UNIVERSIDAD DE ANTIOQUIA

La vigilancia digital en Medellín: percepción ciudadana frente al uso de dispositivos y tecnología en el espacio urbano.

Cristian Camilo Echeverry Vega

Trabajo de grado presentado para optar al título de Sociólogo

Asesor

Gabriel Jaime Vélez Cuartas, Doctor (PhD) en Ciencias Políticas y Sociales

Universidad de Antioquia

Facultad de Ciencias Sociales y Humanas

Sociología

Medellín, Antioquia, Colombia

2026

UNIVERSIDAD DE ANTIOQUIA
1803

Cita	(Echeverry Vega, 2026)
Referencia **Estilo APA 7 (2020)**	Echeverry Vega C. C. (2026). *La vigilancia digital en Medellín: percepción ciudadana frente al uso de dispositivos y tecnología en el espacio urbano.* [Trabajo de grado profesional]. Universidad de Antioquia, Medellín, Colombia.



CRAI María Teresa Uribe (Facultad de Ciencias Sociales y Humanas)

Repositorio Institucional: http://bibliotecadigital.udea.edu.co

Universidad de Antioquia - www.udea.edu.co

El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Antioquia ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por los derechos de autor y conexos.

Dedicatoria

A mi familia que siempre ha creído en mí, especialmente a mi hermana Daniela por su infinita incondicionalidad. En ninguna vida encontraré a alguien con una generosidad tan inmensa como la de ella.

Agradecimientos

Mi más sincero agradecimiento a mi asesor de tesis, quien, con su orientación y acompañamiento, brindó la claridad necesaria para encaminar esta investigación en la dirección adecuada. Asimismo, agradezco a los docentes que hicieron parte de mi proceso académico por los conocimientos compartidos y las enseñanzas que contribuyeron a mi formación.

A todas las personas que hicieron parte de mi paso por la universidad, gracias por enriquecer esta experiencia con su compañía, apoyo y aprendizaje. Finalmente, expreso mi gratitud a la gloriosa Universidad de Antioquia por acogerme y brindarme la oportunidad de crecer, tanto en el ámbito académico como en el personal.

Para Laura Sofía, el amor de esta vida.

Tabla de contenido

Resumen 10

Abstract 11

Introducción 12

2 Planteamiento del problema 15

3 Antecedentes 20

4 Objetivos 27

4.1 Objetivo general 27

4.2 Objetivos específicos 27

5 Marco teórico 28

6 Metodología 33

6.2 Diseño de investigación 34

6.3 Instrumento de recolección de información 35

6.4 Población y muestra 36

6.5 Estrategia de análisis de datos 38

6.6 Consideraciones éticas 39

7 Caracterización de la muestra y percepciones generales sobre la vigilancia digital en Medellín 43

7.1 Caracterización sociodemográfica de la muestra 43

7.2 Percepción sobre la presencia de dispositivos de vigilancia en el espacio urbano 47

7.3 Actitudes frente al uso de tecnologías de vigilancia 49

7.4 Percepción sobre el aumento de la vigilancia en la ciudad 50

7.5 Comprensión ciudadana sobre tecnologías de vigilancia 51

8 Gobernabilidad algorítmica y confianza institucional 54

8.1 Confianza institucional: uso de datos y legitimidad 54

8.3 Transparencia institucional: opacidad del sistema 56
8.4 Gobernabilidad algorítmica: aceptación de la automatización 57
8.5 Ciudadanía, datos y control 58
8.6 Análisis de correlaciones: tensiones estructurales 60
8.7 Discusión: la tensión entre tecnología, confianza y ciudadanía 62
9 Derechos, privacidad y agencia ciudadana 64
9.1 Centralidad de la privacidad en la percepción ciudadana 64
9.2 Percepción de riesgo y producción de sospecha 66
9.3 Vigilancia y percepción de exposición 67
9.4 Demanda de control ciudadano sobre los datos 68
9.5 Agencia ciudadana y transformación del comportamiento 69
9.6 Diferencias sociodemográficas en la percepción de la privacidad y la agencia 70
9.7 Discusión: derechos, vigilancia y ciudadanía en tensión. 71
10 Tipologías ciudadanas frente a la vigilancia digital 73
10.1 Metodología de análisis de clusters 73
10.2 Caracterización de las tipologías ciudadanas desde una perspectiva teórica. 75
10.2.1 Ciudadanía legitimadora 76
10.2.2 Ciudadanía crítica 78
10.2.3 Ciudadanía ambivalente 80
10.2.4 Ciudadanía pasiva 81
10.3 Discusión teórica: tipologías y gobernabilidad algorítmica 83
11 Aporte de la investigación 84
12 Conclusiones 85
13 Recomendaciones 88
Referencias 89

Anexos.....94

Lista de tablas

Tabla 1 Distribución de la muestra según rango de edad....44

Tabla 2 Distribución de la muestra según identidad de género....45

Tabla 3 Distribución de la muestra según nivel educativo....46

Tabla 4 Distribución de la muestra según estrato socioeconómico....47

Tabla 5 Percepción de exposición a cámaras de vigilancia en Medellín 48

Tabla 6 Percepción sobre la efectividad de las cámaras en la seguridad 50

Tabla 7 Percepción de incremento de la vigilancia en los últimos años 51

Tabla 8 Nivel de comprensión sobre sistemas de reconocimiento facial....52

Tabla 9 Correlación de índice de desarrollo tecnológico e índice de ciudadanía 61

Tabla 10 Correlación de índice de sensación de vigilancia y ser considerado sospechoso por la información recopilada.....61

Tabla 11 Percepción de vigilancia vs preocupación por ser considerado sospechoso 67

Tabla 12 Diferencias entre percepción de privacidad según variable de edad....70

Tabla 13 Relación del nivel educativo con la capacidad de agencia....71

Tabla 14 Medias por cluster 73

Tabla 15 Relación entre tipologías ciudadanas y percepción de afectación a la privacidad....77

Tabla 16 Relación entre tipologías ciudadanas y niveles de confianza institucional en el uso de datos 78

Tabla 17 Relación entre tipologías ciudadanas y percepción de intensificación de la vigilancia.81

Lista de Figuras

Figura 1 Confianza institucional 55

Figura 2 Transparencia institucional 56

Figura 3 Percepción sobre el uso de tecnologías vs actuar de la policía 57

Figura 4 Percepción sobre automatización de la seguridad en Medellín 58

Figura 5 Relación entre veeduría ciudadana y protección de datos 59

Figura 6 Preocupación por ser considerado sospechoso vs datos personales 60

Figura 7 Importancia de la protección de los datos 64

Figura 8 Afectación de la privacidad por presencia de cámaras de vigilancia 65

Figura 9 Preocupación por el riesgo de ser señalado o parecer sospechoso 66

Figura 10 Veeduría ciudadana requerida por la ciudadanía 68

Figura 11 Tecnologías de vigilancia y limitación del comportamiento 69

Figura 12 Perfiles de las tipologías ciudadanas según índices estandarizados 75

Siglas, acrónimos y abreviaturas

CCTV	Circuito Cerrado de Televisión
CIS	Centro de Investigaciones Sociológicas (España)
CTI	Ciencia, Tecnología e Innovación
DANE	Departamento Administrativo Nacional de Estadística
DNI	Documento Nacional de Identidad
ENVIPE	Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública
IA	Inteligencia Artificial
IUIPC	Internet Users' Information Privacy Concerns
LPR	License Plate Recognition
PMI	Puntos de Monitoreo Inteligente
PTZ	Pan Tilt Zoom
SIES-M	Sistema Integrado de Emergencias y Seguridad Metropolitano
SNCTeI	Sistema Nacional de Ciencia, Tecnología e Innovación
TRF	Tecnología de Reconocimiento Facial

Resumen

Esta investigación analiza la percepción ciudadana sobre la vigilancia digital en Medellín, con énfasis en el uso de tecnologías como cámaras de seguridad, inteligencia artificial y reconocimiento facial en el espacio urbano. El estudio se enmarca en el campo de la sociología de la vigilancia y la gobernabilidad algorítmica, con el objetivo de comprender cómo los ciudadanos interpretan estas tecnologías, qué niveles de confianza institucional manifiestan y qué implicaciones perciben en términos de derechos, privacidad y comportamiento.

Metodológicamente, se empleó un enfoque cuantitativo basado en la aplicación de una encuesta a 217 participantes. Los datos fueron analizados mediante estadística descriptiva, correlacional y análisis de conglomerados utilizando SPSS, lo que permitió identificar patrones de percepción y construir tipologías ciudadanas.

Los resultados evidencian una relación ambivalente frente a la vigilancia digital: por un lado, se observa una aceptación significativa de las tecnologías como herramientas para mejorar la seguridad; por otro, emergen altos niveles de desconfianza institucional, preocupaciones sobre el uso de datos personales y demandas de mayor transparencia y control ciudadano. Asimismo, se identifican efectos diferenciados en la agencia, evidenciando que la vigilancia influye en el comportamiento de algunos individuos, mientras que otros no perciben cambios en su actuar cotidiano.

A partir del análisis de conglomerados, se construyen cuatro tipologías ciudadanas: ciudadanía legitimadora, crítica, ambivalente y pasiva, lo que permite comprender la heterogeneidad de posiciones frente a la vigilancia digital. En conjunto, los hallazgos sugieren que la gobernabilidad algorítmica no produce una ciudadanía homogénea, sino múltiples formas de relación con el control tecnológico.

La investigación concluye que la legitimidad de la vigilancia digital no depende únicamente de su eficacia técnica, sino de su articulación con la confianza institucional, la transparencia y la protección de los derechos ciudadanos.

Palabras clave: Vigilancia digital, Gobernabilidad algorítmica, Ciudadanía, Privacidad, Datos personales, Confianza institucional, Seguridad urbana

Abstract

This research analyzes citizens' perceptions of digital surveillance in Medellín, focusing on the use of technologies such as CCTV systems, artificial intelligence, and facial recognition in urban spaces. The study is framed within the sociology of surveillance and algorithmic governance, aiming to understand how citizens interpret these technologies, their levels of institutional trust, and the perceived implications for rights, privacy, and behavior.

Methodologically, a quantitative approach was employed through a survey administered to 217 participants. Data were analyzed using descriptive statistics, correlation analysis, and cluster analysis in SPSS, allowing for the identification of perception patterns and the construction of citizen typologies.

The findings reveal an ambivalent relationship with digital surveillance: on the one hand, there is significant acceptance of these technologies as tools for improving security; on the other hand, there are high levels of institutional distrust, concerns regarding personal data use, and demands for greater transparency and citizen oversight. Additionally, differentiated effects on agency were identified, showing that surveillance influences the behavior of some individuals, while others do not perceive changes in their daily actions.

Through cluster analysis, four citizen typologies were identified: legitimizing, critical, ambivalent, and passive citizenship. These typologies highlight the heterogeneity of positions regarding digital surveillance. Overall, the results suggest that algorithmic governance does not produce a homogeneous citizenry, but rather multiple forms of engagement with technological control.

The study concludes that the legitimacy of digital surveillance depends not only on its technical effectiveness but also on its alignment with institutional trust, transparency, and the protection of citizens' rights.

Keywords: Digital surveillance, Algorithmic governance, Citizenship, Privacy, Personal data, Institutional trust, Urban security.

Introducción

En las últimas décadas, las ciudades latinoamericanas han incorporado de manera creciente tecnologías digitales en el diseño y ejecución de sus políticas de seguridad urbana. Cámaras de videovigilancia, sistemas de reconocimiento facial, analítica de datos y plataformas de monitoreo en tiempo real se han convertido en dispositivos centrales de lo que se presenta institucionalmente como modernización, eficiencia y gestión inteligente del territorio. En este contexto, Medellín, reconocida internacionalmente por su apuesta por la innovación y la transformación urbana, ha desplegado una infraestructura tecnológica orientada a fortalecer la seguridad ciudadana mediante herramientas de vigilancia digital.

Sin embargo, más allá de su dimensión técnica, estos dispositivos configuran nuevas formas de relación entre el Estado y la ciudadanía. La incorporación de inteligencia artificial, automatización de procesos policiales y recolección masiva de datos personales no solo transforma la manera en que se administra el orden público, sino que también reconfigura las experiencias cotidianas en el espacio urbano. En este escenario, la vigilancia deja de ser exclusivamente un mecanismo visible de control para convertirse en un entramado algorítmico que opera de manera difusa, permanente y, en muchos casos, poco transparente.

Desde una perspectiva sociológica crítica, estas transformaciones pueden comprenderse en el marco de lo que diversos autores han denominado sociedad de la vigilancia, gubernamentalidad algorítmica o capitalismo de datos. Estas categorías permiten analizar cómo el poder contemporáneo no se ejerce únicamente a través de la coerción directa, sino mediante dispositivos técnicos que producen información, clasifican sujetos y orientan comportamientos. La ciudad se convierte así en un laboratorio de experimentación tecnológica donde seguridad, innovación y gobernabilidad convergen en un mismo discurso legitimador.

No obstante, la implementación de estas tecnologías no ocurre en un vacío social. Se despliega en un contexto marcado por desigualdades históricas, desconfianza institucional y tensiones democráticas propias del Sur Global. En Medellín, ciudad atravesada por procesos complejos de violencia, estigmatización territorial y transformación urbana, la expansión de la vigilancia digital plantea interrogantes fundamentales sobre el ejercicio de la ciudadanía, la protección de derechos y la distribución del poder en el espacio público.

La presente investigación parte de una pregunta central: ¿cómo perciben los habitantes de Medellín el uso de tecnologías de vigilancia digital implementadas en el marco de las políticas de seguridad urbana y qué tensiones emergen entre la innovación tecnológica y el ejercicio de la ciudadanía? Más que medir niveles de aprobación o rechazo, el estudio busca comprender las formas en que los ciudadanos interpretan, legitiman, problematizan o resignifican estos dispositivos en su vida cotidiana.

El objetivo general es explorar las percepciones de los habitantes de Medellín frente al uso de dispositivos de vigilancia digital, con el fin de analizar cómo dichas percepciones evidencian tensiones entre seguridad, innovación y derechos ciudadanos. Para ello, se diseñó y aplicó una encuesta estructurada a 217 personas que transitan por la ciudad, permitiendo construir índices analíticos sobre desarrollo tecnológico, gobernabilidad algorítmica y ciudadanía, así como identificar tipologías diferenciadas de posicionamiento frente a la vigilancia.

Metodológicamente, el estudio combina estadística descriptiva, análisis de correlación y segmentación mediante análisis de clúster, con el propósito de superar una lectura meramente porcentual y avanzar hacia una interpretación sociológica de las configuraciones de ciudadanía emergentes. Esta metodología de análisis permite no solo identificar tendencias generales, sino también explorar cómo dichas percepciones se distribuyen socialmente y qué perfiles ciudadanos se configuran en torno a la vigilancia digital.

