Y A LA IDENTIFICACIÓN A TRAVÉS DE DOCUMENTOS DIGITALES

“Todo ciudadano colombiano pueda acceder a su registro civil de nacimiento y cédula de ciudadanía correspondiente, física o digital para que pueda hacer ejercicio efectivo de sus derechos civiles y políticos, y contraer obligaciones.”.

Sentencia T-527 de 2024



La jurisprudencia constitucional ha referido que el derecho a la personalidad jurídica es un derecho fundamental esencial para la consagración y efectividad del sistema de derechos y garantías contemplado en la Constitución, por lo cual, su materialidad conlleva a los atributos propios de la persona humana, y es propio de los sujetos de derechos en el ordenamiento jurídico constitucional.



Sentencia T-363 de 2016

La personalidad jurídica comprende todos aquellos elementos que distinguen a los sujetos y que demarcan su individualidad. Por lo tanto, el reconocimiento de ese derecho, como garantía superior, implica, a su vez, el reconocimiento y la protección de los atributos mismos de la personalidad

A continuación, se presentan algunos pronunciamientos en los que la Corte ha protegido este derecho en el marco de uso de herramientas digitales.

10.1. Identidad de género en la cédula digital

En la sentencia [T-527 de 2024](#), la Corte amparó los derechos de una persona reconocida como no binaria a la cual la Registraduría le negó la expedición de la cédula digital con el marcador de sexo “No Binario”. Al respecto, la Corte señaló que dicha conducta transgredió los derechos de la persona accionante y en consecuencia se ordenó implementar el marcador no binario para cédula digital. Además, se ordenó a la Registraduría y al DNP implementar la actualización informática necesaria para contar con un sistema que le garantice a las personas de género “No Binario” la expedición de su cédula de ciudadanía en formato digital con el marcador de sexo previamente señalado.



En este pronunciamiento, la Corte destacó que el derecho a la personalidad jurídica y a la identidad también se protegen en el escenario digital y que lo fundamental es garantizar que todo ciudadano colombiano pueda acceder a su cédula de ciudadanía correspondiente, física o digital para que pueda hacer ejercicio efectivo de sus derechos civiles y políticos. Además, señaló que la única diferencia es que la cédula de ciudadanía digital adquiere relevancia en el ámbito del tráfico jurídico digital, en tanto que los ciudadanos pueden gozar de seguridad informática al utilizar este tipo de herramienta.



Sentencia **T-527 de 2024**

El ordenamiento jurídico no distingue diferencias materiales y prácticas entre la cédula de ciudadanía de hologramas amarilla y la cédula de ciudadanía digital para efectos del acceso real a la prestación de servicios que tendría una persona que presentara una u otra para identificarse.

10.2. Garantías para el uso de la firma digital

La firma digital se encuentra definida en el literal c) del artículo 2° de la Ley 527 de 1999 y reglamentada en el Decreto 1747 de 2000 y ha sido considerada como una especie de la firma electrónica. En ese contexto, la firma digital se entiende como “(...) un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido vinculado a la clave criptográfica privada del iniciador, permite determinar que este valor numérico se ha obtenido exclusivamente con la clave criptográfica privada del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación²⁹ .

²⁹ Ley 527 de 1999. Art.2 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.”



En la sentencia [C-242 de 2020](#), respecto a la utilización de la firma digital, la Corte recordó lo siguiente:



Sentencia **C-242 de 2020**

La utilización válida de la firma digital está supeditada a la creación previa de un par de códigos matemáticos por parte de una entidad de certificación, la cual, mediante el uso de técnicas de criptografía, suministra al usuario una contraseña secreta indispensable para la suscripción virtual de los documentos, y una clave pública que permite la verificación de la autenticidad del mismo por parte de los interesados.

Por su parte, en la sentencia [C-662 de 2000](#), la Corte declaró exequibles algunas disposiciones de la ley 527 de 1999. En este fallo, se destacó que a través de la firma digital se pretende garantizar que un mensaje de datos determinado proceda de una persona determinada; que ese mensaje no hubiera sido modificado desde su creación y transmisión y que el receptor no pudiera modificar el mensaje recibido.

