

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA JURÍDICA DISTRITAL
BOGOTÁ

Notas a Jurisprudencia

Smart cities y tecnología para la sostenibilidad: Uso de datos, inteligencia artificial y nuevas tecnologías para la gestión eficiente de las ciudades desde la jurisprudencia colombiana

Santiago Londoño Camacho
Abogado de la Universidad Sergio Arboleda (1996), especialista em Derecho Comercial y Financiero, Magister en Derecho Procesal y Probatorio, y profesor en Especialización y Maestría en Derecho Administrativo con énfasis en Servicios Públicos.

Resumen

Un breve acercamiento del complejo ejercicio administrativo para la modernización de las ciudades en el marco del uso de medios tecnológicos y el respeto a los derechos fundamentales de los ciudadanos.

Palabras claves: *Inteligencia artificial, datos, datos personales, megadatos, ciudad inteligente, desarrollo territorial, seguridad, servicios públicos, modernidad.*

La inteligencia artificial (IA) se ha extendido ampliamente en los últimos años. Desde la aplicación del WhatsApp, hasta el chat GPT en sus distintas versiones (hoy), producto de complejos algoritmos que unen diversas fuentes de información, se convierten en poderosos buscadores de datos en una infinita nube de conocimiento. En este entorno, donde los datos no se limitan a reproducir documentos o archivos en sus repositorios, sino que la IA genera un documento propio. Para entender su alcance, haremos un ejercicio con ChatGPT: le preguntaremos, *"haz un artículo legal que tenga relación con los conceptos de Smart cities y tecnología de la sostenibilidad", veamos los resultados:*

"La integración de tecnologías avanzadas en el desarrollo de ciudades inteligentes plantea desafíos y oportunidades legales significativas. A continuación, se presentan algunos aspectos legales clave relacionados con las ciudades inteligentes y la tecnología de la sostenibilidad:

1. Normativas y Estándares Internacionales

*La **ISO 37120:2018** establece indicadores para medir el desempeño de los servicios urbanos y la calidad de vida en las ciudades. Esta norma proporciona un marco para evaluar la sostenibilidad en el contexto de las ciudades inteligentes, abarcando aspectos como economía, educación, energía, medio ambiente, finanzas, gobernanza, salud, vivienda, seguridad, transporte, entre otros. Wikipedia, la enciclopedia libre*

2. Legislación Ambiental y Objetivos de Neutralidad Climática

*El **Reglamento (UE) 2021/1119** establece objetivos vinculantes para alcanzar la neutralidad climática en la Unión Europea antes de 2050. Este reglamento implica que las ciudades inteligentes deben adoptar tecnologías sostenibles que reduzcan las emisiones de gases de efecto invernadero, promoviendo el uso de energías renovables y mejorando la eficiencia energética en infraestructuras urbanas. revistarue.eu*

3. Protección de Datos y Privacidad

*La implementación de tecnologías de la información y la comunicación (TIC) en las ciudades inteligentes conlleva la recopilación masiva de datos de los ciudadanos. Es fundamental que las legislaciones locales e internacionales, como el **Reglamento General de Protección de Datos (GDPR)** en Europa, aseguren la protección de la privacidad y regulen el uso adecuado de estos datos.*

4. Accesibilidad e Inclusión Social

Las ciudades inteligentes deben garantizar que las tecnologías implementadas sean accesibles para todos los ciudadanos, incluyendo a personas con discapacidades y comunidades vulnerables. Esto requiere el desarrollo de políticas públicas y marcos legales que promuevan la inclusión digital y eviten la brecha tecnológica.

5. Gobernanza y Participación Ciudadana

La adopción de tecnologías sostenibles en las ciudades inteligentes debe ir acompañada de mecanismos legales que fomenten la participación ciudadana en la toma de decisiones. Esto asegura que el desarrollo urbano sea transparente, democrático y refleje las necesidades reales de la comunidad.

6. Seguridad y Ciberseguridad

La interconexión de sistemas en una ciudadinteligente aumenta la vulnerabilidad a ciberataques. Es esencial que las leyes y regulaciones locales e internacionales aborden la ciberseguridad, estableciendo estándares y protocolos para proteger las infraestructuras críticas y la información de los ciudadanos.

Conclusión

El desarrollo de ciudades inteligentes sostenibles requiere un marco legal robusto que aborde desde la protección ambiental hasta los derechos digitales de los ciudadanos. La colaboración entre gobiernos, sector privado y sociedad civil es crucial para crear entornos urbanos que sean tecnológicos, sostenibles y respetuosos con los derechos humanos".

Como podemos constatar, los mecanismos derivados de la IA son cada día más eficientes y exploran el conocimiento humano mediante el análisis de la información contenida en los repositorios digitales. Por ello, debemos comprender sus conceptos y objetivos para que, en el marco del derecho positivo, podamos regular su participación en la sociedad. Para megasociedades como Bogotá, una capital con aproximadamente 11 millones de ciudadanos, estas tecnologías ofrecen respuestas para resolver algunos de sus problemas.