La tesis que orienta este trabajo sostiene que, en Medellín, la vigilancia digital es percibida de manera ambivalente: mientras una parte significativa de la ciudadanía legitima su uso en nombre de la seguridad y el progreso tecnológico, emergen simultáneamente preocupaciones relacionadas con la privacidad, el uso de datos personales, el sesgo algorítmico y la transparencia institucional. Esta ambivalencia no es homogénea, sino que se distribuye socialmente, configurando tipologías diferenciadas de ciudadanía frente al gobierno algorítmico de la ciudad.

La investigación se estructura en seis capítulos. El primero desarrolla el marco teórico sobre vigilancia, poder y gubernamentalidad algorítmica. El segundo presenta el diseño metodológico y las decisiones analíticas adoptadas. Los capítulos tercero, cuarto y quinto exponen los resultados empíricos en torno a percepción general, legitimidad tecnológica y tensiones con los derechos ciudadanos. El sexto capítulo profundiza en la diferenciación social de estas percepciones mediante la construcción de tipologías ciudadanas. Finalmente, se presentan las conclusiones y aportes al debate sobre gobernabilidad urbana en contextos de innovación tecnológica.

En este escenario, la expansión de los sistemas de vigilancia con Inteligencia Artificial no es un fenómeno aislado de Medellín, sino parte de una lucha transnacional por instaurar salvaguardas que respeten la privacidad y el acceso igualitario a la justicia (Feldstein et al., 2022). Como señala Osaba (2015), estas asimetrías de poder entre el Estado y el ciudadano común ponen en riesgo la esencia misma de la democracia si no existe una supervisión ética y una rendición de cuentas clara sobre el alcance de estos sistemas.

2 Planteamiento del problema

En las últimas dos décadas, Medellín se ha consolidado como un referente de innovación urbana en América Latina, al punto de ser declarada en 2021 como Distrito Especial de Ciencia, Tecnología e Innovación mediante el Acto Legislativo 01 de 202, donde se dota a la ciudad con los instrumentos jurídicos y competencias para su organización como Distrito.

> Este gran cambio para la entidad territorial se da por el reconocimiento de la vocación de la ciudad a partir del crecimiento y desarrollo diferenciado frente a los demás municipios, avanzando en un proceso de transformación social, económica y ambiental, que enfoca sus esfuerzos para encontrar en la ciencia, tecnología e innovación, soluciones a grandes problemáticas de la ciudad en temas como seguridad, habitabilidad, salud, equidad y manejo del medio ambiente, entre otros. (Alcaldía de Medellín, s.f. párr. 2)

Esta reglamentación da a la capital antioqueña el acceso a recursos directos y sin intermediarios para promover el desarrollo tecnológico en la ciudad. Esta designación ha potenciado la implementación de políticas públicas orientadas a la transformación digital y la gestión de datos, con el propósito de impulsar el desarrollo económico y social de la ciudad. Es así que, desde el 16 de enero del 2023, luego de sancionada la ley por parte del presidente Petro, en la ciudad es posible definir "Zonas de Tratamiento Especial", espacios utilizados no solo para desarrollar cualquier actividad enfocada en Ciencia, Tecnología e Innovación sino para ofrecer accesibilidad y renovación urbana en temas de ciencia y tecnología. Gracias a esto, el Distrito podría desarrollar las diferentes políticas y programas necesarios para potenciar las capacidades y la transformación en esa materia, así mismo dota a la ciudad de otros instrumentos como la Estampilla Pro-Innovación y el Fondo Distrital de CTI[1] que, aunque no constituyen una política de seguridad, si habilitan y financian las capacidades tecnológicas de diferentes dependencias distritales, como es el caso de la Secretaría de Seguridad y Convivencia (Función pública, 2023), que si hace parte de la política de seguridad de Medellín y que se encuentra bajo la jurisdicción de dicha Secretaría. Estas capacidades, si bien no se derivan automáticamente del régimen CTI, si

[1] CTI: Ciencia, Tecnología e Innovación.

encajan en la orientación a la transformación digital y el uso intensivo de datos públicos, para la seguridad en el espacio público, entendido como aquellos lugares de dominio, propiedad y uso del público en general, como calles, parques, carreteras, edificios, aeropuertos, escenarios deportivos, entre otros. Es así que, de manera paralela, la Secretaría de Seguridad y Convivencia ha incorporado parte de estas capacidades de desarrollo tecnológico, entendido como el despliegue de infraestructuras, dispositivos y sistemas de datos asociados a la innovación digital. Como advierte Feenberg (1999), la tecnología no es neutra, sino que encarna valores y decisiones políticas que moldean la organización social enmarcados en narrativas de progreso y modernización, lo que en el caso de Medellín se refleja en el uso de cámaras inteligentes y plataformas de vigilancia bajo la promesa de eficiencia y seguridad; tal cómo se expone en la investigación de Al Sur[2], en la que buscaban verificar el estado de 38 iniciativas reportadas en el 2021 por 9 países de la región, incluido Colombia, enfocado en conocer información sobre los proveedores de tecnologías de vigilancia, en la cual "se centró en sistemas de reconocimiento facial implementados en políticas públicas, especialmente aquellos destinados a la vigilancia del espacio público y la autentificación de identidad" (Ibarreche et al., 2025), planteando un dilema ético. Esta convergencia plantea una tensión fundamental: mientras la narrativa institucional enmarca la ciencia y la tecnología como motores de progreso y modernización, su uso en la seguridad urbana abre interrogantes sobre la protección de derechos fundamentales, la transparencia de las decisiones gubernamentales y la manera en que la ciudadanía percibe y experimenta estas tecnologías en su vida cotidiana.

En Medellín se cuenta con más de 3.200 cámaras con diversas funcionalidades y tecnologías para el control integral del territorio. Se destacan 2.068 cámaras Pan Tilt Zoom (PTZ), capaces de rotar en ejes horizontal y vertical y realizar acercamientos o alejamientos; 562 cámaras de reconocimiento de placas (LPR), diseñadas para identificar vehículos reportados como hurtados o vinculados a actividades delictivas; y 327 cámaras multisensor, con cobertura de 360° que garantizan el monitoreo de todos los alrededores desde un único punto. A estas se suman 156 cámaras fijas de alta resolución, instaladas estratégicamente para vigilancia constante; 80 cámaras de reconocimiento facial, que identifican personas previamente enroladas en bases de datos; y 37 cámaras analíticas, especializadas en la detección de objetos abandonados, cruces indebidos de líneas, aglomeraciones y otras situaciones de riesgo.

[2] "Al Sur" es un consorcio de 11 organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región.

Tipo de Cámara	Función principal
Cámaras Salva Vidas (fotodetección)	Detectar exceso de velocidad e infracciones viales
Cámaras LPR	Reconocimiento automático de placas vehiculares
Cámaras multisensor 360°	Vigilancia amplia con seguimiento inteligente
Cámaras inteligentes	Expansión del sistema con nuevas cámaras en múltiples puntos
Video Wall de monitoreo (SIES-M)	Centro de visualización unificado y modernizado

Si bien la expansión de dispositivos de videovigilancia en Medellín se presenta en los discursos oficiales como un mecanismo para mejorar la seguridad ciudadana y garantizar el bienestar colectivo, y que además son justificados a través de los informes públicos de la Secretaría de Seguridad y Convivencia como un mecanismo indispensable para reducir el delito y garantizar el bienestar colectivo. Informes oficiales y comunicados de prensa destacan cifras de capturas, recuperación de objetos hurtados y eficiencia operativa. Esta narrativa entra en tensión cuando se observa cómo circula el tema en la opinión pública, la sociedad civil y en los debates jurídicos. En redes sociales y medios locales, no son pocos los cuestionamientos sobre la eficacia de estas tecnologías frente a problemas estructurales de inseguridad, así como sobre el riesgo de vulneración de derechos fundamentales como la privacidad y la protección de datos personales —incluidas la Ley 1266 de 2008 y la Ley 1581 de 2012 sobre protección de datos personales— que establece límites al uso de información sensible, lo que genera interrogantes sobre si la implementación de sistemas de reconocimiento facial o de algoritmos predictivos cumple con dichos estándares. Casos concretos, como la controversia por la plataforma Medellín Me Cuida, que recogió datos personales de cientos de ciudadanos recolectados inicialmente con fines de salud pública durante emergencia sanitaria por COVID-19, pero que luego fueron reutilizados en campañas informativas sin claridad suficiente sobre el consentimiento informado, los datos no fueron eliminados en los plazos anunciados, entre otras situaciones que generaron malestar y denuncias por el presunto uso indebido de datos (Caracol Radio, 2022). En redes sociales y medios locales se ha registrado la molestia de varios ciudadanos que recibieron mensajes de la Alcaldía a través de datos suministrados para otro propósito, sin tener certeza de haber autorizado ese uso o de haber recibido información completa del tratamiento de sus datos, de modo que algunas funcionalidades no

parecen estar claramente justificadas en la emergencia epidemiológica que motivó su creación (Fundación Karisma, 2020).

En estudios regionales sobre reconocimiento facial, se destaca que la utilización de sistemas biométricos en el espacio público tiende a producir ajustes mínimos a los derechos fundamentales, con escasa evaluación de impacto, mecanismos de auditoría débiles y muy poca deliberación social (Venturini & Garay, 2021). De esta manera, más allá de la promesa técnica de control y eficiencia, lo problemático radica en las contradicciones entre los objetivos institucionales, la percepción ciudadana y las garantías jurídicas, lo que evidencia la necesidad de un análisis sociológico más riguroso sobre los alcances del gobierno algorítmico en la ciudad, que a través de la captura y procesamiento de grandes volúmenes de datos conlleva a orientar la toma de decisiones públicas. Según Rouvroy y Berns (2013), este tipo de gubernamentalidad reemplaza la norma jurídica por la modulación algorítmica de conductas, generando nuevas tensiones sobre transparencia, sesgos y control social.

Sin embargo, estas transformaciones suscitan interrogantes clave sobre los límites entre la seguridad, la privacidad y la libertad individual. Estas preguntas no son meramente teóricas: en Medellín el despliegue de sistemas de reconocimiento facial y de videovigilancia inteligente ha sido cuestionado por organizaciones de derechos digitales que alertan sobre los riesgos de sesgo y de afectación a derechos fundamentales sin suficiente control ciudadano o institucional (Venturini & Garay, 2021). Incluso, en escenarios políticos, el debate sobre el modelo de seguridad en la ciudad ha enfrentado a sectores que justifican estas tecnologías como garantes de eficacia policial frente a otros que señalan un déficit de participación y un posible exceso de control estatal (El Colombiano, 2023).

A pesar de estas discusiones puntuales, la indagación empírica sobre cómo los ciudadanos de Medellín interpretan y experimentan estos procesos en su vida cotidiana sigue siendo escasa. Existe también un vacío en el análisis crítico de los modelos de vigilancia digital que se han consolidado bajo el amparo de la condición de la ciudad como Distrito Especial de Ciencia, Tecnología e Innovación, lo cual hace necesario explorar no solo la infraestructura tecnológica, sino también su percepción y tensiones subjetivas que emergen en la ciudadanía desde su implementación.

Explorar la manera en que la ciudadanía de Medellín tanto habitantes como visitantes perciben el uso de tecnologías y dispositivos de vigilancia, permite atender tanto a los imaginarios

sociales que circulan sobre la seguridad como a los posibles efectos sobre el ejercicio de la libertad y los derechos civiles. Tal como plantea Isin (2009), la ciudadanía implica actos de agencia mediante los cuales los sujetos aceptan, resisten o resignifican los marcos de gobierno que los afectan. En el campo internacional de los estudios sociales de la ciencia y la tecnología, múltiples investigaciones han mostrado que la percepción ciudadana frente a dispositivos de vigilancia oscila entre la aceptación pragmática en nombre de la seguridad y la desconfianza ante el riesgo de afectación de derechos (Lyon, 2018; Zuboff, 2019). No obstante, en Medellín este tipo de análisis sigue siendo incipiente y fragmentario.

Estudiar estos mecanismos de control en la vida urbana moderna, desde el panoptismo foucaultiano hasta las sociedades de control que plantea Deleuze, permite pensar en la relación de Medellín, el despliegue de tecnologías y dispositivos de vigilancia y en como la ciudad constituye un laboratorio donde estas teorías cobran vigencia, con la manera en la que los ciudadanos interpretan estas formas de vigilancia. Con el fin de vislumbrar cómo se reconfigura el control social en el contexto urbano local y así comprender las percepciones ciudadanas frente a: si estas tecnologías son legitimadas, resistidas o resignificadas por los habitantes.

En este sentido, esta investigación busca llenar dicho vacío empírico y contribuir a la comprensión crítica del fenómeno, articulando debates teóricos sobre la gobernabilidad algorítmica con la experiencia subjetiva de los ciudadanos frente a la vigilancia digital. De ahí se deriva la siguiente pregunta de investigación: *¿Qué percepciones tienen los habitantes de Medellín sobre el uso de dispositivos de vigilancia digital implementados como parte de las políticas de seguridad urbana, y cómo estas percepciones reflejan tensiones entre la innovación tecnológica y el ejercicio de la ciudadanía en el espacio público?*

3 Antecedentes

La investigación propuesta, enfocada en la vigilancia digital en Medellín y la percepción ciudadana frente a la seguridad y la libertad, se inscribe en varios campos académicos relacionados con estudios sociológicos y politológicos que aborda la proliferación de tecnologías de control. La revisión de la literatura permite establecer un marco conceptual que se ubica en torno a las tecnologías de vigilancia, los discursos de legitimación institucional, la manera en la evolucionan los modelos de control social y la tensión fundamental entre la seguridad pública y los derechos ciudadanos. La robustez de los resultados y conclusiones en este campo de estudio proviene de una combinación de metodologías cualitativas, análisis documental, y estudios de caso específicos.

La metodología para abordar la evolución de los modelos de control social y conceptualizar el paso de las sociedades disciplinarias a las sociedades de vigilancia requiere de una indagación teórica y bibliográfica (García Martín, 2017) que toma como punto central el Panóptico de Jeremy Bentham y lo relaciona con conceptos contemporáneos como el ban-opticón (Ragnedda, 2011) o la biopolítica avanzada (Castro Orellana, 2009). Este enfoque teórico es esencial para analizar el tránsito hacia la gubernamentalidad algorítmica, que redefine el ordenamiento social a través de procedimientos epistémicos computarizados. En el ámbito del derecho comparado, Gil Márquez (2004) analiza cómo los sistemas de seguridad pública deben equilibrar la eficacia policial con el respeto absoluto a los derechos fundamentales consagrados en las constituciones democráticas. Por su parte, Barcelona Llop (2012) advierte que la videovigilancia no tiene la misma naturaleza en un Estado democrático que en uno autoritario, subrayando que su legitimidad depende de una exigencia acentuada de compatibilidad con el libre ejercicio de las libertades públicas. A nivel regional, Pérez Esquivel (2021) examina el caso de Buenos Aires, señalando que la videovigilancia automatizada busca a menudo convertir en 'sospechosos vitalicios' a todos los ciudadanos bajo una lógica de prevención anticipatoria.