Asimismo, señaló que esta firma debe cumplir con idénticas funciones que una firma plasmada en papel. De esta forma, la firma digital permite:



DERECHOS en el escenario DIGITAL y de las TIC



	Identificar a una persona como el autor.
	Dar certeza de la participación exclusiva de esa persona en el acto de firmar.
	Asociar a esa persona con el contenido del documento.

Gráfica 26. *Elaboración propia con base en la sentencia C-662 de 2000.*

Por otra parte, la Corte se pronunció sobre el papel de las entidades de certificación como encargadas de validar la integridad de las firmas digitales. Respecto a estas entidades manifestó que:



Sentencia C-662 de 2000

Aunque su carácter eminentemente técnico no se discute, comoquiera que se desprende inequívocamente del componente tecnológico que es característico de los datos electrónicos, lo cierto es que participa de un importante componente de la tradicional función fedante, pues al igual que ella, involucra la protección a la confianza que la comunidad deposita en el empleo de los medios electrónicos de comunicación así como en su valor probatorio, que es lo realmente relevante para el derecho, pues, ciertamente es el marco jurídico el que crea el elemento de confianza.



Sobre este mismo punto, en la sentencia [C-219 de 2015](#), la Corte declaró exequibles algunas disposiciones del Decreto Ley 019 de 2012. En uno de los cargos de la demanda, se reprochó el hecho de que este Decreto haya modificado la autorización previa de la Superintendencia de Industria y Comercio a las actividades de las entidades de certificación, por la acreditación del ONAC como ente privado. Al respecto, la Corte advirtió que los requisitos de la autorización y de la acreditación son similares y que, en efecto, no se creó un nuevo procedimiento para avalar su existencia de estas entidades ni se agravó el existente. En esta oportunidad, se recordó que estas entidades de certificación prestan un servicio público y tienen como fin proporcionar seguridad jurídica a las relaciones comerciales por vía informática.



Sentencia **C-219 de 2015**

Los deberes de las entidades de certificación (...) se refieren a garantizar condiciones de confidencialidad y de seguridad para la creación de firmas digitales y la conservación de la información y de los certificados, la obligación de prestar oportunamente los servicios, de proporcionar información requerida por entidades administrativas o judiciales competentes, realizar publicaciones, permitir la realización de auditorías por parte del ONAC y llevar un registro de los certificados.



10.3. Protección de datos e implementación de sistemas de identificación biométrica

Según lo señalado, entre otras, en las sentencias [C-748 de 2011](#) y [T-561 de 2023](#), los datos biométricos son datos sensibles intrínsecamente ligados a la identidad y la intimidad de las personas que permiten identificarlas, ya sea a través de su huella, un video o, incluso, el iris de sus ojos.



Sentencia *T-561 de 2023*

Frente a los datos biométricos (incluidos como datos sensibles), la Superintendencia de industria y Comercio ha señalado que aquellos incluyen información sobre “características físicas” (rostro; huella dactilar; palma de la mano; retina y ADN) y “comportamentales” (forma de firmar, o tono de voz) sobre las personas.

En este mismo pronunciamiento se precisó que la imagen de una persona puede en algunos casos constituir un dato biométrico (v.gr., cuando contiene huellas dactilares) y, por lo tanto, constituir un dato sensible.

En materia electoral, en la sentencia [C-490 de 2011](#), se declaró exequible la disposición que introdujo la posibilidad de implementar el voto electrónico y con ello la identificación biométrica de los electores. Al respecto, la Corte señaló que es razonable la introducción de nuevos medios para agilizar y dar transparencia en todas las votaciones. Así mismo, recalcó que es posible que se adopten mecanismos electrónicos para ejercer el derecho al voto siempre que estén orientados a la realización plena del derecho al sufragio.



Sentencia *C-490 de 2011*

El mandato de implementación de sistemas de identificación biométrica, dirigido a la autoridad electoral tampoco contraviene la Constitución, toda vez que se orienta a fortalecer el procedimiento electoral mediante la introducción de mecanismos que permitan mayor seguridad y fiabilidad en los sistemas de identificación de los electores, y a rodear de mayor transparencia y eficacia los procesos de votación y escrutinio. Se trata de una estrategia operativa que en abstracto no ofrece reparos de constitucionalidad, pero que en su configuración, implementación y aplicación exige la preservación de la dignidad, la autonomía y la libertad del elector.