La IA y sus efectos se abren paso en la sociedad a tal velocidad que no nos ha permitido procesar debidamente sus consecuencias. Por ello, debemos, desde el derecho y, en especial, desde la jurisprudencia más reciente, resolver los efectos que de ella derivan.

En los estudios de derecho, siempre se nos ha enseñado que primero vienen los hechos y luego el derecho, como estructura fundamental de la sociedad para imponer una norma jurídica. Es por ello que no hablamos de regulación del espectro electromagnético en 1886, pues eran conceptos ajenos a la realidad humana. Normalmente, el Derecho tiene la oportunidad de abordar sus procesos a través del legislador, con tiempo, análisis e investigación, ya sea en temas como la clonación, las telecomunicaciones o los derechos constitucionalmente protegidos.

Sin embargo, esto no ocurre en el caso de la inteligencia artificial y sus efectos, que rebasan al legislador con tal rapidez que, cuando este reacciona y genera una norma, ésta ya nace desueta. Con ello, el panorama no es alentador para la organización del Estado: las nuevas tecnologías y sus desarrollos ni siquiera respetan las curvas de aprendizaje, pero sí producen efectos jurídicos.

Los procesos de observación y los efectos jurídicos de la tecnología en las ciudades son más fáciles de percibir. En ese entorno urbano, se presenta la tensión objeto de análisis: la tecnología despliega sus desarrollos y utiliza al ciudadano como unidad de experimentación, para la aplicación de sus avances. Se prueban aplicaciones, productos,

procesos, y es el ciudadano —muchas veces de manera inconsciente— quien actúa como receptor de la máquina.

El concepto de *"Smart City"* como una *"estrategia de fortalecimiento de capacidades mediante el acompañamiento especializado, asesoría consultiva, así como la apropiación del Modelo de Medición de Madurez de Ciudades y Territorios Inteligentes. Todas estas herramientas permiten la definición de una hoja de ruta para que las entidades territoriales puedan avanzar en su transformación digital territorial"*[1]. Así lo concibe el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y mediante la Resolución 1117 del 2022 establece los siguientes lineamientos bajo el concepto de transformación digital de ciudades y territorios. Veamos sus líneas de acción, derivadas de este estudio:

1. Línea de acción #1. Modelo de Madurez de Ciudades y Territorios Inteligentes

Conforme a la "ESTRATEGIA NACIONAL DIGITAL DE COLOMBIA 2023-2026", la Política de Gobierno Digital liderada por MinTIC, debe contemplar como acción prioritaria la adopción del Modelo de Madurez de Ciudades y Territorios Inteligentes.

El Modelo es una herramienta de autodiagnóstico que permite identificar la situación actual de una entidad territorial con relación a las dimensiones de calidad de vida, hábitat, medio ambiente, desarrollo económico, gobernanza y personas. Esto ayuda a identificar las verticales de ciudad que pueden apoyarse mediante iniciativas de ciudades inteligentes, posibilitando la creación de fuentes de información (datos) para orientar los esfuerzos del gobierno local hacia el mejoramiento de la calidad de vida de sus habitantes.

De esta manera se promueve la transformación digital territorial en todos los sectores de la sociedad, y se incentiva a que, desde las entidades públicas territoriales, se diseñen las condiciones necesarias para que se puedan desarrollar los proyectos e iniciativas de ciudades y territorios inteligentes. Los principales beneficios del Modelo son:

Identificar el estado actual de la ciudad o territorio con respecto a las distintas dimensiones que se evalúan.

Identificar las principales necesidades de los ciudadanos, los problemas y desafíos de los territorios.

Articular los resultados del Modelo de Medición de Madurez con las prioridades de los planes de Desarrollo.

Fortalecer y optimizar la capacidad institucional de las entidades territoriales

Disponer de decisiones rápidas y oportunas basadas en información y datos en tiempo real para mejorar la calidad de vida de los ciudadanos.

Fortalecer los vínculos urbanos-rurales que incluya la participación ciudadana para identificar prioridades de intervención tecnológica en los territorios con baja cobertura y acceso a internet.

1 Ministerio de Tecnologías de la Información y las Comunicaciones, *Ciudades y Territorios Inteligentes*, Recuperado de: https://gobiernodigital.mintic.gov.co/portal/Iniciativas/Ciudades-y-Territorios-Inteligentes/.

Línea de acción #2 Acompañamiento técnico y lineamientos de ciudades y territorios inteligentes

En el marco de la estrategia "Ciudades y Territorios Digitales", MinTIC viene realizando acompañamiento técnico a las iniciativas y requerimientos postulados por las diferentes entidades territoriales. Por medio del acompañamiento técnico, el Ministerio TIC brinda asesoría a las entidades territoriales para la formulación de sus iniciativas de ciudades inteligentes. Para cumplir este objetivo, el Ministerio pone a disposición de las entidades, el equipo de consultores especializados de ciudades inteligentes.