Así mismo, estudiar los discursos de legitimación institucional se ha sustentado en el análisis de contenido de documentos oficiales. Como en el caso del texto de Jasso López (2018), cuyo estudio se definió como principalmente cualitativo y analizó Planes de Desarrollo en México con apoyo del software de análisis cualitativo NVIVO para describir y elaborar conclusiones sobre la política pública de videovigilancia. De manera más específica en el caso local, Londoño Osorio y Guerrero-C. (2024), utilizaron una ruta metodológica cualitativa que incluyó la sistematización

y el contraste del discurso oficial (planes de desarrollo, videos institucionales de la alcaldía) con la información de prensa y veeduría, considerando los videos institucionales como fuente fundamental para analizar la configuración del "teatro tecnológico de la vigilancia".

Esta espectacularidad del sistema local exige analizarlo no solo como un despliegue técnico, sino bajo la lupa del derecho comparado. El marco jurídico para el uso de estas tecnologías no es neutral; como sostiene Ull Salcedo (2005), el derecho a la intimidad constituye un límite infranqueable que exige subordinar la vigilancia al principio de proporcionalidad e idoneidad, evitando que la lógica de prevención anticipatoria convierta a los ciudadanos en 'sospechosos vitalicios' (Pérez Esquivel, 2021).

Para examinar la tensión fundamental entre la seguridad pública y los derechos ciudadanos, mientras el abordaje se realiza principalmente mediante el análisis legal y dogmático, en el caso del texto de Bilbao (2016), donde se estudió la instalación de cámaras por parte de las Fuerzas y Cuerpos de Seguridad, está sujeta a la valoración obligatoria del principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. A diferencia de lo expuesto en el texto de Malamud (2018) que analizó la doctrina emanada de las cortes chilenas en casos de videovigilancia avanzada (como "Globos" y "Drones") para problematizar la ausencia del examen de proporcionalidad.

La dimensión empírica de la vigilancia se ha nutrido de investigaciones de campo y estudios de caso cualitativos. En el texto de Arteaga Botello (2010), cuyo trabajo de investigación se realizó durante 2006 y 2007 e incluyó entrevistas al supervisor general y al operador del sistema de videovigilancia en Tlalnepantla para analizar la evolución de los CCTV y su orientación al control social y político, encontrando que el uso del sistema de CCTV va más allá de la prevención del delito con una clara orientación al control y la gestión poblacional a través del procesamiento de datos. Asimismo, en el texto de Lío (2020), que utilizó un diseño metodológico cualitativo que combinó entrevistas en profundidad con actores involucrados y notas de campo tomadas a partir de observaciones para indagar en las funciones, límites y efectividad de la videovigilancia en Argentina. La investigación indagó en los modos en que las tecnologías interactúan con los actores humanos y no-humanos, delineando las posibilidades y límites de estos sistemas de monitoreo urbano, según este estudio, A pesar de la falta de evidencia concluyente de reducción del delito y las fallas operativas, la videovigilancia se mantiene y expande porque se convierte en un "punto de paso obligado" para el diseño de políticas de seguridad pública.

En términos generales, la literatura empírica internacional y regional muestra tres rasgos recurrentes en sus análisis, el primero es que la percepción ciudadana es ambivalente, Galdon-Clavell (2015) se basó empíricamente en los datos del Centro de Investigaciones Sociológicas (CIS) de España, que demostró que el 68.7% de la población apoya la videovigilancia porque les da seguridad, mientras que solo una minoría del 10% de la población total manifiesta un rechazo. Es dentro de este grupo opositor donde la preocupación por la pérdida de privacidad es determinante, siendo la razón principal para el 79.4% de quienes rechazan el sistema (Galdon-Clavell, 2015). Esta coexistencia de aceptación y rechazo es intrínseca a la tecnología, es decir, coexisten aceptación pragmática por razones de seguridad e inquietud por la privacidad; en segundo lugar las evaluaciones dependen de manera exponencial del contexto como en el caso del texto de Lio (2020), que utilizó un diseño metodológico cualitativo basado en entrevistas en profundidad y observación en Argentina, con este método encontró que, ante la falta de evidencia empírica de efectividad en la reducción del delito, los defensores del sistema recurren a la dimensión subjetiva (el sentimiento de inseguridad) para redefinir la eficacia de las cámaras (Lio, 2020), es decir, debido a un evento reciente, como se está moviendo el clima político y/o por el grado de confianza en la institucionalidad; y tercero desde la institucionalidad por la falta de confianza y transparencia que proyectan a la ciudadanía al momento de realizar la rendición de cuentas y de mostrar evidencias sobre los impactos reales, lo que deja el camino abierto para el análisis empírico local. Este debate entre seguridad y privacidad sugiere una falsa dicotomía, pues la vigilancia y captación de imágenes, aunque se produzca en lugares públicos, no es una actividad neutra y afecta los derechos fundamentales (De la Serna Bilbao, 2016; Parrilli, 2013).

En el ámbito del derecho comparado, Gil Márquez (2004) analiza cómo los sistemas de seguridad pública deben equilibrar la eficacia policial con el respeto absoluto a los derechos fundamentales consagrados en las constituciones democráticas. Por su parte, Barcelona Llop (2012) advierte que la videovigilancia no tiene la misma naturaleza en un Estado democrático que en uno autoritario, subrayando que su legitimidad depende de una exigencia acentuada de compatibilidad con el libre ejercicio de las libertades públicas. A nivel regional, Pérez Esquivel (2021) examina el caso de Buenos Aires, señalando que la videovigilancia automatizada busca a menudo convertir en “sospechosos vitalicios” a todos los ciudadanos bajo una lógica de prevención anticipatoria.

Otros estudios con un alcance a gran escala utilizan metodologías cuantitativas, cómo por ejemplo encuestas de opinión realizadas por instituciones como Pew Research Center, que se ha encargado por años de medir la temperatura publica respecto a la vigilancia y la privacidad, mostrando diferenciaciones a nivel sociodemográfico en datos como la edad, nivel educativo y la confianza en las instituciones (Pew Research Center, 2019). En el ámbito académico, instrumentos adaptados y utilizados en diversos contextos, como el IUIPC (Internet Users' Information Privacy Concerns — Malhotra, Kim & Agarwal, 2004) o escalas sobre *trust y perceived surveillance* para capturar sensibilidad hacia el manejo de datos y la aceptación de instrumentos tecnológicos. Estos instrumentos ofrecen ítems validados sobre la preocupación por la privacidad, la percepción de control sobre los datos, percepción de beneficio y confianza en las autoridades y las empresas.

Encuestas realizadas por el Centro de Investigaciones Sociológicas (CIS) en España (2008, 2009 y 2011) indican un elevado nivel de apoyo al uso de cámaras, presentándose como resultado la aceptación por el uso de estas. Los resultados de 2009 revelaron que el 68.7% de la población española apoya la videovigilancia (Galdon-Clavell, 2015). Las principales motivaciones para este apoyo son que las cámaras proporcionan seguridad (66.4%), permiten la identificación de delincuentes (18%) y funcionan como prevención del delito (15.2%) (Galdon-Clavell, 2015). Empero, el 79.4% del 10% de los encuestados que rechaza las cámaras, lo hacen principalmente por la pérdida de privacidad (Galdon-Clavell, 2015). Dicha aceptación y oposición con sus distintas motivaciones varían, según la ubicación de los dispositivos de videovigilancia; en el caso de los bancos, hospitales e instituciones educativas es desde donde hay un mayor apoyo, mientras que en espacio de ocio como bares, restaurantes y espacios públicos tienen un apoyo significativamente menor.

En México la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) muestra que el 74.3% de los mexicanos se siente inseguro, y el 42% de los hogares ha adoptado medidas de protección, incluyendo la instalación de videovigilancia (Jasso López, 2018). En el ámbito de la participación cívica en línea, estudios comparativos con jóvenes universitarios de México y Perú con muestras de 1.239 y 720 encuestados, respectivamente, han demostrado una relación positiva entre el capital social, el sentimiento de eficacia política y la participación en línea (Santiago et al, 2019). Ahora bien, en contraste, las revisiones de evaluaciones internaciones reafirman que los sistemas de videovigilancia en el espacio público pueden reducir la delincuencia, pero de manera desigual (Galdon-Clavel, 2015), puesto que la reducción es mayor en lugares de

poca actividad social y control informal, como en estacionamientos aislados, que en los centros urbanos. Estudios también sugieren que el impacto es mayor cuando existen carteles indicativos, pues tienen un efecto disuasorio (Lio, 2020).

Ciertas categorías delictivas, como los delitos violentos y la delincuencia contra las personas, con frecuencia no se ven alteradas por la presencia de cámaras (Galdon-Clavell, 2015). Además, las cifras de disminución de ilícitos relacionadas con zonas donde se han instalado sistemas de videovigilancia suelen rondar el 4%, una tasa bastante baja y que no permite concluir que la reducción es una consecuencia directa de la instalación de cámaras. En el caso de Argentina, debido a la falta de evidencia empírica por la falta de estudios y evidencia, los defensores de los sistemas recurren a la dimensión subjetiva, redefiniendo la efectividad en términos de la reducción del sentimiento de inseguridad (Lio, 2020). Particularmente en el municipio de Tigre, aunque los datos fueron generados por un conglomerado de aseguradoras (CESVI) sugieren una disminución en robos y hurtos automotores, persiste la falta de estudios que permitan conocer el impacto a nivel nacional (Lio, 2020).

También se han utilizado una combinación de encuestas representativas presenciales u *online* para medir prevalencias y correlaciones, también entrevistas cualitativas y *focus groups* para identificar matices a través de marcos interpretativos, análisis de medios y redes sociales para trazar la agenda pública y las narrativas institucionales y, otros estudios más técnicos miden la percepción a través de la evaluación de la misma tecnología y sus funcionalidades por ejemplo, una cámara usa tecnología de reconocimiento facial, mientras que otra solo graba imágenes y cuya comparación cambia la percepción del ciudadano (Londoño Osorio, I. S., & Guerrero-C., J, 2024). Vale la pena destacar que en general la combinación de metodologías que más predomina, de acuerdo a las investigaciones estudiadas, es la encuesta y los grupos focales siempre que estos estudios buscan medir la temperatura pública en factores como la aceptación, resignificación y el rechazo a los dispositivos de vigilancia (Galdon-Clavell, 2015).

Los estudios actuales han evolucionado para analizar como la ratificación y la gobernanza algorítmica están transformando la vigilancia, superando la tecnología de Circuito Cerrado de Televisión (CCTV) tradicional (Domínguez González & Domínguez Sánchez-Pinilla, 2023), ya que las tecnologías avanzadas, como el reconocimiento facial (TRF), requieren alto estándares técnicos e implementan *video analytics* para detectar automáticamente patrones y monitorear más imágenes con menos operadores (Vizcaíno, 2020). Esta vigilancia algorítmica busca traducir el

contexto social a procesos computable para clasificar a los ciudadanos según dimensiones específicas, como tipos psicométricos, estados emocionales o preferencias políticas (Katzenbach y Ulbricht, 2022), con el objetivo de predecir y modificar comportamientos considerados socialmente sospechosos. Por lo tanto, las dinámicas operativas de videovigilancia se vinculan con el concepto de "teatro de la vigilancia" (Londoño, 2024), donde la tecnología se despliega con fines de espectáculo y discurso político para reconfigurar la percepción ciudadana del espacio, a menudo enfocándose en la persecución de "incivilidades" en ligar de delitos graves, para validar el sistema ante el público; que en la modernidad opera como un "ensamblaje de vigilancia" (Londoño, 2024) donde se acoplan formas de vigilancia (bases de datos, call centers, sistemas de control de tráfico, y equipos biométricos) que funcionan de forma unificada como una "entidad funcional"(Arteaga,2010), lo que les permite extender su función inicial de apoyo al tránsito hacia el control social y político, especialmente monitoreando movilizaciones de protesta (Arteaga,2010).

En el caso específico de la ciudad de Medellín, la evidencia existente es mayormente no académica, se encuentra en informes de organizaciones civiles, notas de prensa, comunicaciones oficiales y documentación propia del SIES-M (Londoño, 2024). Esta realidad pone en evidencia que la investigación en el ámbito nacional sobre el sistema de vigilancia con cámaras, desde la perspectiva de Estudios de Ciencia, Tecnología y Sociedad (CTS), ha sido escasa. Por lo tanto, el análisis de las fuentes no académicas, contrastando el discurso oficial relacionado con los planes de desarrollo y seguridad, con la información de la prensa y la veeduría de organizaciones civiles como Medellín cómo Vamos, resulta crítico para obtener una visión amplia del sistema.

Lo que es interesante en el sentido del uso de metodologías de análisis que permitan desde una mirada académica estudiar el espectro de la ciudad de Medellín, es que la integración de actores y artefactos del sistema SIES-M, se ha apoyado históricamente bajo un discurso de "atajo tecnológico", que sugiere que la simple presencia de cámaras garantiza la seguridad o reduce la delincuencia. Esta aproximación es problemática, dado que la evidencia ha demostrado ser contradictoria; por ejemplo, en el año 2017, menos del 10% de las cámaras instaladas sirvió para identificar delitos (Londoño, 2024).

La necesidad de emplear como metodología la encuesta estructurada para comprender la configuración, donde el despliegue de tecnología de punto se utiliza para reconfigurar la percepción ciudadana sobre el espacio y dar la sensación de que se actúa frente a la inseguridad. Esta lógica

de vigilancia digital, influenciada por las nuevas tecnologías, se inscribe en un contexto de "sociedad de la vigilancia a través del control de los datos" (Lozano, 2013) y en la noción de la vigilancia como una herramienta que oscila entre el cuidado y el control social (Arteaga, 2010).

Esta mirada permitirá analizar cómo estos mecanismos, que utilizan información procesada para influir, administrar y controla a la población, se transforman en instrumentos de control social y político, impactando la forma en que diversos sectores de la población ejercen su ciudadanía.

4 Objetivos

4.1 Objetivo general

Explorar las percepciones de los habitantes de Medellín frente al uso de dispositivos de vigilancia digital implementados en el marco de las políticas de seguridad urbana, con el fin de analizar cómo dichas percepciones evidencian tensiones entre la innovación tecnológica y el ejercicio de la ciudadanía en el espacio urbano.