De igual forma, este tipo de sistemas de identificación se han utilizado en el caso de las personas migrantes que pretenden adelantar algún trámite de regularización. Por ejemplo, para acceder al Permiso por Protección Temporal-PPT- es necesario realizar el registro biométrico presencial. En las sentencias [T-100 de 2023](#), [T-552 de 2023](#), [T-078 de 2024](#) y [T-143 de 2024](#), la Corte ha estudiado casos relacionados con el cumplimiento de este requisito.



DERECHOS en el escenario DIGITAL y de las TIC



11. PROTECCIÓN CONSTITUCIONAL FRENTE A RIESGOS ASOCIADOS A LA INTERACCIÓN EN EL ESCENARIO DIGITAL

“La mayor exposición que proporcionan las redes sociales es una fuente de amenaza para los derechos fundamentales, por cuanto poseen herramientas incontrolables de procesamiento y permiten un uso ilimitado de la información depositada por los usuarios”

Sentencia T-145 de 2016



11.1. Violencia digital o violencia en línea

De acuerdo con lo mencionado en la jurisprudencia, entre las formas de violencia digital están los discursos que incitan al odio; las formas de deslegitimación que hacen referencia al cuerpo, conocimientos, habilidades o experiencia; las amenazas contra la integridad física haciendo uso de plataformas digitales; el uso de redes sociales para rastrear o vigilar con el fin de intimidar; la extracción de datos; la distribución no consensuada de imágenes íntimas; el acoso; el bullying y el “troleo”. Tal como se ha reconocido en las sentencias [T-064 de 2023](#), [T-087 de 2023](#), [T-280 de 2022](#), [T-206 de 2024](#) y [T-149 de 2025](#), entre otras, estas formas de violencia afectan de manera diferenciada y muchas veces desproporcionada a las mujeres, por ello se ha acuñado el concepto de violencia digital de género.



Sentencia *T-280 de 2022*

La violencia de género digital está constituida por todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico³⁰.

De este pronunciamiento se destaca también el exhorto realizado al Congreso de la República para que cumpla con las recomendaciones formuladas por

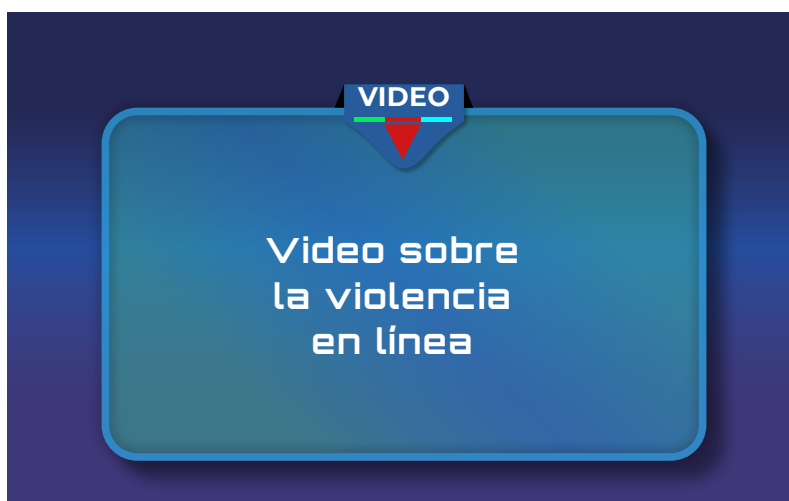
³⁰ Texto citado en la sentencia T-280 de 2022 MP. José Fernando Reyes Cuartas. ONU. Consejo de Derechos Humanos. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. (2018) A/HRC/38/47, párr. 23.



el Consejo de Derechos Humanos de la ONU y por la OEA en relación con la prevención, protección, reparación, prohibición y penalización de la violencia de género digital según lo establecido en la parte considerativa de esta sentencia.