El MinTIC brinda asesoría especializada a las entidades territoriales para la formulación y estructuración de sus proyectos afines con ciudades y territorios inteligentes, esto lo hará en coordinación con las entidades nacionales lideres del sector y así definirán los lineamientos técnicos soportados en los Acuerdos Marco de Precios - AMP. Los AMP son contratos de demanda agregada a los cuales se pueden adherir las entidades públicas y contratar por medio de ellos. Los AMP incentivan el desarrollo en el país para que puedan resolver las necesidades de sus ciudadanos. Los AMP pueden ser consultados en la Tienda Virtual del Estado Colombiano https://colombiacompra.gov.co/content/tienda-virtual.

Línea de acción #3. Cofinanciación de estrategias de ciudades y territorios inteligentes

En caso de que el MinTIC así lo estime, se habilitarán diferentes mecanismos tales como convenios interadministrativos y convocatorias públicas que permitan la cofinanciación de proyectos de ciudades y territorios inteligentes. Para ello, estableció los lineamientos relacionados con los mecanismos de cofinanciación de las estrategias de ciudades y territorios inteligentes con recursos del Fondo Único de TIC - FUNTIC. Esta información, que se encuentra disponible en el anexo 3 de la Resolución, también proporciona a las entidades territoriales todos los aspectos que se deben tener en cuenta para participar en los mecanismos de cofinanciación.

Línea de acción #4. Plataforma de ciudades y territorios inteligentes

La plataforma de ciudades y territorios inteligentes de MINTIC es un esfuerzo nacional por brindar una herramienta transversal para que los proyectos y beneficios de las ciudades inteligentes sean más fáciles de implementar por parte de cualquier entidad.

La plataforma de MinTIC está diseñada con el principio de integración de datos generados a partir de fuentes de diversa naturaleza tales como IOT, redes sociales, datos estructurados, semiestructurados y no estructurados con enfoque en la analítica y visualización de los datos que llegan a la plataforma relacionados con cualquiera de las verticales de ciudad.

La plataforma de ciudades y territorios inteligentes implementa tecnologías de la Cuarta Revolución Industrial y tecnologías de analítica de datos para el apoyo a la

toma de decisiones basadas en datos con enfoque en la analítica y visualización de datos generados por IoT.

Con lo anterior, queda claro que, desde el Gobierno central se le otorga relevancia al concepto de ciudad inteligente, el cual se fundamenta en la creación de espacios adecuados para el análisis de datos. En abril de 2022, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) publicó el Documento Anexo 2, en el marco del producto Ciudades y Territorios Inteligentes, como desarrollo del artículo 147 del Plan Nacional de Desarrollo 2018–2022 y del Decreto 1008 de 2015, por el cual se *"establecen los lineamientos generales de la Política de Gobierno Digital, el Ministerio de TIC plantea la estrategia de acompañamiento técnico para la formulación de iniciativas de Ciudades y Territorios Inteligentes. Por medio del acompañamiento técnico, el Ministerio de TIC brinda asesoría consultiva a las entidades públicas en la estructuración de estrategias relacionadas con Ciudades y Territorios Inteligentes".*

Otro de los aspectos fundamentales del Ministerio en este proyecto es la Política de Gobierno Digital (PGD), definida por este como el *"instrumento gubernamental del orden nacional que propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TIC. La PGD hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de gestión y desempeño institucional[2]".* Tiene como producto el Decreto 767 del 2022, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital, *"entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio".*

En este punto hemos visto los desarrollos legales del concepto de avance digital. En todo caso, la norma en comento trae a colación algunos interesantes aspectos que vale la pena ahondar antes de continuar:

> ***6. Respeto de los Derechos Humanos:*** *Los sujetos obligados a la aplicación, implementación, interpretación y ejecución de la Política de Gobierno Digital, garantizarán el respeto de los Derechos Humanos y de los principios constitucionales y legales. Los sujetos obligados que usen Tecnologías de la Información y las Comunicaciones deberán asegurar mecanismos suficientes y adecuados que garanticen el ejercicio pleno de los derechos de las personas en sus relaciones con el Estado.*

2 Ministerio de Tecnologías de la Información y las Comunicaciones, Política de Gobierno Digital, Recuperado de: https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/.

12. Resiliencia Tecnológica: *Los sujetos obligados a la aplicación de la presente Política tomarán acciones respecto de la prevención de riesgos que puedan afectar la seguridad digital y con ello propenderán por la disponibilidad de los activos, la recuperación y continuidad de la prestación del servicio ante interrupciones o incidentes.*

3.2. Seguridad y Privacidad de la Información: *Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.*

4.2. Decisiones Basadas en Datos: *Esta línea de acción busca promover el desarrollo económico y social del país impulsado por datos, entendiéndolos como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección y tratamiento de datos personales y permitan mejorar la toma de decisiones y la prestación de servicios de los sujetos obligados*.