4.2 Objetivos específicos

- Describir las tecnologías de vigilancia implementadas en Medellín y su articulación con las políticas de seguridad urbana.
- Analizar los discursos institucionales que legitiman el uso de dichos dispositivos en nombre de la innovación tecnológica, el progreso y la seguridad ciudadana.
- Identificar las percepciones, valoraciones y preocupaciones de los habitantes de Medellín frente al uso de dispositivos de vigilancia digital en su vida cotidiana.
- Examinar las tensiones que emergen entre el despliegue de dispositivos de vigilancia digital y el ejercicio de los derechos ciudadanos, particularmente la privacidad, la libertad y la participación.
- Reflexionar desde una perspectiva sociológica crítica sobre las implicaciones de estas tecnologías en la configuración de la ciudadanía y la gobernabilidad urbana en Medellín.

5 Marco teórico

El estudio de la vigilancia en las sociedades contemporáneas ha estado marcado por varias teorías que permiten comprender cómo las tecnologías reconfiguran el control social, la seguridad y la vida urbana. Desde Michel Foucault hasta las perspectivas actuales del gobierno algorítmico, existe una tendencia creciente que, lejos de considerar la tecnología como un recurso neutral, la entiende como un dispositivo cargado de valores, intereses políticos y relaciones de poder. En el caso de Medellín, ciudad que ha apostado por convertirse en un laboratorio de innovación urbana y que fue declarada en 2021 como Distrito Especial de Ciencia, Tecnología e Innovación, que refuerzan una política de ciudad inteligente anclada en la promesa del progreso. Feenberg (1999) insiste en que "la tecnología encarna valores sociales y políticos que orientan su diseño y aplicación" (p. 15), lo cual permite problematizar el despliegue de dispositivos de vigilancia en Medellín bajo una narrativa de modernización y eficiencia. Es así como el despliegue de dispositivos de videovigilancia, reconocimiento facial y plataformas de datos abre preguntas urgentes sobre cómo los ciudadanos experimentan y resignifican estas transformaciones en su cotidianidad.

En su análisis del panóptico, Foucault (1975/2002) mostró cómo la arquitectura del poder se reorganiza a través de mecanismos de vigilancia que producen sujetos dóciles, así constituye un punto de partida fundamental para comprender las lógicas de vigilancia contemporáneas. Aunque la metáfora panóptica ha sido ampliamente debatida, sigue siendo útil para analizar las cámaras distribuidas en el espacio público, donde la posibilidad de ser visto en cualquier momento genera un efecto disciplinario, independientemente de si se está siendo observado efectivamente. En *Vigilar y castigar*, el autor describe el paso del poder soberano al poder disciplinario y biopolítico, que se ejerce mediante dispositivos de observación y control de los cuerpos. Como señala: "El panoptismo constituye un mecanismo de poder en el cual los individuos se vigilan a sí mismos, como si fueran objeto de una mirada permanente" (Foucault, 1975, p. 202). En Medellín, con más de 3.200 cámaras de diferentes funcionalidades operadas por el Sistema Integrado de Emergencias y Seguridad Metropolitano (SIES-M), la lógica panóptica se actualiza bajo la promesa de eficiencia y seguridad. En la actualidad, las tecnologías digitales y los sistemas algorítmicos amplían esta dinámica hacia formas más difusas, donde la vigilancia no es ya localizada en una institución cerrada, sino distribuida en el entramado urbano y mediada por datos. Deleuze (1990) actualiza

esta perspectiva al plantear que las sociedades disciplinarias han dado paso a las "sociedades de control", caracterizadas por un poder continuo y ubicuo que opera mediante códigos y flujos de información más que por encierros institucionales. Por ejemplo, los sistemas de reconocimiento facial y de lectura automática de placas (LPR), por ejemplo, no solo observan, sino que anticipan movimientos, predicen riesgos y orientan decisiones policiales.

La videovigilancia en la sociedad panóptica contemporánea ha transformado las máquinas de visión en armas que confunden lo público con lo privado (Bañuelos, 2003). Esta influencia del panóptico de Bentham trasciende el ámbito arquitectónico para convertirse en una "arquitectura moral" y un sistema de visibilidad permanente que asegura el funcionamiento automático del poder (Lozano Jiménez, 2013). En este nuevo orden informacional, Domínguez y Domínguez (2023) plantean que el panoptismo digital opera de forma silenciosa e inconsciente, donde el deseo y la libertad se convierten en dimensiones activas de la gubernamentalidad algorítmica.

David Lyon ha retomado y expandido la herencia foucaultiana para pensar la "sociedad de la vigilancia". Según el autor, "la vigilancia se ha normalizado como parte de la vida cotidiana, al punto de convertirse en una cultura en la que los propios sujetos colaboran activamente en su observación" (Lyon, 2018, p. 14). Por lo tanto, la sociedad es caracterizada la recopilación sistemática de datos personales y su uso para clasificar y gestionar poblaciones. Según el autor, la vigilancia no se limita a los dispositivos policiales, sino que atraviesa la vida social en múltiples dimensiones: desde las interacciones cotidianas hasta los mercados de datos que sostienen el capitalismo digital. Esta noción de *cultura de la vigilancia* es particularmente pertinente para Medellín, donde los dispositivos de videovigilancia son presentados institucionalmente como garantes de seguridad, y muchos ciudadanos tienden a aceptarlos como inevitables o incluso deseables. De esta manera, la vigilancia no se impone únicamente desde el Estado, sino que se vuelve una práctica social legitimada, donde la frontera entre consentimiento y coerción se vuelve difusa. En sintonía, Zuboff (2019) plantea el concepto de "capitalismo de la vigilancia" para referirse a la extracción masiva de datos como base de un nuevo modelo económico que mercantiliza la experiencia humana.

La crítica a estos procesos ha sido desarrollada también por autores como Byung-Chul Han (2013), quien advierte que la lógica de la transparencia y la hiperconectividad generan una forma de autoexplotación y autoexposición que refuerza la vigilancia sin necesidad de coerción directa. Han complementa esta mirada al mostrar cómo el neoliberalismo produce sujetos que participan

de su propia vigilancia. En *La sociedad de la transparencia*, Han (2013) sostiene que "la exposición total se convierte en una coacción sistémica: el sujeto se entrega voluntariamente al control en nombre de la libertad y la eficiencia" (p. 78). Esta lógica de autoexplotación y autovigilancia conecta con la manera en que los ciudadanos aceptan compartir datos o ser monitoreados bajo la promesa de seguridad, sin advertir plenamente las implicaciones para su privacidad o autonomía. Edison Lema-Taday (2021) profundiza en esta problemática desde América Latina al señalar que los procesos de digitalización y control algorítmico importan modelos del Norte Global que no necesariamente responden a los contextos sociales, políticos y culturales locales, reproduciendo desigualdades y generando nuevas formas de exclusión.

Un ejemplo que vale la pena mencionar es el caso de Estonia, un Estado que ha apostado por un modelo de gobernanza ciento por ciento digital, ofreciendo a los estonios el acceso a la totalidad de los tramites y servicios asociados al Estado de manera digital a través de herramientas y tecnologías de última generación. El modelo e-Estonia3, llamada por ellos mismos "la sociedad digital coolest [más moderna]", posee un ecosistema basado en la identidad digital obligatoria (DNI), y en el que los tramites y servicios están centrados en el usuario/ciudadano, cuyo acceso a los mismos se da usando la tarjeta de identificación en un 64%, el 19% usando el ID móvil y el 51% usa Smart-ID. Además, es un gobierno pionero en el uso de la tecnología blockchain4 para la verificación de integridad de los registros y datos del gobierno, asegurando que en la cadena de bloques no se almacenen los datos. (Republic of Estonia, s.f.).

Sin embargo, modelos de gobernanza urbana como el de Estonia, no son neutrales. Autores como Lema-Taday (2022) y Silva Arriola (2009) advierten que estos modelos de gestión algorítmica a menudo se implementan sin una discusión pública amplia ni una regulación clara, lo que permite que sistemas inteligentes se inserten en la ciudad sin el debido escrutinio democrático. Lema-Taday en sus trabajos sobre gubernamentalidad algorítmica, muestra cómo los sistemas

[3] e-Estonia se refiere a la sociedad digital de Estonia, un modelo de país que ha transformado radicalmente la interacción de sus ciudadanos y residentes con el estado mediante el uso extensivo de soluciones de Tecnologías de la Información y la Comunicación (TIC). Este enfoque integral permite realizar trámites gubernamentales en línea las 24 horas del día, los 7 días de la semana, incluyendo servicios como la Junta de Impuestos electrónica, el comercio y la banca electrónica, el voto electrónico, la prescripción electrónica y hasta el matrimonio electrónico.

[4] Blockchain: La tecnología de cadena de bloques es un mecanismo avanzado de bases de datos que permite compartir información transparente dentro de la red de una empresa. Una base de datos de cadena de bloques almacena los datos en bloques que se vinculan entre sí en una cadena. Los datos son cronológicamente consistentes debido a que no es posible eliminar ni modificar la cadena sin el consenso de la red. Como resultado, se puede utilizar la tecnología de cadena de bloques para crear un libro mayor inalterable o inmutable para realizar un seguimiento de los pedidos, los pagos, las cuentas y otras transacciones. El sistema incluye mecanismos integrados que evitan las entradas de transacciones no autorizadas y crean coherencia en la vista compartida de estas transacciones.

inteligentes, como los algoritmos de predicción del crimen, se insertan en lógicas de gestión urbana sin suficiente escrutinio democrático. Lema-Taday (2022), plantea que estos dispositivos pueden profundizar desigualdades existentes y reproducir sesgos estructurales bajo una apariencia de neutralidad técnica.

Desde una mirada crítica, estos procesos pueden inscribirse en lo que Foucault denominó el paso del poder soberano al poder disciplinario y biopolítico, donde el control ya no se ejerce exclusivamente sobre los cuerpos, sino sobre los flujos de datos, los movimientos y los comportamientos. A su vez, Shoshana Zuboff (2019) introduce el concepto de *capitalismo de la vigilancia* para explicar cómo las empresas tecnológicas han construido un modelo económico basado en la extracción y análisis masivo de datos personales. Como advierte la autora, "el capitalismo de la vigilancia reclama la experiencia humana como materia prima gratuita para traducción en datos de comportamiento" (p. 8). Aunque su análisis se centra en corporaciones globales, su planteamiento ilumina cómo en los datos recolectados a través de cámaras, sensores o plataformas estatales pueden adquirir valor económico y político, generando una hibridación entre control estatal y acumulación privada de información. Esta condición de visibilidad permanente es descrita por Sabater (2008) bajo la metáfora de las "vidas de cristal". En la sociedad de la información, el ciudadano se convierte en el protagonista de una exposición continua e involuntaria, donde las fronteras entre lo público, lo privado y lo íntimo se desdibujan, transformando la privacidad de un derecho personal en un elemento residual del control estatal y comercial."

David Lyon actualiza la teoría foucaultiana con el concepto de "sociedad de la vigilancia", en la que los datos personales se recolectan masivamente para predecir y gobernar comportamientos. En textos como *Surveillance Studies* (2007) o *The Culture of Surveillance* (2018), Lyon sostiene que la vigilancia se ha normalizado al punto de convertirse en una cultura participativa, donde los sujetos, muchas veces, consienten o incluso colaboran con su propia vigilancia (self-surveillance).

Otro referente clave es Oscar Gandy, quien en The Panoptic Sort (1993) muestra cómo los sistemas de clasificación automatizada (como los algoritmos predictivos) no solo observan, sino que jerarquizan y excluyen. Esta perspectiva sirve para comprender cómo los algoritmos de vigilancia predictiva o los sistemas de reconocimiento facial pueden reproducir desigualdades estructurales, afectando desproporcionadamente a ciertos grupos o territorios de la ciudad. Del

mismo modo, Haggerty y Ericson (2000) introducen la idea de *surveillant assemblage*, al sostener que la vigilancia contemporánea se configura como un ensamblaje múltiple y descentralizado de tecnologías y bases de datos. En sus palabras, "la vigilancia se dispersa y se reensambla en una red que no tiene un solo centro, sino múltiples nodos interconectados" (p. 611). Esta noción resulta clave para pensar Medellín, donde el sistema de seguridad integra cámaras, software predictivo, bases de datos biométricas y aplicaciones móviles en un entramado que funciona de manera coordinada, pero difícil de auditar.

Finalmente, desde el campo de los estudios sobre ciudadanía, Isin (2009) recuerda que ser ciudadano no es solo tener derechos formales, sino también ejercer actos de agencia mediante los cuales se aceptan, resisten o resignifican los marcos de gobierno. Así, la vigilancia digital no debe ser entendida únicamente como un dispositivo de control, sino como un campo de disputa donde los ciudadanos construyen sentidos y responden de maneras diversas: algunos legitiman los dispositivos como necesarios, otros los cuestionan en nombre de los derechos, y otros los resignifican en su cotidianidad.

6 Metodología

La presente investigación se desarrolla desde un enfoque cuantitativo de carácter exploratorio y analítico, orientado a examinar las percepciones ciudadanas frente al uso de tecnologías de vigilancia digital en la ciudad de Medellín. Este enfoque resulta pertinente en la medida en que permite identificar tendencias generales en las opiniones, valoraciones y preocupaciones de los ciudadanos frente a la incorporación de dispositivos tecnológicos en las políticas de seguridad urbana.

Desde la sociología, el estudio de las percepciones no busca asumir las respuestas como reflejos transparentes de la realidad social, sino como expresiones situadas que permiten identificar climas de opinión, marcos interpretativos y posicionamientos ciudadanos frente a determinados fenómenos públicos. En este sentido, las respuestas recogidas mediante encuesta deben ser comprendidas como indicadores de tendencias perceptivas que se configuran en contextos políticos, culturales y tecnológicos específicos.

Tal como señalan diversos estudios sobre opinión pública, los resultados de encuestas pueden estar influidos por factores contextuales como el clima político, los debates mediáticos o la coyuntura institucional por el miedo de los individuos al aislamiento social al percibir un clima político hostil a sus ideas (Noelle-Neumann, 1995). Por esta razón, el análisis de las percepciones sobre vigilancia digital no se interpreta como una medición absoluta de actitudes ciudadanas, sino como una aproximación empírica a la forma en que distintos sectores de la población interpretan la relación entre seguridad, tecnología y derechos ciudadanos.

El carácter exploratorio del estudio responde además a la relativa escasez de investigaciones empíricas sobre percepción ciudadana de tecnologías de vigilancia digital en contextos urbanos latinoamericanos, y particularmente en el caso de Medellín. En consecuencia, la investigación busca contribuir a la comprensión sociológica de este fenómeno mediante la identificación de patrones de percepción, niveles de confianza institucional y tensiones asociadas al uso de datos personales en el espacio urbano.