Por su parte, en la sentencia [T-087 de 2023](#), la Corte amparó los derechos de varias mujeres periodistas que argumentaron haber sido víctimas de diferentes ataques en línea a través de la red social Twitter. Esta providencia señaló que la violencia por razón de género cometida contra las mujeres a través del uso de las tecnologías es un tipo de agresión que las afecta de manera desproporcionada y que se ha exacerbado porque puede incluso incitar a otros tipos de violencia o amenazas en su contra.

En esta oportunidad, la Corte reiteró el exhorto de la sentencia [T-280 de 2022](#) y, además, formuló uno nuevo dirigido a todos los partidos y movimientos políticos para que adopten en los Códigos de Ética directrices para sancionar los hechos de violencia o de incitación a la violencia en línea; e implementen una ruta de acceso para las mujeres víctimas de cualquier tipo de violencia, que facilite poner en conocimiento este tipo de conductas, a través de mecanismos expeditos, canales web o las herramientas que se estimen pertinentes para asegurar la investigación y la sanción, de ser el caso, de los hechos vulnerados.





A su turno, en la sentencia [T-206 de 2024](#) se estudió un caso en el que una inspección de policía adelantó un proceso verbal abreviado para resolver una controversia relacionada con la posible afectación generada por un periodista al realizar publicaciones ofensivas sobre un grupo de funcionarios(as) públicos. Como resultado de este proceso, la inspectora de policía impuso “requerimientos” contra el accionante, tales como, abstenerse de publicar cualquier escrito relacionado con las personas convocantes y eliminar de sus redes sociales todos los escritos en los que hiciera referencia a estas personas.

A juicio de la Corte, si bien se advirtió la vulneración de los derechos al debido proceso administrativo y a la libertad de expresión del actor al imponer medidas restrictivas, también se identificaron conductas que afectaron el derecho a una vida libre de violencia en el entorno digital de las funcionarias públicas sobre las cuales se realizó las publicaciones, a saber: (i) el accionante publicó “expresiones denigrantes contra la mujer”, siendo este tipo de manifestaciones una forma de violencia que “escapa de la órbita de protección del derecho a la libertad de expresión en Internet”. (ii) La inspectora de policía no orientó a las convocantes acerca de los mecanismos dispuestos en el ordenamiento jurídico para la protección de sus derechos y no dio traslado de sus denuncias a las autoridades competentes; y (iii) los jueces de instancia no tuvieron en cuenta los criterios fijados por esta Corporación para dar solución a los casos donde se evidencie cualquier forma de discriminación que se configure en contravía de los derechos de la mujer. Por lo anterior, se emitieron órdenes tendientes a proteger a las funcionarias contra este tipo de violencia.

11.2. Ciberacoso o *cyberbullying* escolar

La Corte, en las sentencias [T-453 de 2022](#), [T-145 de 2016](#) y [T-365 de 2014](#) ha mencionado que el ciberacoso, también conocido como *cyberbullying*, es una modalidad de *bullying* que hace referencia al acoso digital o maltrato a través del uso deliberado de tecnologías de la información (internet, redes socia-



les virtuales, telefonía móvil y videojuegos online³¹. La Corte advirtió que este fenómeno consiste en el uso de estas herramientas para amenazar físicamente, asediar verbalmente o excluir socialmente a un individuo de un grupo.



Sentencia T-145 de 2016

El “bullying” en el ambiente virtual como aquel con base en el cual el autor utiliza las herramientas de la tecnología de la información y las comunicaciones, en especial del internet y el celular, para maltratar a sus semejantes. (...) también se ha definido como un tipo de agresión psicológica en la que se usan teléfonos celulares, internet y juegos en línea para enviar o publicar mensajes, correos, imágenes o videos con el fin de molestar e insultar a otra persona, el cual no se hace de frente y por ello no es fácil identificar a su autor. Así, se ha recalcado que el ciberacoso se ha hecho popular entre niños y jóvenes, quienes creen que pueden usar la red y estos dispositivos anónimamente para molestar a sus compañeros sin percatarse del daño que hacen.