Así las cosas, todo nuestro entorno personal, social, familiar y laboral se encuentra definido dentro de este marco. Nuestro nombre, junto con nuestra identificación, constituye en sí mismo información que debería estar dirigida únicamente a un destinatario autorizado por la voluntad del sujeto; es decir, no debería ser pública. Para profundizar en este tema, acudimos a la Superintendencia de Industria y Comercio y a su análisis sobre los contenidos de la Ley 1581 de 2012:

- Datos Personales: Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.
- Dato Público: Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.
- Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.
- Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.
- Dato Sensible: Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

La Corte Constitucional no ha sido ajena a esta discusión. Al respecto, en su jurisprudencia ha desarrollado que:

"Los datos personales pueden ser clasificados en cuatro grandes categorías: públicos, semiprivados, privados y sensibles.

De acuerdo con la Ley 1266 de 2008, es público el dato calificado "como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados (...).

Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".

Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Son semiprivados aquellos datos "que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general".

Por lo demás, son privados aquellos que datos "por su naturaleza íntima o reservada sólo [son] relevante[s] para el titular".

Son datos sensibles "aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición[,] así como los datos relativos a la salud, a la vida sexual y los datos biométricos". Por su propia naturaleza, estos datos se vinculan con la salvaguarda de la intimidad de su titular o con la proscripción de actos discriminatorios[3]".

Volviendo sobre el dato personal, todos los procesos de innovación y nuevas tecnologías se encuentran acoplados a dinámicas conductuales de los ciudadanos. Ya se sabe qué le gusta comer a una persona, a dónde viaja, qué enfermedades padece y un sinfín de otras preferencias personales asociadas a su nombre, número de teléfono, dirección de correo electrónico y cualquier otro mecanismo digital que utilice información personal. A esto se suma el hecho de que el propio ciudadano alimenta aún más esa macro base de datos al publicar lo que come, adónde viaja, sus recorridos, sus gustos, su trabajo, sus mascotas y sus preferencias personales.

El concepto de intimidad y datos personales se encuentra muy ligado, en tanto están profundamente atados uno del otro y muchas veces no es fácil evaluar los alcances de cada uno. Respecto al concepto de intimidad, la Corte Constitucional ha manifestado que:

> *"El derecho a la intimidad se encuentra reconocido en el artículo 15 de la Constitución, conforme al cual, en lo pertinente: (i) todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar; (ii) la correspondencia y demás formas de*

3 Corte Constitucional, Sentencia T-706 de 2014. M.P. Luis Guillermo Guerrero Pérez.

comunicación privada son inviolables y sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley; y (iii) para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley"[4].

Por su parte, respecto a la privacidad, la Corte ha señalado que:

> *"la expectativa de privacidad es un criterio relevante para establecer si determinadas expresiones o manifestaciones de la vida de las personas pueden entenderse comprendidas por el ámbito de protección del derecho a la intimidad o si, por el contrario, pueden ser conocidas o interferidas por otros. Tal categoría impone definir, atendiendo diferentes factores contextuales, si (i) quien alega la violación puede considerar válidamente que su actividad se encuentra resguardada de la interferencia de otros; y (ii) si es o no posible concluir que dicha valoración es oponible a los terceros que pretenden acceder a la información o divulgarla*[5]*".*

Todos estos elementos deben ser analizados en el contexto de la proyección de una ciudad "inteligente", ya que algunos derechos entran en evidente tensión cuando se abordan temas como la seguridad ciudadana o la movilidad urbana, especialmente en relación con los datos personales. En tal sentido, y con fundamento en el concepto jurídico de interés general, la Corte, en la sentencia en comento[6], señala:

> *"En vista de todo lo anterior, la Corte considera necesario condicionar el contenido del artículo 237 de la Ley Estatutaria 1801 de 2016. En este sentido, debido a que existe un fin legítimo asociado con el objeto de la norma, consistente en proteger el interés general y garantizar el orden público, no se puede proscribir la misma, en la medida que su finalidad está asociada a la prevención del crimen y la promoción de la seguridad jurídica. Lo anterior, admite que, si bien podría afectarse eventualmente el comportamiento de las personas y su expectativa de privacidad en los sitios señalados por la norma demandada, no se puede desconocer el beneficio en materia de seguridad, interés general y protección del orden público.*
>
> *Por esta razón, la Corte aclara que la captación y/o almacenamiento de información, datos o imágenes a los que se refiere la norma acusada deberá ceñirse en todo momento a los principios establecidos en la Ley 1581 de 2012, en especial, la determinación del tiempo de conservación de la información, las obligaciones de tratamiento de la misma, y las personas entre las cuales se puede circular.*
>
> *Asimismo, en el marco de la respectiva regulación, se deberán especificar las formas y los términos en los que se llevará a cabo el tratamiento de la información, para que no afecte el derecho al habeas data. De este modo, su uso debe seguir una serie de principios y garantías adscritas al derecho*