6.2 Diseño de investigación

El estudio adopta un diseño transversal, basado en la aplicación de una encuesta estructurada dirigida a personas residentes o que transitan habitualmente por Medellín. La difusión del instrumento se realizó mediante plataformas digitales y redes sociales, por lo que la participación fue voluntaria y se dio a través de un proceso de autoselección. En consecuencia, la composición final de la muestra estuvo condicionada por los canales de difusión empleados, concentrándose principalmente en población adulta joven y adulta, siendo este segmento que utiliza con mayor frecuencia este tipo de aplicaciones/plataformas digitales.

El instrumento fue diseñado con el objetivo de captar diferentes dimensiones de la relación entre ciudadanía y vigilancia digital, incluyendo aspectos como:

- percepción del despliegue tecnológico en la ciudad
- confianza institucional en el uso de datos
- valoración de la inteligencia artificial aplicada a la seguridad
- preocupaciones sobre privacidad y uso de información personal
- posibles tensiones entre seguridad y derechos ciudadanos

La encuesta incluyó preguntas de carácter sociodemográfico, preguntas de percepción general y una batería de afirmaciones evaluadas mediante escala tipo Likert, lo que permitió construir posteriormente indicadores analíticos sobre diferentes dimensiones del fenómeno estudiado. Este tipo de diseño es ampliamente utilizado en investigaciones sociales que buscan vincular variables de perfil con constructos complejos, permitiendo la generación de índices sintéticos a partir de promedios y tendencias de respuesta (De la Garza Montemayor et al., 2019).

Para comprender la coherencia de las percepciones ciudadanas, este estudio se apoya en la premisa del estructuralismo genético de Goldmann (1967), quien plantea que los hechos humanos no son piezas aisladas, sino estructuras significativas. Bajo este enfoque, las opiniones recogidas no se analizan como datos individuales, sino como respuestas de un sujeto colectivo que intenta equilibrar su relación con el entorno tecnológico y social.

6.3 Instrumento de recolección de información

El instrumento de investigación utilizado fue una encuesta estructurada, compuesta por preguntas cerradas y una batería de afirmaciones evaluadas mediante una escala tipo Likert de cinco niveles. Esta herramienta constituye el estándar en investigaciones sociales para medir percepciones, ya que permite captar dimensiones subjetivas complejas —como la confianza y el riesgo— y facilita la construcción de indicadores comparables (Hernández-Sampieri et al., 2014). El objetivo es identificar patrones iniciales en fenómenos sociales emergentes que, por su naturaleza, requieren un abordaje exploratorio (Cazau, 2006).

En este caso, los participantes debían indicar su posición frente a diferentes afirmaciones relacionadas con el uso de tecnologías de vigilancia en Medellín, seleccionando una de las siguientes opciones:

1. Totalmente en desacuerdo
2. En desacuerdo
3. Ni de acuerdo ni en desacuerdo
4. De acuerdo
5. Totalmente de acuerdo

Este tipo de escala permite capturar matices en las percepciones ciudadanas y facilita posteriormente la construcción de índices analíticos que sintetizan tendencias de respuesta en torno a diferentes dimensiones conceptuales.

Las escalas tipo Likert permiten medir el grado de acuerdo o desacuerdo de los encuestados frente a determinadas afirmaciones, lo cual resulta especialmente útil para analizar percepciones, actitudes y valoraciones en estudios de opinión pública. Este tipo de medición ha demostrado ser eficaz para captar dimensiones subjetivas como la confianza, la percepción de riesgo o la valoración de tecnologías, posibilitando la construcción de indicadores sobre fenómenos sociales complejos (Field, 2013).

El cuestionario incluyó tres tipos principales de preguntas:

1. **Preguntas sociodemográficas**, orientadas a caracterizar a los participantes (edad, género, nivel educativo, entre otros).

2. **Preguntas de percepción general**, relacionadas con la presencia de cámaras y tecnologías de vigilancia en la ciudad.
3. **Batería de afirmaciones Likert**, orientadas a medir niveles de aceptación tecnológica, confianza institucional, preocupaciones sobre privacidad y valoración del uso de datos personales.

Adicionalmente, el instrumento incluyó una pregunta final opcional que invitaba a los participantes a manifestar su disposición a participar en futuras entrevistas o grupos focales, lo que abre la posibilidad de complementar el análisis cuantitativo con estrategias cualitativas en investigaciones posteriores.

El cuestionario fue implementado mediante un formulario digital autoadministrado, diseñado en la plataforma Microsoft Forms, permitiendo que cada participante diligenciara el instrumento de manera autónoma desde cualquier dispositivo con acceso a internet. Lo anterior facilitó la recolección de información durante un periodo continuo de cuatro meses, garantizando además el anonimato de las respuestas y reduciendo posibles sesgos derivados de la interacción y encuestado (Hernández-Sampieri et al., 2014).

6.4 Población y muestra

La población de interés de esta investigación estuvo conformada por personas residentes y transeúntes que interactúan cotidianamente con el espacio urbano de Medellín, potencialmente expuestos a tecnologías de vigilancia digital como dispositivos como cámaras de seguridad, sistemas de monitoreo urbano y tecnologías de reconocimiento facial. Aunque el instrumento estuvo disponible para cualquier persona interesada en participar de manera voluntaria, la estrategia de difusión utilizada favoreció principalmente la participación de población adulta joven y adulta, razón por la cual este segmento constituye el universo empírico sobre el que se desarrollan los análisis de la investigación.

La encuesta fue aplicada mediante un muestreo no probabilístico de tipo conveniencia con participación voluntaria. Los participantes accedieron libremente al cuestionario a través de diferentes canales digitales, por lo que la conformación de la muestra respondió a un proceso de autoselección. No obstante, esta autoselección estuvo condicionada por los medios utilizados para la difusión del instrumento, principalmente Meta Ads y Facebook, plataformas cuya penetración

es considerablemente entre adolescentes o personas menores de 60 años. En consecuencia, la distribución etaria obtenida corresponde a una aleatoriedad inducida por los canales de difusión y no a un criterio de selección definido de manera previa.

Dado que el objetivo principal del estudio es de carácter exploratorio y busca identificar tendencias de percepción más que realizar inferencias estadísticas representativas de toda la población. De acuerdo con la literatura metodológica, los estudios exploratorios permiten aproximarse a fenómenos poco estudiados o emergentes, identificando patrones iniciales y variables relevantes para futuras investigaciones (Cazau, 2006).

En total se recolectaron 217 encuestas válidas, las cuales constituyen la base empírica del análisis presentado en esta investigación. La aplicación del instrumento se realizó en la ciudad de Medellín, municipios del Valle de Aburrá y aledaños, mediante estrategias de difusión digital, a través de campañas en redes sociales utilizando la plataforma Meta Ads. La encuesta fue promovida desde la página de Facebook "Vigilancia Digital Medellín" creada con el objeto de esta investigación y adicionalmente difundida de manera orgánica en grupos locales de la ciudad con temáticas diversas, también existentes en la plataforma Facebook, entre ellos: "Lo vi en San Antonio de Prado", "Arriendos en Medellín", "San Antonio de Prado", "Clasificados Barichara, San Antonio de Prado y La Estrella", "La Estrella, Antioquia", "Valle de Aburrá Ventas y Servicios", "Apartamentos, Habitaciones y Arriendos Medellín", "Asamblea UdeA" y "Respondemos encuestas – Difusión de Encuestas, Cuestionarios y Estudios". Lo que permitió alcanzar una diversidad de participantes en términos sociodemográficos.

El instrumento fue administrado de manera autogestionada por los participantes mediante un formulario estructurado en línea, garantizando la anonimidad de las respuestas, la voluntariedad de la participación y el acceso abierto a la encuesta durante el periodo de recolección. Este proceso se desarrolló entre el 17 de diciembre de 2025 y el 15 de abril de 2026, tiempo durante el cual se logró consolidar una muestra suficiente para el análisis exploratorio planteado.

Como resultado de la estrategia de difusión implementada, el 98,2% de los participantes corresponde a personas entre los 19 y los 59 años, mientras que únicamente el 1,8% pertenece a otros grupos etarios. Esta distribución no obedeció a un criterio de selección deliberado, sino al perfil predominante de usuarios de las plataformas digitales utilizadas para la convocatoria. Asimismo, la participación de integrantes de comunidades universitarias, particularmente a través del grupo Asamblea UdeA, pudo favorecer una mayor representación de personas con formación

técnica, tecnológica y profesional. Se realiza esta claridad, aunque, las reacciones en la publicación no tuvieron gran alcance (una reacción y tres comentarios), sin que esto sea un indicador determinante en el aumento de la cantidad de encuestas recibidas de este público en específico. Por lo que los resultados deben interpretarse considerando un posible sesgo hacia población con niveles medios y altos de escolaridad, circunstancia que no invalida el estudio, pero delimita el alcance de sus inferencias.

Finalmente, si bien este tamaño muestral no permite realizar generalizaciones estadísticas estrictas para la totalidad de la población de Medellín, sí resulta suficiente para identificar patrones de percepción, relaciones entre variables y configuraciones de opinión relevantes para el análisis sociológico del fenómeno estudiado. Es por eso que, aunque el presente estudio corresponde a un muestreo no probabilístico por conveniencia, se estimó mediante la fórmula para poblaciones finitas, el margen de error con fines descriptivos, tomando como referencia la población residente de Medellín, equivalente aproximadamente a 1.465.555 habitantes[5] con edades entre los 20 y 59 años, de acuerdo a las proyecciones oficiales de población del Departamento Administrativo Nacional de Estadística (DANE, 2025). Considerando un nivel de confianza del 95%, una proporción esperada de máxima variabilidad ($p = q = 0,5$) y una muestra efectiva de 217 participantes, el margen de error estimado corresponde aproximadamente a ±6,65 %. Este cálculo se presenta únicamente como un referente para dimensionar el tamaño de la muestra, dado que el propósito del estudio no consiste en realizar inferencias estadísticas representativas de la población, sino identificar tendencias, asociaciones y configuraciones perceptivas propias de una este tipo de investigación (Hernández-Sampieri et al., 2014).

6.5 Estrategia de análisis de datos

El análisis de la información recolectada se realizó mediante el software estadístico SPSS, utilizando diferentes técnicas de análisis descriptivo y exploratorio.

En primer lugar, se realizaron análisis de estadística descriptiva, con el fin de identificar la distribución de las respuestas en cada una de las preguntas del cuestionario. Este paso permitió

[5] La cifra 1.465.555 de habitantes, se obtuvo a partir de la suma de los grupos quinquenales de edad de las proyecciones oficiales del DANE para Medellín.

establecer tendencias generales en las percepciones ciudadanas frente a la vigilancia digital en la ciudad.

En segundo lugar, se construyeron índices analíticos a partir de las baterías de preguntas tipo Likert, agrupando diferentes ítems que correspondían a dimensiones conceptuales similares. Estos índices permitieron sintetizar la información en tres dimensiones principales:

- **Índice de desarrollo tecnológico**, relacionado con la percepción de la presencia y expansión de tecnologías de vigilancia en la ciudad.
- **Índice de gobernabilidad algorítmica**, asociado a la confianza institucional y a la legitimidad del uso de tecnologías por parte del Estado.
- **Índice de ciudadanía**, orientado a medir preocupaciones relacionadas con derechos, privacidad y agencia ciudadana frente a los sistemas de vigilancia.

Posteriormente, se realizaron análisis de correlación bivariada entre estos índices y diferentes variables sociodemográficas, con el fin de identificar posibles asociaciones entre características sociales y posicionamientos frente a la vigilancia digital.

Finalmente, se aplicó un análisis de conglomerados (cluster analysis) utilizando los índices construidos, lo que permitió identificar diferentes tipologías de posicionamiento ciudadano frente al fenómeno de la vigilancia digital en Medellín.

6.6 Consideraciones éticas

La investigación se desarrolló siguiendo principios éticos propios de la investigación social. Antes de responder el cuestionario, los participantes tuvieron acceso a un consentimiento informado, en el cual se explicaba el propósito académico del estudio, el carácter voluntario de la participación y el uso exclusivamente investigativo de la información recolectada.

La encuesta fue diseñada de manera anónima, por lo que no se solicitó ni registró ningún dato que permitiera identificar directamente a los participantes. Asimismo, se informó a los encuestados que podían retirarse o dejar de responder en cualquier momento sin ninguna consecuencia.

En los casos en que algunos participantes decidieron voluntariamente dejar datos de contacto para futuras entrevistas o grupos focales, se incluyó un consentimiento adicional relacionado con el tratamiento de datos personales, en concordancia con la normativa colombiana sobre protección de datos, particularmente la Ley 1581 de 2012 y las disposiciones relacionadas con el derecho fundamental al habeas data.

Para esta investigación se utilizará un enfoque mixto con predominio cualitativo, debido a que se busca a través de la misma, explorar las percepciones ciudadanas frente al uso de dispositivos de vigilancia implementados en Medellín como parte de las políticas de seguridad urbana. En ese sentido, se busca articular dos técnicas principales: la aplicación de una encuesta estructurada a habitantes y visitantes de Medellín y un análisis documental. Esta sinergia metodológica permitirá la identificación de tendencias generales sobre la percepción que tienen los ciudadanos con el uso de estas tecnologías, sino también contextualizar esas percepciones en el marco de las narrativas institucionales, jurídicas y mediáticas en las que se encuentran enmarcadas.

El alcance de la investigación es exploratorio y descriptivo. Exploratorio porque, si bien se ha escrito sobre la vigilancia desde teóricos y narrativas institucionales, estás no logran abarcar la percepción ciudadana específicamente sobre vigilancia digital en Medellín, y descriptivo porque se pretende ofrecer un panorama sobre cómo los ciudadanos interpretan estas tecnologías en su vida cotidiana.

La encuesta será estructurada y se utilizará como técnica principal para identificar las percepciones y actitudes de los habitantes de Medellín frente al uso de dispositivos de vigilancia digital —tales como cámaras inteligentes, sistemas de reconocimiento facial, lectores automáticos de placas y plataformas de monitoreo predictivo—.

El cuestionario incluirá preguntas cerradas y escalas tipo Likert, organizadas a partir de las tres categorías de análisis definidas en el planteamiento del problema: desarrollo tecnológico (nivel de confianza en la innovación aplicada a la seguridad), gobernabilidad algorítmica (percepciones sobre la toma de decisiones basadas en datos y algoritmos) y ciudadanía (relación entre estas tecnologías y los derechos fundamentales como privacidad, libertad y participación).

La población objetivo de la encuesta serán los habitantes y visitantes de Medellín mayores. Se propone un muestreo estratificado por lugar de residencia, que permita recoger la diversidad territorial de la ciudad. El tamaño de la muestra se definirá según criterios de representatividad y

disponibilidad de recursos, buscando un equilibrio entre amplitud y viabilidad, previamente se estima la aplicación de unas 300 encuestas.