En la sentencia [T-365 de 2014](#), la Corte mencionó que uno de los problemas que ha crecido debido a las nuevas tecnologías es el acoso escolar ya que estas facilitan para que crezcan este tipo de conductas, en intensidad y nocividad, al potenciar el daño causado. En esta providencia se instó al Ministerio de Educación Nacional y al Instituto Colombiano de Bienestar Familiar (ICBF), para que

³¹ Ley 1620 de 2013” Por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar.”



coordinadamente y en el ámbito propio de sus respectivas funciones, formulen y desarrollen una política general que permita la prevención, oportuna detección, atención y protección, frente al hostigamiento, acoso o matoneo escolar, incluyendo el llamado “ciber matoneo” o “cyberbullying”.

En la sentencia [T-449 de 2023](#), la Corte amparó los derechos de una niña la cual fue víctima de ciberacoso escolar y la institución educativa no investigó la conducta. La Corte estableció que el acoso escolar, ya sea en entornos físicos o digitales, afecta gravemente el desarrollo integral de los niños, niñas y adolescentes, razón por la cual, las instituciones educativas tienen la obligación de implementar protocolos efectivos para prevenir, detectar y atender oportunamente estas situaciones, garantizando así un entorno educativo seguro. Casos similares se han estudiado en las sentencias [T-453 de 2022](#) y [T-252 de 2023](#).

11.3. *Sharenting* o exposición de información de niños o niñas en redes sociales por parte de sus padres

En la sentencia [T-245A de 2022](#), la Corte estudió un caso de un hombre que, en representación de su hijo, formuló una acción de tutela en contra de la madre del menor de edad por publicar fotografías del niño en sus redes sociales. Según el actor, las redes de la accionada están vinculadas a una cuenta para adultos. En sus consideraciones, la Corte resaltó el rol de garantes, cuidadores y protectores que recae sobre los padres y aclaró que resulta desproporcionado exigirles, para realizar la exposición de la imagen de sus hijos en sus redes sociales propias, que deban contar con su consentimiento libre, previo y expreso en todos los casos. Sin embargo, enfatizó que debe privilegiarse el respeto por las opiniones de los niños y niñas, de forma que se dé prevalencia a su voluntad y se antepongan sus intereses y derechos a los de los padres.



Sentencia T-245A de 2022

Aunque en Colombia no existe una definición normativa que precise su contenido y alcance, se entiende que esta práctica consiste en documentar la vida personal de los hijos desde temprana edad en internet a través de las redes sociales, mediante comentarios, fotografías, videos u otro material. Así, el sharenting puede implicar una sobreexposición de la imagen de los hijos menores de edad en las redes sociales (...).

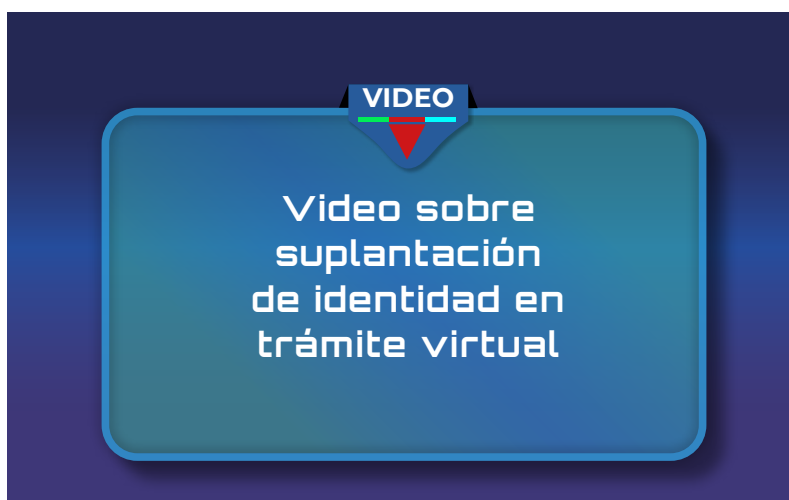
Esta práctica va dejando una huella digital o rastro de información que puede ser accesible a terceras personas, por lo que los niños y niñas pueden ser expuestos a los riesgos y amenazas que surgen en el entorno digital, entre otros, la pornografía infantil, el ciberacoso, el cyberbullying y la suplantación de identidad.