4 Corte Constitucional, Sentencia C-094 de 2020. M.P. Alejandro Linares Cantillo.

5 Ibidem.

6 Ibidem.

al habeas data reconocido en el artículo 15 de la Carta Política. Estos principios, y declarados ajustados a los mandatos constitucionales en la sentencia C-1011 de 2008, son los siguiente:

i. Principio de legalidad: El tratamiento de datos es una actividad reglada que debe sujetarse a lo establecido en las disposiciones legales aplicables y en las demás disposiciones que la desarrollen.

ii. Principio de finalidad y utilidad: De la relevancia en el día a día de su aplicación de fijar límites al tipo de información que pueda ser captada[106], esto es debe obedecer a un fin constitucionalmente legítimo. En consecuencia, se considerará que la expresión "libre acceso" conlleva a que la información pública podrá ser conocida por autoridades públicas en los casos en los que tal información sea útil para la realización de los propósitos identificados.

iii. Principio de libertad: Las actividades de registro y divulgación de los datos personales sólo pueden ejercerse con el consentimiento libre y previo del titular de esa información.

iv. Principio de transparencia: El tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

v. Principio de acceso y circulación restringida: Se debe prohibir la divulgación indiscriminada de datos personales. Las actividades de recolección, procesamiento y divulgación de información personal deben estar sometidas a los límites específicos determinados por el objeto de la base de datos, y sujetarse a principios de confidencialidad, inviolabilidad y reserva.

vi. Principio de necesidad: La necesidad de limitar, con fundamento en los principios de finalidad, necesidad y circulación restringida, los objetivos que pueden perseguir tales actividades y los sujetos entre los que pueden circular. De esta forma, la base de datos debe identificar de forma clara, expresa y suficiente el propósito de la recolección y tratamiento de datos, por cuanto, la información personal concernida debe ser aquella estrictamente necesaria para el cumplimiento de los fines de la base de datos.

vii. Principio de seguridad y confidencialidad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

viii. *Principio de caducidad: Se debe prohibir la conservación indefinida de datos personales, después de que hayan desaparecido las causas que justificaron su acopio y administración.*

Por consiguiente, las imágenes, sonidos o conversaciones de las personas que son captados por cámaras de vigilancia u otros sistemas tecnológicos son, en general, datos personales cuyo tratamiento debe sujetarse a los contenidos del derecho al habeas data. De esta forma, en términos generales, los responsables del tratamiento de los datos deben obligarse a respetar el carácter lícito y leal de la recopilación y el tratamiento automatizado de los datos personales, las finalidades legítimas de la grabación y del registro, la limitación de la conservación de estas imágenes a un plazo estrictamente necesario, el carácter adecuado y no excesivo del sistema respecto a los objetivos que se persiguen, así como la pertinencia de los datos y la obligación de actualizarlos. De esta misma forma, deben propender por proscribir el tratamiento de datos personales, y garantizar, asimismo, el derecho que tienen las personas a conocer la información sobre ellas almacenada y de exigir, en su caso, las rectificaciones que sean precisas".

Por su parte, el Consejo de Estado ha compartido la línea argumentativa de la Corte Constitucional, también ha expresado lo siguiente:

> *2.3. Derecho a la intimidad y el habeas data: El derecho a la intimidad personal y familiar, consagrado en el artículo 15 de la Constitución Política, es una garantía compleja que comprende varias áreas de concreción en la vida social de las personas residentes o transeúntes en el territorio colombiano.*

En efecto, la referida norma constitucional señala:

> *"ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.*
>
> *La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".*
>
> *La Corte Constitucional en sentencia SU-089 de 1995 expuso que entre los distintos aspectos que comprende el derecho a la intimidad se encuentran "los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto*

que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación que éstos tienen de aquel".

Ahora, como se lee del artículo 15 de la Constitución de 1991 una de las órbitas del derecho a la intimidad se traduce en el "(...) derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas". Además, señala que "[e]n la recolección, tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución". Estos preceptos, leídos en conjunto con la primera parte del mismo artículo 15, el artículo 16 (derecho al libre desarrollo de la personalidad) y el artículo 20 (derecho a la información activo y pasivo y el derecho a la rectificación), han dado lugar al reconocimiento jurisprudencial de un derecho fundamental autónomo catalogado como derecho al habeas data. El derecho al habeas data ha sido definido por la Corte Constitucional como aquel que "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 los mismos de conformidad con los principios que regulan el proceso de administración de datos personales".

Asimismo, el habeas data comprende la autodeterminación informática y tiene "la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo."

"Los principios de finalidad y libertad, fundamentales en el régimen de protección de datos, suelen encontrarse en tensión, espec8 ialmente cuando se está frente a protecciones del interés general. En esta medida, si bien resulta claro que "la obtención y divulgación de datos personales sin la previa autorización del titular o en ausencia de un claro y preciso mandato legal, se consideran ilícitas" la jurisprudencia constitucional ha admitido que la rigidez del principio de necesidad antes descrito pueda ceder ante la necesidad de cumplir con un fin superior"[7].