Los resultados de la encuesta se analizarán mediante estadística descriptiva (frecuencias, porcentajes y cruces simples), lo que permitirá establecer patrones generales en las percepciones ciudadanas y contrastarlos con los discursos institucionales.

El análisis documental complementará los hallazgos de la encuesta al situar las percepciones ciudadanas en un marco más amplio de narrativas sociales, institucionales y jurídicas. Este componente se alimentará mediante la revisión de documentos oficiales, como el Plan de Desarrollo de Medellín, informes de la Secretaría de Seguridad y Convivencia, y las normativas relacionadas con la protección de datos (Ley 1266 de 2008 y Ley 1581 de 2012). Además, se analizarán fuentes primarias, específicamente medios como *El Colombiano*, *El Tiempo* y *Caracol Radio*, que han reportado casos que han generado polémica. Finalmente se hará seguimiento del debate en las redes sociales, mediante el rastreo de hashtags y publicaciones vinculadas a la vigilancia digital, la privacidad y la seguridad en Medellín.

El análisis se llevará a cabo a través de la técnica de análisis crítico del discurso, que permite identificar cómo se construyen y disputan los significados sobre la vigilancia digital, la seguridad y los derechos ciudadanos en diferentes escenarios: el institucional, el mediático y el ciudadano. Esta perspectiva analítica posibilita examinar cómo los discursos configuran realidades sociales, evidenciando tanto las narrativas de legitimación como las prácticas de resistencia y las formas en que las instituciones estructuran el control y la regulación (Badillo Mendoza & Marta-Lazo, 2019).

Se tendrán en cuenta las siguientes consideraciones en la aplicación del instrumento de investigación –la encuesta estructurada– garantizando para los participantes el anonimato y la confidencialidad de los datos a través del otorgamiento de su consentimiento informado antes de responder. En el caso del análisis documental, se recurrirá únicamente a fuentes de acceso público, respetando los principios de transparencia y rigor académico.

Con el fin de ofrecer panorama sociológico más amplio, el análisis de resultados se realizará a nivel empírico, es decir, identificando patrones y tendencias en las percepciones ciudadanas a partir de los datos obtenidos en la encuesta y a nivel discursivo con la interpretación crítica de las narrativas institucionales y mediáticas sobre la vigilancia digital. Esto permitirá dar cuenta de lo que piensan y sienten los ciudadanos, así como también estos discursos se insertan en el marco de

las políticas de seguridad y del modelo de innovación tecnológica de Medellín como Distrito Especial de Ciencia, Tecnología e Innovación.

7 Caracterización de la muestra y percepciones generales sobre la vigilancia digital en Medellín

7.1 Caracterización sociodemográfica de la muestra

La encuesta fue aplicada a 217 personas que transitan o habitan en el Valle de Aburrá, con el objetivo de explorar sus percepciones frente al uso de tecnologías de vigilancia digital en la ciudad de Medellín. Si bien el estudio no pretende representar estadísticamente a toda la población de la ciudad, ya que no corresponde a un diseño probabilístico representativo, la muestra permite identificar tendencias relevantes en la forma en que distintos sectores de la ciudadanía interpretan la presencia de tecnologías de monitoreo en el espacio urbano.

El análisis sociodemográfico permite contextualizar las respuestas obtenidas, dado que variables como la edad, el nivel educativo o el tipo de relación con la ciudad pueden influir en la forma en que los ciudadanos interpretan el uso de dispositivos tecnológicos de vigilancia.

En términos generales, la distribución de la muestra evidencia una participación predominante de personas con niveles educativos medios y altos, lo que sugiere que las respuestas pueden estar influenciadas por niveles relativamente altos de alfabetización digital y acceso a información sobre tecnologías de vigilancia. Este elemento resulta relevante para interpretar las percepciones sobre privacidad, reconocimiento facial o uso institucional de datos personales.

Asimismo, la diversidad de perfiles dentro de la muestra permite identificar distintas formas de relación con los dispositivos tecnológicos presentes en el espacio urbano, lo cual será particularmente relevante en los análisis posteriores sobre confianza institucional y derechos ciudadanos.

- **Distribución por edad**

La distribución por rangos de edad muestra la participación de ciudadanos pertenecientes a distintos grupos generacionales, lo que permite captar percepciones diversas con relación al uso de tecnologías digitales en el espacio urbano. En los datos recolectados (**Tabla 1**), se cuenta con una fuerte presencia de población joven y adulta dentro de la muestra, en la que el 53% de los encuestados se encuentra entre los 19 y 30 años, mientras que el 45,2% corresponde al rango entre

31 y 59 años. Los grupos extremos de edad presentan una participación mucho menor, con 1,4% entre los 12 y los 18 años y el 0,5% de personas mayores de 60 años.

Tabla 1

Distribución de la muestra según rango de edad

Selecciona el rango de edad en el que te encuentras

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	60 años en adelante	1	,5	,5	,5
	Entre 12-18 años	3	1,4	1,4	1,8
	Entre 19-30 años	115	53,0	53,0	54,8
	Entre 31-59 años	98	45,2	45,2	100,0
	Total	217	100,0	100,0	

Este patrón sugiere que la encuesta logra recoger principalmente percepciones de población en edad productiva y con alta interacción con el espacio urbano, esto resulta relevante para el análisis de tecnologías de vigilancias presentes en la vida cotidiana de la ciudad. Esta predominación en los grupos etarios puede relacionarse con una mayor exposición a entornos digitales y a debates contemporáneos sobre tecnología, privacidad y seguridad, lo que potencialmente incluye en la forma en que se evalúan los sistemas de monitoreo urbano. Estos aspectos resultan relevantes, ya que investigaciones previas han señalado que la relación con las tecnologías de vigilancia puede variar según el grado de familiaridad con los entornos digitales.

- **Distribución por género**

En cuanto al género, la muestra presenta una distribución relativamente equilibrada (**Tabla 2**). El 54,4% de los encuestados se identifica como mujer, mientras que el 43,3% se identifica como hombre. Un 0,5% se identifica como no binario, y el 1,8% prefirió no responder a esta pregunta.

Tabla 2

Distribución de la muestra según identidad de género

¿Con cuál género te identificas?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Hombre	94	43,3	43,3	43,3
	Mujer	118	54,4	54,4	97,7
	No binario	1	,5	,5	98,2
	Prefiero no responder	4	1,8	1,8	100,0
	Total	217	100,0	100,0	

Esta composición permite identificar en las percepciones diversas opiniones sobre la vigilancia digital, considerando que las experiencias de seguridad, control y exposición en el espacio público pueden variar según el género. Es así cómo diversos estudios han señalado que las mujeres tienen a experimentar el espacio urbano desde condiciones diferenciadas de vulnerabilidad y riesgo, lo que puede influir en su valoración de tecnologías de vigilancia asociadas a la seguridad (Pain, 2000). En este sentido, la presencia significativa de mujeres en la muestra es relevante para interpretar las percepciones sobre cámaras de seguridad y monitoreo urbano.

- **Nivel educativo**

Con relación con el nivel educativo, la muestra capturada presenta una concentración importante en niveles de formación media y superior (**Tabla 3**). El 41,9% de los encuestados cuenta con formación de pregrado, mientras que el 33,6% tiene formación técnica o tecnológica. El resto de la muestra se distribuye en estudios de posgrados con un 12,9% y el 11,5% indican haber alcanzado el niel de secundaria como máximo nivel educativo.

Tabla 3

Distribución de la muestra según nivel educativo

¿Cuál es tu nivel educativo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Posgrado	28	12,9	12,9	12,9
	Pregrado	91	41,9	41,9	54,8
	Secundaria	25	11,5	11,5	66,4
	Técnico/Tecnológico	73	33,6	33,6	100,0
	Total	217	100,0	100,0	

En términos generales, estos datos permiten inferir que una proporción considerable de los participantes cuenta con nieles relativamente altos de formación académica, esto es clave porque puede influir en la forma en que se interpretan las implicaciones de las tecnologías de vigilancia y a las políticas adoptadas por los gobiernos con relación a los sistemas de vigilancia digital.

Desde el campo de los estudios sociales de la tecnología, se ha señalado que el nivel educativo puede incidir en el grado de alfabetización digital y en la capacidad de problematizar críticamente el uso de tecnologías de monitoreo y recopilación de datos (Selwyn, 2004).

- **Estrato socioeconómico**

La muestra también refleja (**Tabla 4**), en términos socioeconómicos, una distribución consistente con la estructura urbana del Valle de Aburrá. El 51,2% de los encuestados reporta en la encuesta vivir en estrato 3, seguido por 30% en estrato 2. Los estratos 4 y 5 presentan participaciones menores, con 10,1% y 2,3% respectivamente, mientras que el 6,5% pertenece al estrato 1.

Tabla 4

Distribución de la muestra según estrato socioeconómico

¿En qué estrato socioeconómico vives?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	1	14	6,5	6,5	6,5
	2	65	30,0	30,0	36,4
	3	111	51,2	51,2	87,6
	4	22	10,1	10,1	97,7
	5	5	2,3	2,3	100,0
	Total	217	100,0	100,0	

Este patrón, sumado a los demás resultados obtenidos, indica que la mayoría de los participantes proviene de sectores medios y medios-bajos de la ciudad, lo cual resulta ser particularmente relevante para analizar percepciones sobre seguridad urbana, dado que estas poblaciones suelen experimentar de manera más directa las dinámicas de vigilancia, control territorial y políticas de seguridad implementadas en los diferentes escenarios que hacen parte del espacio público.

7.2 Percepción sobre la presencia de dispositivos de vigilancia en el espacio urbano

Uno de los primeros aspectos explorados en la encuesta fue la percepción que tienen los ciudadanos sobre la presencia de cámaras y dispositivos de vigilancia en la ciudad.

En este sentido, la mayoría de los encuestados reconoce la presencia visible de dispositivos de videovigilancia en Medellín, lo que indica que estas tecnologías forman parte del paisaje urbano cotidiano. Las cifras obtenidas y que se observan en la ***Tabla 5*** muestran que 32,3% de los encuestados considera que aparece en cámaras "algo o de forma neutral", mientras que 15,7% señala que aparece bastante y 17,1% afirma aparecer mucho en estos sistemas de monitoreo. En contraste, 23% percibe aparecer poco y 12% considera que no aparece en cámaras de vigilancia. Este resultado sugiere que la vigilancia tecnológica ha alcanzado un grado importante de normalización social, en el cual la presencia de cámaras se percibe como un elemento habitual de la infraestructura urbana sumando a la experiencia cotidiana de movilidad y tránsito en el espacio público.

Tabla 5

Percepción de exposición a cámaras de vigilancia en Medellín

¿Qué tanto percibe que usted aparece en cámaras de vigilancia en Medellín?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada	26	12,0	12,0	12,0
	Poco	50	23,0	23,0	35,0
	Neutral / Algo	70	32,3	32,3	67,3
	Bastante	34	15,7	15,7	82,9
	Mucho	37	17,1	17,1	100,0
	Total	217	100,0	100,0	

Sin embargo, la percepción de presencia no necesariamente se traduce en una comprensión clara sobre el funcionamiento de estas tecnologías o sobre el uso que las instituciones hacen de la información recopilada. Como se verá en los apartados posteriores, existe una diferencia significativa entre percibir la presencia de vigilancia y comprender los sistemas tecnológicos asociados a ella.

Este hallazgo es consistente con la literatura sobre vigilancia contemporánea, la cual señala que muchas tecnologías de monitoreo operan en contextos donde los ciudadanos reconocen su existencia, pero tienen información limitada sobre su funcionamiento o sus implicaciones (Lyon, 2018). En este sentido, las cámaras y otros dispositivos de monitoreo no solo cumplen funciones de seguridad, sino que también configuran nuevas formas de relación entre los ciudadanos, el espacio urbano y las instituciones encargadas de su administración, lo que se relaciona con el fenómeno denominado normalización de la vigilancia por Lyon.

7.3 Actitudes frente al uso de tecnologías de vigilancia

La encuesta también exploró la valoración que los ciudadanos hacen del uso de cámaras de vigilancia como herramienta para mejorar la seguridad en Medellín, y las actitudes generales frente a estas tecnologías, particularmente en relación con su utilidad.

Los resultados muestran que una proporción significativa de los encuestados considera que el uso de cámaras y sistemas tecnológicos puede contribuir a mejorar la seguridad urbana. Esto se observa en la **Tabla 6** donde se muestra una distribución relativamente equilibrada entre posiciones favorables, neutrales y críticas. El 24,9% de los encuestados se declara de acuerdo con que las cámaras ayudan a mejorar la seguridad, mientras que el 23% se muestra totalmente de acuerdo con esa afirmación. En conjunto, cerca de la mitad de la muestra expresa una valoración positiva hacia la videovigilancia.

Esta percepción refleja una tendencia ampliamente documentada en estudios internacionales sobre videovigilancia, donde las tecnologías de control urbano suelen legitimarse a partir de discursos asociados a la seguridad pública y la prevención del delito (Galdon-Clavell, 2015) a través de discursos y promesas de aumentar la seguridad ciudadana, incluso cuando la evidencia empírica sobre su efectividad resulta ambigua.

No obstante, esta aceptación no necesariamente implica una confianza plena en el funcionamiento de los sistemas, ni en las instituciones responsables de su implementación, ni en el uso que las autoridades hacen de la información recopilada. De hecho, en varias respuestas se observa la coexistencia de actitudes favorables hacia la tecnología con preocupaciones relacionadas con la privacidad y el manejo de datos personales. Como lo demuestra el resto de resultados, en los que el 26,7% adopta una posición neutral, lo que sugiere la existencia de percepciones cautelosas frente a la eficacia de estas tecnologías.

Finalmente, 25,3% manifiesta desacierto o total desacuerdo con esta afirmación, lo que indica la presencia de una proporción significativa de ciudadanos que cuestiona el papel de las cámaras como herramienta efectiva para mejorar la seguridad urbana.

Tabla 6

Percepción sobre la efectividad de las cámaras en la seguridad

Considero que las cámaras ayudan a mejorar la seguridad en Medellín

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	22	10,1	10,1	10,1
	En desacuerdo	33	15,2	15,2	25,3
	Ni de acuerdo ni en desacuerdo	58	26,7	26,7	52,1
	De acuerdo	54	24,9	24,9	77,0
	Totalmente de acuerdo	50	23,0	23,0	100,0
	Total	217	100,0	100,0	

Esta ambivalencia constituye uno de los elementos más relevantes para comprender las percepciones ciudadanas frente a la vigilancia digital, ya que evidencia que el apoyo a estas tecnologías no es absoluto, sino que se encuentra condicionado por factores como la confianza institucional, el conocimiento tecnológico y las preocupaciones por los derechos ciudadanos.