11.4. Ciberdelincuencia y suplantación de identidad en trámites virtuales

En la sentencia [C-224 de 2019](#), la Corte declaró exequible el Convenio sobre la ciberdelincuencia o Convenio de Budapest y su Ley aprobatoria (Ley 1928 de 2018). En este pronunciamiento, la Corte señaló que este Convenio establece las condiciones para prevenir la comisión de ilícitos en las redes informáticas a través de la materialización de una política criminal común en contra de la comisión de delitos cibernéticos. Lo anterior, como una respuesta a los profundos cambios provocados por la digitalización, convergencia y globalización de datos y sistemas informáticos.



La comisión de este tipo de delitos cada vez es más frecuente y demanda toda la atención de las autoridades. Un ejemplo ilustrativo se encuentra en la sentencia [T-360 de 2022](#), donde la Corte conoció un caso de suplantación de identidad a través del uso indebido de documentos y las huellas digitales. Estos datos fueron utilizados para solicitar tres productos bancarios de manera virtual por cuyo incumplimiento se reportó al accionante a las centrales de riesgo. En esta oportunidad, la Corte amparó los derechos y señaló que las entidades bancarias, crediticias o financieras, cuando adviertan un posible caso de suplantación de identidad deben llevar a cabo una investigación interna, con la finalidad de establecer si los productos fueron adquiridos mediante fraude.



11.5. Uso indebido de las redes sociales como mecanismos extraprocesales de cobro

En la sentencia [T-304 de 2023](#), la Corte amparó los derechos de dos accionantes que solicitaron un crédito digital mediante una aplicación. Al incurrir en mora, la accionada utilizó la información personal de los accionantes y envió mensajes amenazantes e injuriosos a los contactos del deudor por WhatsApp. La Corte afirmó que el uso indebido de la información personal vulnera los derechos a la honra, el buen nombre y el habeas data, y desconoce los principios que deben cumplir los administradores de bases de datos.



Por su parte, en la sentencia [T-584 de 2023](#), un ciudadano indicó que, tras solicitar un préstamo dinerario mediante una aplicación móvil e incurrir en mora en el pago, la accionada publicó en redes sociales información personal del actor. La Corte señaló que la divulgación de información personal en redes sociales como medida de cobro extraprocesal vulnera el derecho a la intimidad y constituye un mecanismo de coacción indebida y deshonor pública.

En este caso, se ampararon los derechos del actor y se exhortó a la SIC a realizar seguimiento a las quejas relacionadas con aplicaciones que ofrecen préstamos de dinero y a adoptar medidas para regular y supervisar sus actuaciones, especialmente las relacionadas con los métodos de cobro de sus acreencias.



Sentencia **T-584 de 2023**

No pueden involucrar la divulgación de la información crediticia a un grupo ilimitado e indiscriminado de personas, sino solamente a quienes tengan un interés legítimo y cierto en ella. En consecuencia, la divulgación por canales en los que haya un acceso masivo o indiscriminado, como las redes sociales y plataformas digitales, no está permitida.



DERECHOS en el escenario DIGITAL y de las TIC



BUSCADOR DE RELATORÍA

El siguiente enlace corresponde al Buscador de Relatoría, en el cual se pueden encontrar las providencias proferidas por la Corte Constitucional sobre la temática abordada en el presente boletín:
CORTE CONSTITUCIONAL DE COLOMBIA

VIDEO

Además, puede consultar
el siguiente video para
conocer cómo funciona el
buscador de Relatoría.

INDICE

187



DERECHOS en el escenario DIGITAL y de las TIC



ÍNDICE DE NORMAS





Instrumentos internacionales

Declaración Americana de los Derechos y Deberes del Hombre (1948)

Pacto Internacional de Derechos Civiles y Políticos (1966)

Convención Americana de Derechos Humanos (1978)

Convenio 156 sobre la igualdad de oportunidades y de trato entre trabajadores y trabajadoras: trabajadores con responsabilidades familiares (1981)

Convenio 159 Convenio sobre la readaptación profesional y el empleo (1983)

Comité de los Derechos del Niño (1991)

Convención Interamericana para la Eliminación de Todas las Formas de Discriminación contra las Personas con Discapacidad (1999)

Protocolo Adicional a la Convención Americana de Derechos Humanos o Protocolo de San Salvador (1999)

Declaración de Principios sobre Libertad de Expresión (2000)

Convenio sobre la Ciberdelincuencia (2001)