Hasta ahora, nos hemos referido únicamente a la generación y protección de los datos personales; ahora pasamos al ejercicio de materializar estos conceptos en relación con la ciudad y su desarrollo.

Bogotá D.C. es una ciudad con un sistema de transporte, tanto particular como público, claramente colapsado. Esta situación no solo se evidencia en la realidad vial que padecen a diario los ciudadanos de la capital —la más congestionada de esta parte del hemisferio—, sino que también se respalda en el *Informe de Gestión y Resultados de la Secretaría de Movilidad,* con corte al 31 de diciembre de 2024[8], en el cual se menciona:

7 Consejo de Estado, Sentencia del 15 de diciembre de 2021, Consejero Ponente: Carlos Enrique Moreno Rubio, exp. 070005-00.

8 Secretaría de Movilidad, 2024. Recuperado de: https://www.movilidadbogota.gov.co/web/sites/default/files/Paginas/24-02-2025/informe_de_gestion_y_resultados_2024_ajuste_definitivo.pdf

"El año 2024 es una vigencia de importantes logros para el Sector Movilidad, es el primero de la administración del Alcalde Carlos Fernando Galán , donde su Plan de Gobierno se materializa en el plan de desarrollo económico, social, ambiental y de obras públicas del Distrito Capital 2024-2027 "BOGOTÁ CAMINA SEGURA", en el marco de lo cual, el Sector cuenta con 5 programas y 49 metas para la mejora de la calidad de vida de las personas que habitan en Bogotá, garantizando el ejercicio pleno de sus derechos, una mayor seguridad, inclusión, libertad, igualdad de oportunidades y un acceso más justo a bienes y servicios públicos.

La Secretaría Distrital de Movilidad implementa soluciones que generan opciones de movilidad convenientes, amables, saludables y seguras para cada viaje, con el fin de optimizar el modelo de movilidad y de gestión en vía de la ciudad con enfoque de eficiencia, sostenibilidad e inclusión, recuperación del espacio público para la movilidad, superación del rezago en infraestructura, favorecimiento de la competitividad de la Ciudad-Región y aporte a los compromisos del plan de acción climática", pero cuya tediosa revisión revela un pobre ejercicio en materia de modernización de la ciudad, cuyo resultado es claro, no se plantean productos o procesos de modernización y uso de nuevas tecnologías, salvo multas, que no es más que el poder coercitivo de la Administración. No obstante, el futuro de la información vial y su automatización es algo claramente inevitable, y allí tendrán que discutirse todos los aspectos relacionados con el uso de información del usuario y la inteligencia artificial para su manejo, pues la actual congestión vehicular genera más contaminación e inseguridad y desmejora notablemente la calidad de vida de sus ciudadanos y que la Administración se permita entender el funcionamiento de la ciudad como un organismo vivo, para con ello dictar políticas claras de mejoramiento de la calidad de vida no solo en transporte y movilidad, sino en el uso masivo de oficinas satélites en áreas sectorizadas para sus funcionarios, aplicable al Nivel Nacional y privados, pues no es de recibo desplazamientos de más de 20 kilómetros por recorrido para trabajar en el centro u occidente de la ciudad de más de 3 horas al día; trabajos híbridos, pero reales, las normas de teletrabajo (Ley 1221 de 2008, el Decreto 0884 de 2012, el Decreto 1072 de 2015 y, finalmente, la Circular 0027 de 2019) son saludos a la bandera, no se aplican masivamente y las entidades públicas y privadas siguen amarrando el funcionario a su escritorio. La inteligencia artificial y el uso de datos personales compartidos en el sistema integrado de transporte debe ser una prioridad, Transmilenio como eje fundamental del proceso, deberá ser el primero en hacer uso de este tipo de herramientas que realmente organice la distribución de sus buses y permitan una operación más eficiente, sin desconocer las actuales mejoras en servicio y seguridad.

En el ámbito de la seguridad, los retos son aún mayores. Bogotá deberá enfrentar una modernización urgente de sus sistemas electrónicos de vigilancia, que no solo implique

cámaras, sino también tecnologías como el reconocimiento facial, la detección digital de vehículos y las alertas automáticas.

La seguridad no puede sustentarse únicamente en el aumento del pie de fuerza, sino en el uso estratégico de medios tecnológicos para enfrentar las amenazas provenientes de bandas criminales, tanto físicas como informáticas. Actualmente, delitos como extorsión, suplantación de identidad y otras conductas criminales que se valen del uso indebido de información personal y medios electrónicos están en aumento exponencial.