7.4 Percepción sobre el aumento de la vigilancia en la ciudad

Con este estudio también se encontró información de valor de las personas encuestadas con respecto al aumento de la vigilancia de la ciudad durante los últimos años.

Lo resultados en la

Tabla *7* indican que una parte significativa de los encuestados 26,7% percibe que la vigilancia en el espacio urbano ha aumentado con el paso del tiempo, por lo que se sienten mucho más vigilado. Este fenómeno puede asociarse tanto a la expansión de infraestructuras tecnológicas de monitoreo como a la creciente presencia de discursos públicos sobre seguridad y control urbano, mientras que el 23% afirma sentirse bastante más vigilado. A estos grupos se suma un 20,7% que mantiene una posición neutral o intermedia frente a esta afirmación.

En contraste, el 13,8% señala sentirse poco más vigilado y 15,7% indica no percibir un aumento en la vigilancia. En conjunto, estos datos indican que casi la mitad de los participantes percibe un incremento significativo de la vigilancia tecnológica en la ciudad.

Este hallazgo resulta consistente con la expansión de infraestructuras tecnológicas de monitoreo urbano implementadas en Medellín durante la última década, incluyendo redes de

videovigilancia, sistemas de monitoreo centralizado y el uso de tecnologías de análisis de datos en estrategias de seguridad urbana.

Tabla 7

Percepción de incremento de la vigilancia en los últimos años

¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada	34	15,7	15,7	15,7
	Poco	30	13,8	13,8	29,5
	Neutral / Algo	45	20,7	20,7	50,2
	Bastante	50	23,0	23,0	73,3
	Mucho	58	26,7	26,7	100,0
	Total	217	100,0	100,0	

Desde una perspectiva teórica, este proceso se relaciona con lo que Gilles Deleuze (1990) describió como la transición hacia sociedades de control, caracterizadas por formas de regulación social que operan mediante sistemas tecnológicos distribuidos en múltiples espacios de la vida cotidiana. Esta percepción puede interpretarse como parte de la transición hacia formas de regulación social mediadas por tecnologías digitales, fenómeno que diversos autores han descrito como el surgimiento de nuevas formas de gubernamentalizad algorítmica, donde los sistemas automatizados adquieren un papel creciente en la administración del orden público.

Es así como la expansión de dispositivos de vigilancia no solo transforma las prácticas institucionales de control, sino también la manera en que los ciudadanos perciben su relación con el espacio público.

7.5 Comprensión ciudadana sobre tecnologías de vigilancia

Los ciudadanos encuestados también declararon tener algún nivel de conocimiento sobre tecnologías específicas de vigilancia, particularmente aquellas basadas en inteligencia artificial o reconocimiento facial aplicados a la seguridad en el espacio público.

Los resultados muestran que, aunque muchos ciudadanos reconocen la presencia de cámaras en la ciudad, una proporción considerable declara no comprender claramente el funcionamiento de tecnologías como el reconocimiento facial o los sistemas automatizados de análisis de datos (**Tabla 8**). Por lo que se evidencia que el nivel de comprensión sobre estas tecnologías es relativamente limitado dado que no comprenden cómo funcionan.

Un 25,8% de los encuestados se encuentra totalmente en desacuerdo con la afirmación de que entienden bien cómo funcionan estos sistemas, mientras que 17,5% se declara en desacuerdo. Esto significa que 43,3% de los encuestados reconoce no comprender claramente el funcionamiento de estas tecnologías. Por su parte, 30,4% adopta una posición neutral, mientras que 26,3% afirma comprender en alguna medida el funcionamiento de estos sistemas.

Tabla 8

Nivel de comprensión sobre sistemas de reconocimiento facial

Entiendo bien cómo funcionan los sistemas de reconocimiento facial

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en desacuerdo	56	25,8	25,8	25,8
	En desacuerdo	38	17,5	17,5	43,3
	Ni de acuerdo ni en desacuerdo	66	30,4	30,4	73,7
	De acuerdo	31	14,3	14,3	88,0
	Totalmente de acuerdo	26	12,0	12,0	100,0
	Total	217	100,0	100,0	

Este hallazgo apunta a la existencia de una brecha entre la expansión tecnológica y la comprensión pública de sus implicaciones, lo cual puede afectar la forma en que los ciudadanos evalúan los riesgos y beneficios asociados a estos sistemas.

Autores como Feenberg (1999) han señalado que los sistemas tecnológicos no son simplemente herramientas neutrales, sino estructuras que incorporan decisiones políticas, institucionales y económicas que muchas veces permanecen invisibles para los usuarios, este fenómeno se ha interpretado como una forma de asimetría informacional. Esta situación, se relaciona con procesos más amplios de gubernamentalidad tecnológica, en los cuales las decisiones sobre el uso de sistemas automatizados de control se desarrollan en marcos institucionales y

técnicos que no siempre son plenamente transparentes para la ciudadanía (Katzenbach & Ulbricht, 2022).

En este sentido, la limitada comprensión sobre estas tecnologías puede dificultar la formación de debates públicos informados sobre sus implicaciones para la privacidad, para los derechos de los ciudadanos y la transparencia institucional.

8 Gobernabilidad algorítmica y confianza institucional

El análisis de las percepciones ciudadanas frente a las tecnologías de vigilancia digital no puede limitarse a su aceptación funcional en términos de seguridad, así como el despliegue de tecnologías de vigilancia digital en el espacio urbano no implica únicamente transformaciones en los mecanismos de control y seguridad, sino también en las formas en que los ciudadanos perciben y legitiman la acción del Estado. Resulta fundamental entonces, examinar cómo estas tecnologías se articulan con la confianza en las instituciones que las implementan, así como con las percepciones sobre el uso, control y protección de los datos personales, para comprender la aceptación o el cuestionamiento de estos sistemas.

En ese sentido, el presente capítulo aborda la relación entre gobernabilidad algorítmica con relación al uso de tecnologías de vigilancia en Medellín y la confianza que los ciudadanos depositan en las instituciones encargadas de su implementación, con especial atención en el papel de la Alcaldía como actor central en la gestión de datos y dispositivos tecnológicos, con los cuales gestiona la seguridad urbana a través del procesamiento de información y el monitoreo de la población.

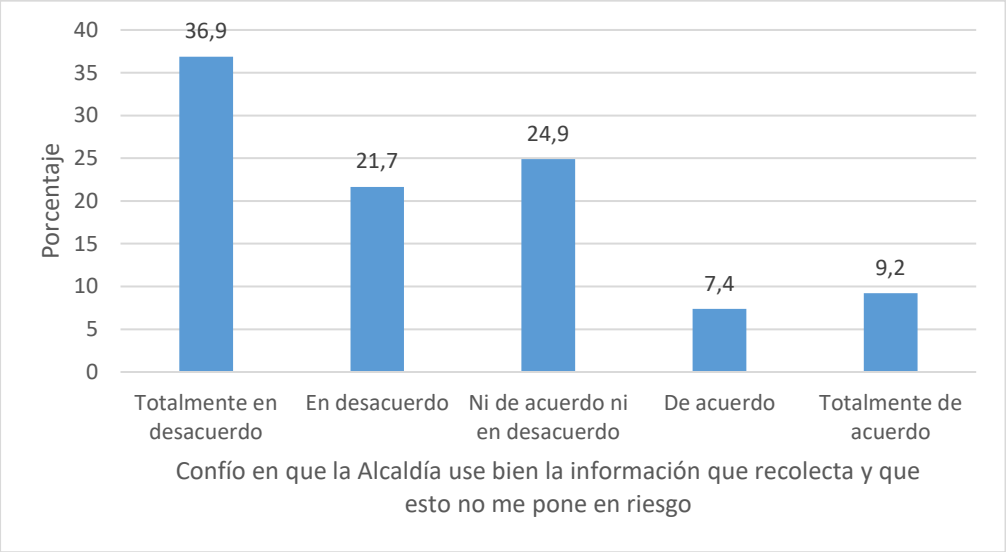
Los resultados empíricos evidencian una configuración particular en la relación entre ciudadanía, tecnología e instituciones, caracterizada por la coexistencia de aceptación tecnológica, desconfianza institucional y preocupación por los datos personales. Esta tensión puede ser interpretada a la luz de distintos enfoques teóricos contemporáneos sobre vigilancia, poder y tecnología.

8.1 Confianza institucional: uso de datos y legitimidad

Los resultados evidencian un bajo nivel de confianza en la Alcaldía respecto al uso de la información recolectada a través de sistemas de vigilancia. Tal como se muestra en la **Figura 1** el 36,9% de los encuestados se encuentra totalmente en desacuerdo con la afirmación de que la Alcaldía utiliza adecuadamente la información sin ponerlos en riesgo, mientras que un 21,7% adicional manifiesta desacuerdo. En conjunto, 58,6% de la muestra expresa desconfianza directa frente al manejo institucional de los datos.

En contraste, únicamente el 16,6% presenta una postura favorable (de acuerdo o totalmente de acuerdo), mientras que el 24,9% adopta una posición neutral.

Figura 1
Confianza institucional



Este resultado muestra que la legitimidad institucional en el manejo de datos es limitada y frágil, lo que sugiere que la aceptación de tecnologías de vigilancia no se traduce automáticamente en confianza hacia las instituciones que las operan. Desde la perspectiva de Michael Foucault, el poder moderno opera a través de dispositivos que organizan la conducta de los individuos más que mediante coerción directa. En *Vigilar y castigar*, plantea que "el poder produce realidad; produce dominios de objetos y rituales de verdad" (Foucault, 1975, p. 194). Entonces, los sistemas de vigilancia no solo controlan, sino que configuran formas de relación entre el Estado y los ciudadanos.

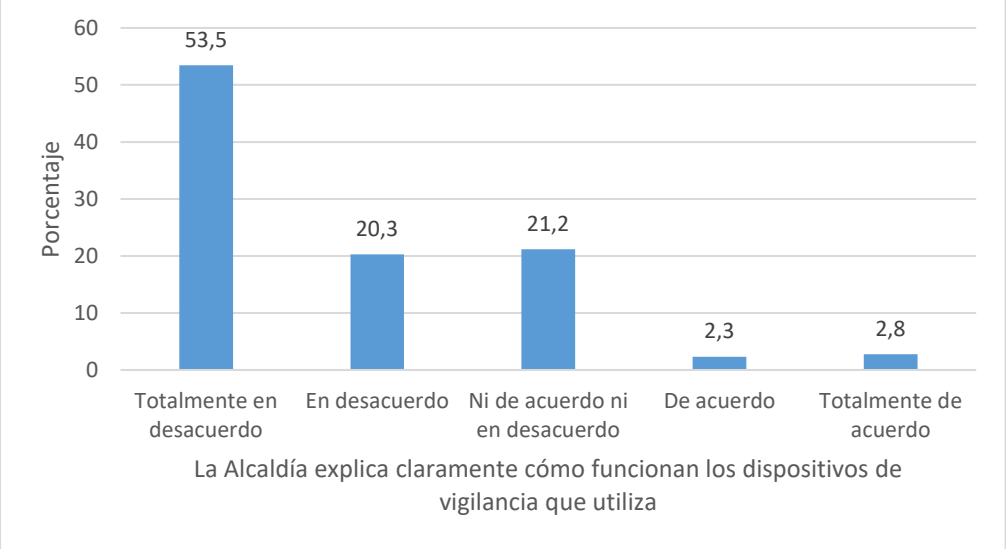
Ahora bien, esta interpretación, relacionada con la percepción ciudadana identificada es clave porque evidencia una ruptura entre tecnología y legitimidad política, donde los dispositivos pueden ser aceptados en abstracto, pero no necesariamente, son aceptados, quienes los gestionan.

8.3 Transparencia institucional: opacidad del sistema

La percepción de transparencia institucional presente resultados aún más contundentes. En la **Figura 2**, el 53,5% de los encuestados se encuentra totalmente en desacuerdo con la afirmación de que la Alcaldía explica claramente el funcionamiento de los dispositivos de vigilancia, y un 20,3% adicional manifiesta desacuerdo. En conjunto, 73,8% percibe falta de claridad o transparencia.

Por otro lado, apenas un 5,1% considera que sí existe claridad, mientras que el 21,2% mantiene una posición neutral.

Figura 2
Transparencia institucional



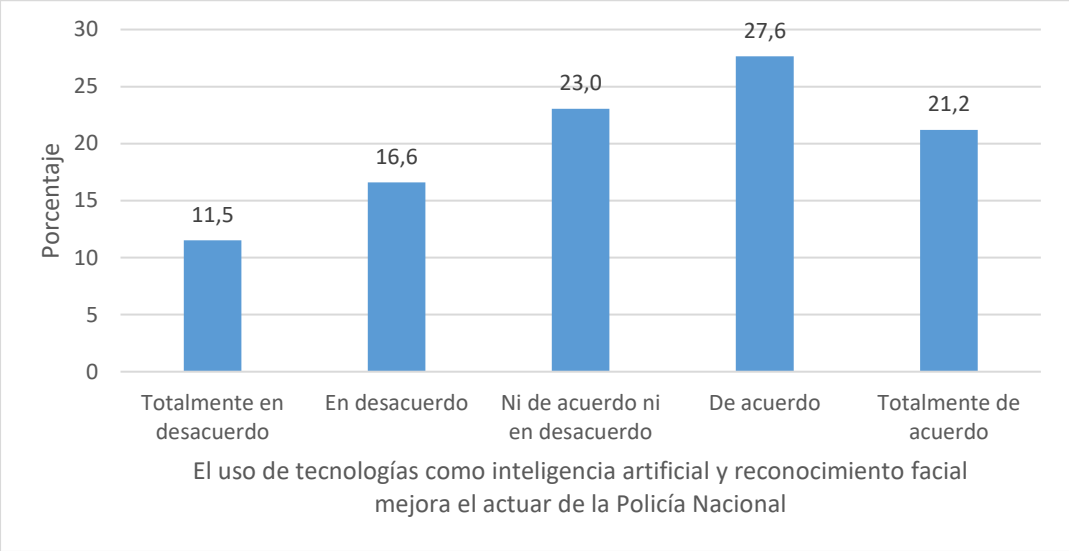
Este resultado permite afirmar que los sistemas de vigilancia operan en un contexto de opacidad institucional percibida, lo cual tiene implicaciones profundas en términos de gobernabilidad. Además, esta opacidad puede interpretarse como una característica central de los sistemas contemporáneos de control, donde las tecnologías funcionan como “cajas negras” para la ciudadanía, dificultando la comprensión y el control social sobre su funcionamiento.