Carta de Santo Domingo por el Libre Acceso a la Información Pública (2002)

Convención Interamericana sobre la protección de los Derechos Humanos de las Personas Mayores (2015)

Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública (2020)



DERECHOS en el escenario DIGITAL y de las TIC



Normativa nacional relevante	
Número	Descripción
Constitución Política de 1991	
Resolución No. 1995 de 1999	Por la cual se establecen normas para el manejo de la Historia Clínica.
Ley 270 de 1996	Estatutaria de la administración de justicia.
Ley 361 de 1997	Por la cual se establecen mecanismos de integración social de las personas con limitación y se dictan otras disposiciones.
Decreto 1543 de 1997	Por el cual se reglamenta el manejo de la infección por el Virus de Inmunodeficiencia Humana (VIH), el Síndrome de la Inmunodeficiencia Adquirida (SIDA) y las otras Enfermedades de Transmisión Sexual (ETS).
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 633 de 2000	Por la cual se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial.
Acuerdo N.º 1591 de 2002	Por el cual se establece el sistema de información de gestión de procesos y manejo documental (Justicia XXI).



Decreto 643 de 2004	Por el cual se modifica la estructura del Departamento Administrativo de Seguridad y se dictan otras disposiciones.
Ley 906 de 2004	Por la cual se expide el Código de Procedimiento Penal.
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1098 de 2006	Por la cual se expide el Código de la Infancia y la Adolescencia.
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones “TIC”, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1450 de 2011	Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014



Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 019 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Decreto 233 de 2012	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional.
Decreto 884 de 2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
Ley 1564 de 2012	Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones
Resolución 2886 de 2012	Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.
Resolución 2774 de 2013	Por la cual se reglamenta el uso de inhibidores, bloqueadores y amplificadores de señales radioeléctricas.
Ley 1620 de 2013	Por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar.



Acuerdo No. PSAA14-10215	Por el cual se autoriza la adecuación del sistema de información de gestión de procesos y manejo documental (Justicia XXI) en ambiente Web.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1072 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo.
Ley 1751 de 2015	Por medio de la cual se regula el derecho fundamental a la salud y se dictan otras disposiciones.
Ley 1755 de 2015	Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Ley 1801 de 2016	Por la cual se expide el Código Nacional de Seguridad y Convivencia Ciudadana.
Resolución 1823 de 2018	Por la cual se modifica la Resolución 2774 de 2013
Ley 1928 de 2018	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
Circular DEAJC19-9 de 2019	Cumplimiento político de tratamiento de datos personales y de la información Ley 1581 de 2012.



Circular 01 de 2019	Manejo y Uso de Redes Sociales
Circular 01 de Circular 041 de 2020	Lineamientos respecto del trabajo en casa
Ley 295 de 2020	Proyecto de Ley estatutaria [p]or medio de la cual se modifica la ley 270 de 1996 – Estatutaria de la Administración de Justicia.
Decreto 491 de 2020	Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica.
Decreto Legislativo 771 de 2020	Mediante el cual se dispone una medida para garantizar el acceso a servicios de conectividad en el marco del estado de emergencia económica, social y ecológica en todo el territorio nacional
Decreto 806 de 2020	Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de Emergencia Económica, Social y Ecológica.
Ley 2015 de 2020	Por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones.
Acuerdo PCSJA20-11631 del 2020	Por el que se adopta el Plan Estratégico de Transformación Digital de la Rama Judicial -PETD 2021- 2025



Ley 2088 de 2021	Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
Ley 2121 de 2021	Por medio de la cual se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones.
Ley 2213 de 2022	Por medio de la cual se establece la vigencia permanente del Decreto Legislativo 806 de 2020 y se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia y se dictan otras disposiciones.
Decreto 1227 de 2022	Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9. y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo, relacionados con el Teletrabajo.
Circular CDJC23-1 de 2023	Condiciones de publicación de contenidos en el portal Web de la Rama Judicial, para proteger el derecho a la intimidad personal y familiar de las personas.
Ley 2305 de 2023	Por la cual se expiden disposiciones sobre las estadísticas oficiales en el país
Acuerdo PCSJA24-12243	Por el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial.

Sentencias publicadas hasta 12 de septiembre de 2025.