Si bien existen disposiciones penales que protegen a las víctimas, este fenómeno debe ser una de las principales líneas de atención tanto de la Fiscalía General de la Nación como de la Policía Nacional, en el marco de sus competencias como autoridades de apoyo judicial. Sin seguridad no hay desarrollo, no hay prosperidad, y mucho menos puede hablarse de un Estado Social de Derecho.

Lo anterior implicará un necesario —y complejo— equilibrio entre la protección de datos personales, el derecho a obtener información, su categorización, uso y difusión, siempre orientado por el principio del bienestar general sobre el interés particular.

La seguridad, como concepto moderno, está ligada al conjunto de dispositivos o medios tecnológicos mediante los cuales es posible obtener información de terceros. Estos van desde la simple cámara de vigilancia pública, pasando por las cámaras "salvavidas" o de fotomultas, hasta llegar a una segunda generación de tecnologías que incorporan reconocimiento facial o biométrico.

La Corte Constitucional se ha ocupado de este tema, haciendo incluso algunas referencias extranjeras en el ámbito de la intimidad. En este sentido, ha señalado:

> *"La regla general es que las cámaras solo pueden recopilar información en la esfera pública. Por ejemplo, el uso de cámaras en la parte frontal de los vehículos ha sido considerado como beneficioso. Estos dispositivos permiten resolver disputas en accidentes de tránsito, reducir los litigios y evitar los costos de los peritajes. De allí que sean permitidos, bajo algunas restricciones, en Bélgica, Lituania y el Reino Unido.*
>
> *Sin embargo, se ha destacado el riesgo que implican para la protección de la intimidad de terceros, la defraudación de la expectativa de intimidad y la inexistencia de consentimiento. Esto ha llevado a que se prohíban mediante multas (Austria), se excluya el uso de esos videos en los procesos (Alemania) y se considere desproporcionado que se capten rostros de personas en la calle sin su consentimiento (Luxemburgo).*
>
> *En ese mismo ámbito, uno de los principales retos que representan los teléfonos móviles equipados con cámaras o las minúsculas cámaras digitales es el hecho de que pueden captar la imagen de las personas sin que estas lo sepan[9]"*, por lo que se plantean unas reglas en su uso definidas en varias sentencias, veamos:

9 Corte Constitucional, Sentencia T-280 de 2022. M.P. José Fernando Reyes Cuartas.

- **Sentencia T-768 del 2008:**
  1. La instalación de métodos de vigilancia en los espacios laborales no vulnera los derechos fundamentales a la intimidad, a la dignidad humana, al debido proceso y al trabajo en condiciones dignas y justas cuando se persigue un objetivo legítimo.
  2. Para analizar si este fin es viable, proporcional y necesario, los operadores judiciales deben verificar el objeto social que desarrolla la empresa.
  3. Además, se debe revisar el sitio de instalación para que sea dentro del ambiente laboral y no invada arbitrariamente lugares abiertos al público (i.e. los baños).
  4. El fin de la vigilancia debe estar directamente relacionado con una medida de seguridad necesaria, que se hayan estudiado formas menos invasivas y la mitigación de los perjuicios para los trabajadores.
  5. Es obligación informar sobre la instalación de las cámaras de vigilancia.
  6. Finalmente, está proscrito cualquier trato inhumano, cruel o degradante derivado de la medida de seguridad.
- **Sentencia T-407 de 2012:**
  1. Cuando se trate de los niños, las niñas y los adolescentes estudiantes (sujetos de especial protección), se debe aplicar un juicio de proporcionalidad estricto para establecer la constitucionalidad de la instalación de las cámaras de vigilancia en las aulas de clase.
  2. Al aplicar dicho test, el tribunal determinó que los métodos de vigilancia en las instituciones educativas tienen un fin constitucional: la seguridad de los estudiantes y de las instalaciones. También pretenden evitar infracciones por parte de los estudiantes e identificar a los responsables cuando tales hechos ocurran.
  3. El tribunal destacó que las cámaras no siempre son necesarias porque existen otros mecanismos de seguridad (i.e. celadores) que son menos lesivos para el derecho a la intimidad.
  4. Por último, la Corte concluyó que la medida afectaba desproporcionadamente los derechos de los estudiantes, constituía una auténtica *panoptización* e inhibía las expresiones y manifestaciones propias de los entornos escolares.
- **Sentencia T-487 de 2917:**
  1. La información obtenida a través de las grabaciones de video de la calle o el espacio público es privada.
  2. La Corte afirmó que la entrega de material fílmico a los particulares puede vulnerar el derecho a la intimidad de las terceras personas porque su imagen pudo quedar registrada en la grabación solicitada por el ciudadano.
  3. El material fílmico se debe reclamar, tratar, cuidar, custodiar y proteger por una autoridad.
  4. Cuando se trate de un proceso penal, la Fiscalía General de la Nación debe incorporar la prueba.

- **Sentencia T-114 de 2018:**

    1. 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 (i.e. imágenes en vestido de baño) constituyen información privada.

    2. Dicha información solo puede ser obtenida por orden de una autoridad judicial en el cumplimiento de sus funciones.

- **Sentencia C-094 del 2020:**

    1. La instalación de las cámaras en los medios de transporte público masivo es una limitación leve al derecho de intimidad porque las medidas de vigilancia obedecen al interés general de la población.

    2. Esta medida se encuentra justificadaen un fin legítimo y cumple con los requisitos de proporcionalidad y razonabilidad exigidos por la jurisprudencia constitucional.

Revisados los requisitos, no será sencillo el tránsito hacia una ciudad que le permita a las autoridades hacer uso de la información captada masivamente, como ocurre en capitales como Londres, donde las autoridades utilizan el reconocimiento facial mediante cámaras públicas para ubicar y hacer seguimiento a delincuentes, como parte de sus estrategias de prevención del delito o de sus planes de contingencia.

Finalmente, en el marco del concepto de ciudad y territorio, y considerando el agua como elemento fundamental para el cumplimiento de los fines del Estado, la ciudad de Bogotá y sus empresas de servicios públicos deberán generar nuevos catastros de usuarios, reales y ajustados al verdadero consumidor. Esto implicará la implementación de tecnologías que no solo midan los consumos en tiempo real, sino que también permitan generar alertas por daños internos en las redes, brindar información en línea a los operadores, entre otras condiciones de operación.

Todo ello con el objetivo de llegar, en los próximos años, a un "estado del arte" donde la tecnología permita evaluar de manera más precisa la estratificación del consumidor y, muy seguramente, implementar un sistema de prepago digital del consumo, dejando en el pasado los procesos de facturación que hoy conocemos bajo el modelo de cuentas contrato.

Como usuarios de los servicios públicos, sabemos que nuestro principal derecho se funda en la correcta medición del consumo. Al respecto, el Consejo de Estado en sus pronunciamientos lo ha analizado, señalando que:

> *"El artículo 9 de la Ley 142 de 1994 estableció como derecho de los usuarios de los servicios públicos domiciliarios, la medición de sus "consumos reales" y obtener información completa sobre todos los aspectos de la prestación del servicio. (...) En la exposición de motivos del proyecto que posteriormente se convertiría en la Ley 142 de 1994, el artículo 9.1 estaba incluido en el capítulo denominado "protección al usuario", y su justificación se formulaba así:*
>
> *"Se garantiza a los usuarios el derecho a usar o no usar los servicios públicos [y] a pagar por ello un precio que tenga relación*

con su consumo". Como claramente se establece en la norma transcrita y en sus antecedentes, el derecho del usuario a la medición de sus consumos reales tiene relación directa con el precio del servicio y comporta la obligación correlativa de la empresa de servicios públicos (en adelante, ESP) de disponer los instrumentos tecnológicos apropiados para realizar dicha medición. El deber de la empresa de medir los consumos hace parte, además, de la prestación misma del servicio, toda vez que la noción legal de cada uno de los servicios públicos, en particular el de energía eléctrica, incluye la medición. (...)

De conformidad con el citado artículo 9.4, también es un derecho de los usuarios obtener información "completa, precisa y oportuna, sobre todas las actividades y operaciones directas o indirectas que se realicen para la prestación de los servicios públicos", lo cual indiscutiblemente incluye la información sobre la medición del servicio.

Obviamente el derecho de los usuarios se refleja en la obligación correlativa de las ESP de satisfacer tal derecho. La mencionada relación derecho - deber se ve reforzada con lo dispuesto en la Ley Estatutaria 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", cuyo objeto es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información (artículo 1)"[10], pero en parte alguna se menciona los mecanismos de la medición, no el medidor como tal, sino del proceso de medición, por lo que las empresas podrán iniciar el tránsito al uso de nuevas tecnologías en dichos procesos, momento en el cual nos veremos avocados a la formulación de nuevos acuerdos sobre el uso de la información personal.

Este breve estudio ha buscado presentar una aproximación inicial a la compleja relación entre el avance tecnológico y los debates jurisprudenciales en el contexto del desarrollo urbano. La inteligencia artificial, la recopilación masiva de datos y la implementación de tecnologías inteligentes en las ciudades, plantean desafíos urgentes para el Derecho, especialmente en lo relativo a la privacidad, la seguridad y la gestión equitativa de los recursos.

Bogotá, como capital y epicentro de transformación, enfrenta una doble exigencia: por un lado, avanzar en la construcción de una ciudad inteligente que responda a las necesidades de sus ciudadanos; y por otro, garantizar que dicho proceso se realice bajo los principios rectores del Estado Social de Derecho, donde la dignidad humana, la protección de datos personales, el acceso a servicios públicos eficientes y la justicia social sean el eje de toda política pública.

10 Consejo de Estado, Sentencia del 22 de febrero de 2016, Consejero Ponente: Germán Alberto Bulla Escobar, exp. 11001-03-06-000-2014-00259-00(2236).