8.4 Gobernabilidad algorítmica: aceptación de la automatización

A pesar de la baja confianza institucional, los datos muestran una aceptación relativa del uso de tecnologías avanzadas en la gestión de seguridad. En la **Figura 3** los datos indican que el 48,8% de los encuestados está de acuerdo o totalmente de acuerdo con que tecnologías como la inteligencia artificial y el reconocimiento facial mejoran el actuar de la policía. En contraste, el 28,1% manifiestas desacuerdo, y el 23% adopta una posición neutral.

Figura 3

Percepción sobre el uso de tecnologías vs actuar de la policía

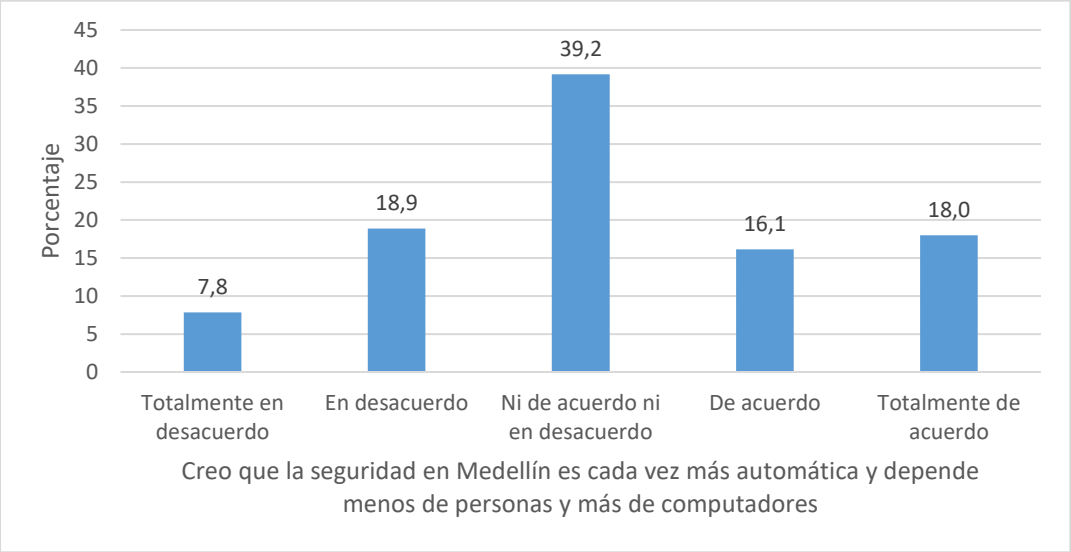


Este resultado refleja lo que David Lyon denomina la normalización de la vigilancia, donde "la vigilancia se ha convertido en una característica rutinaria de la vida cotidiana" (Lyon, 2018, p. 3).

Sin embargo, aunque existe cierto escepticismo, una proporción significativa de la ciudadanía reconoce el potencial de estas tecnologías para mejorar la gestión de la seguridad. En contraposición, cuando se indaga por la percepción de automatización de la seguridad, los resultados (**Figura 4**) muestran mayor ambivalencia. El 39,2% de los encuestados adopta una posición neutral, mientras que el 34,1% está en desacuerdo y el 34,1 está de acuerdo en que la seguridad depende cada vez más de computadores que de personas.

Figura 4

Percepción sobre automatización de la seguridad en Medellín



Este patrón puede interpretarse a partir de lo planteado por Gilles Deleuze (1990), quien sostiene que “las sociedades de control operan mediante mecanismos continuos y sin límites definidos”. Así mismo, en contraposición está la noción de gubernamentalidad algorítmica desarrollada por Christian Katzenbach y Lena Ulbricht, quienes señalan que “la gobernanza algorítmica describe formas de regulación social en las que los algoritmos juegan un papel central en la toma de decisiones” (Katzenbach & Ulbricht, 2022, p. 4).

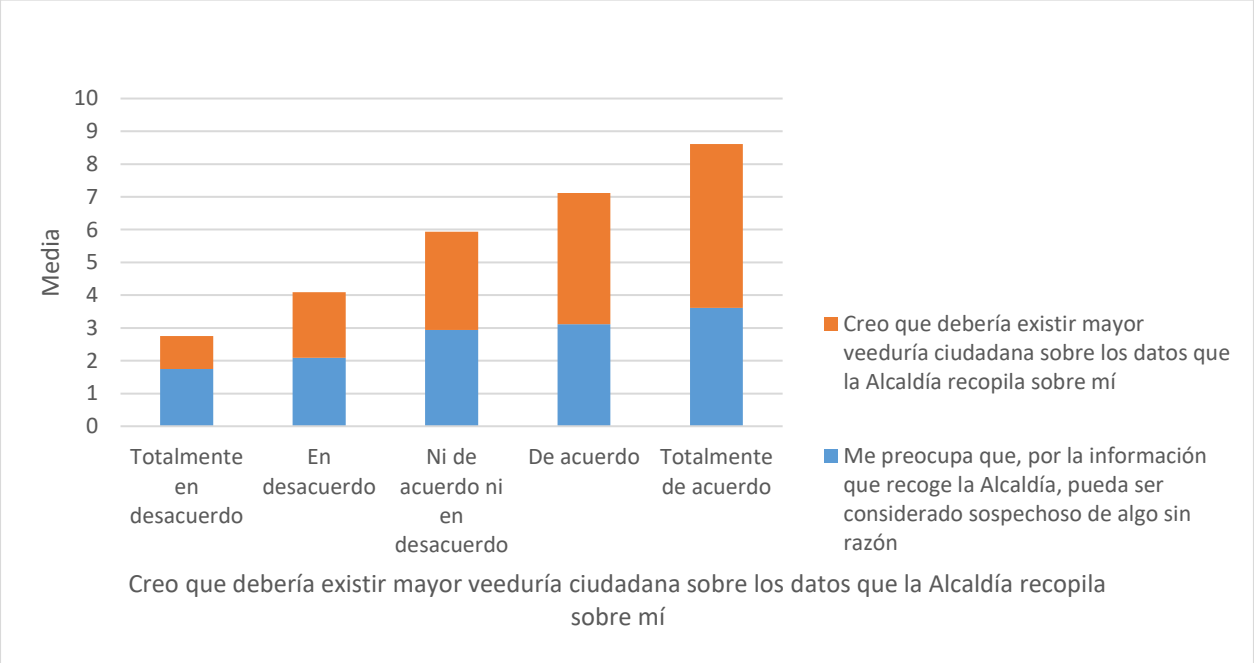
8.5 Ciudadanía, datos y control

La gobernanza digital desplaza la soberanía territorial hacia una **soberanía digital**, donde la autonomía del Estado y la autodeterminación de los usuarios se encuentran en constante tensión (Juri, 2023). Como advierte Bonilla Gutiérrez (2024), la explotación masiva de datos mediante IA erosiona el derecho a la autodeterminación informativa, transformando a los individuos en simples productores involuntarios de insumos para la economía digital. Esta 'sociedad de la transparencia', analizada también por Noain Sánchez (2016) a partir de la obra de Byung-Chul Han, paradójicamente puede 'cegar' en lugar de iluminar si no existen marcos claros de rendición de cuentas.

El análisis de la relación entre ciudadanía y datos personales revela uno de los hallazgos más contundente del estudio. En la

Figura *5* se observa que el 71,9% de los encuestados está de acuerdo o totalmente de acuerdo en que debería existir mayor veeduría ciudadana sobre los datos que la Alcaldía recopila. Este resultado indica una demanda clara de control democrático sobre la información personal.

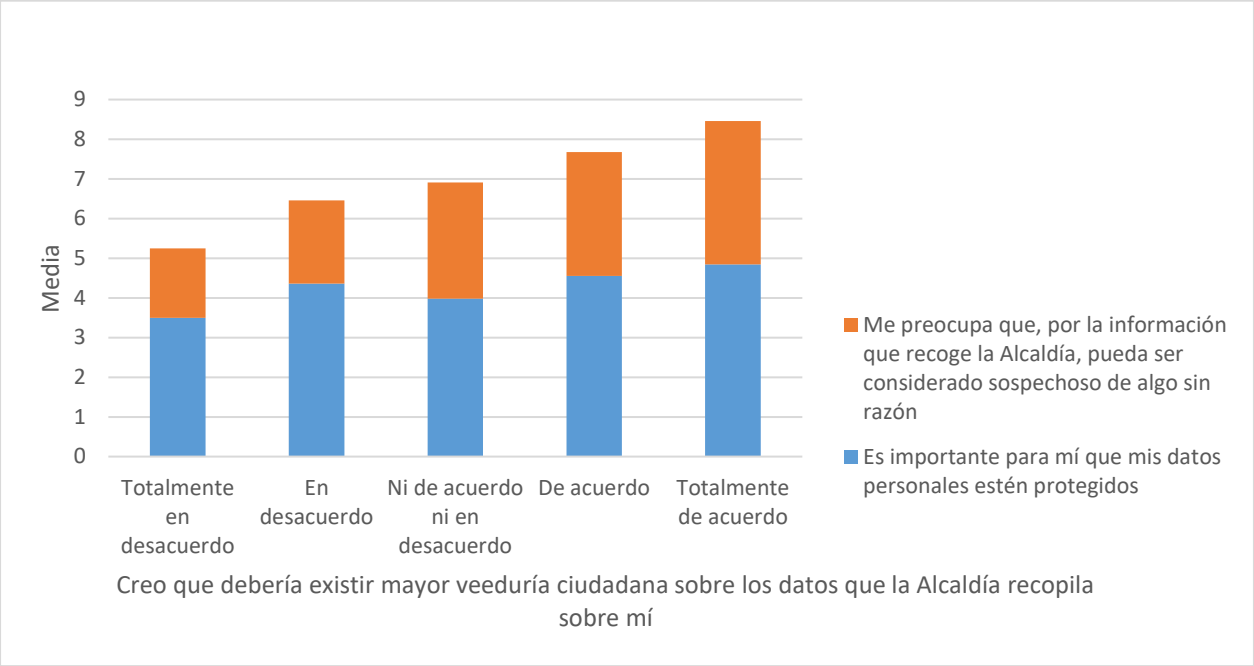
Figura 5
Relación entre veeduría ciudadana y protección de datos



Asimismo, en la **Figura 6**, el 43,8% expresa preocupación por la posibilidad de ser considerado sospechoso injustamente a partir del uso de sus datos, lo que evidencia la percepción de riesgo asociada a los sistemas de vigilancia. Adicionalmente, el 85,7% considera importante que sus datos personales estén protegidos, lo que refleja un consenso casi generalizado sobre la centralidad de la privacidad.

Figura 6

Preocupación por ser considerado sospechoso vs datos personales



Estos resultados dialogan con lo planteado por Byung-Chul Han, quien señala que "la sociedad de la transparencia es una sociedad de la exposición total" (Han, 2013, p. 12). Sin embargo, en el caso analizado, no se observa una transparencia institucional efectiva, sino una acumulación de datos acompañada de incertidumbre. Y, aunque la tecnología puede ser aceptada como herramienta de seguridad, los ciudadanos mantienen una alta sensibilidad frente al uso de sus datos, especialmente en términos de control, protección y posibles abusos.

8.6 Análisis de correlaciones: tensiones estructurales

El análisis de correlaciones permite identificar relaciones significativas entre las variables estudiadas. En primer lugar, como se observa en la **Tabla 9**, hay correlación negativa entre el índice de desarrollo tecnológico y el índice de ciudadanía ($r = -0{,}240$; $p < 0{,}001$). Este resultado indica que, a mayor aceptación o percepción positiva de la tecnología, tiende a disminuir la preocupación o posicionamiento crítico en términos de derechos ciudadanos.

Tabla 9

Correlación de índice de desarrollo tecnológico e índice de ciudadanía

		Indice_DesarrolloTecnológico	Indice_Ciudadanía
Indice_Desarrollo Tecnológico	Correlación de Pearson	1	-,240***
	Sig. (bilateral)		,000
	Suma de cuadrados y productos vectoriales	151,973	-29,365
	Covarianza	,704	-,136
	N	217	217
Indice_Ciudadanía	Correlación de Pearson	-,240***	1
	Sig. (bilateral)	,000	
	Suma de cuadrados y productos vectoriales	-29,365	98,371
	Covarianza	-,136	,455
	N	217	217

***. Correlation at 0.001(2-tailed)

Este hallazgo es particularmente relevante, ya que sugiere la existencia de una tensión estructural entre tecnología y ciudadanía, donde el fortalecimiento de imaginarios tecnológicos puede coexistir con una menor problematización de sus implicaciones sociales y políticas.

Por otro lado, se identifica (**Tabla 10**) una correlación positiva moderada ($r = 0,315$; $p < 0,001$) entre la percepción de mayor vigilancia en los últimos años y la preocupación por ser considerado sospechoso injustamente.

Tabla 10

Correlación de índice de sensación de vigilancia y ser considerado sospechoso por la información recopilada.

		¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?	Me preocupa que, por la información que recoge la Alcaldía, pueda ser considerado sospechoso de algo sin razón
¿Se siente más vigilado en los últimos años debido al aumento	Correlación de Pearson	1	,315***
	Sig. (bilateral)		,000
	Suma de cuadrados y productos vectoriales	426,691	130,705

de cámaras y tecnologías de monitoreo?	Covarianza	1,975	,605
	N	217	217
Me preocupa que, por la información que recoge la Alcaldía, pueda ser considerado sospechoso de algo sin razón	Correlación de Pearson	,315***	1
	Sig. (bilateral)	,000	
	Suma de cuadrados y productos vectoriales	130,705	403,539
	Covarianza	,605	1,868
	N	217	217

***. Correlation at 0.001(2-tailed)

Esto indica que, a mayor percepción de vigilancia, mayor es también la percepción de riesgo, lo que refuerza la idea de que los sistemas de monitoreo no solo generan sensación de seguridad, sino también de exposición y vulnerabilidad.

Esta distribución de resultados evidencia que la ciudadanía no tiene una posición consolidada frente a la automatización de control, la opacidad no es accidental, sino estructural: los sistemas funcionan como cajas negras, dificultando el acceso ciudadano a su lógica de operación, y que la necesidad de una mayor veeduría sugiere un proceso de reconfiguración de las formas de autoridad y vigilancia. En ese sentido, la ambivalencia observada sugiere que la ciudadanía percibe la transformación del control, pero aún no consolida una posición clara frente a ella.

8.7 Discusión: la tensión entre tecnología, confianza y ciudadanía

Los resultados presentados permiten identificar una configuración compleja en la relación entre ciudadanía, tecnología e instituciones.

Por un lado, existe una aceptación significativa del uso de tecnologías de vigilancia como herramientas para mejorar la seguridad. Por otro, se evidencia una fuerte desconfianza institucional, una percepción de opacidad en el funcionamiento de los sistemas y una alta preocupación por el uso de los datos personales. Esta combinación configura un escenario que puede definirse como de *aceptación tecnológica con desconfianza institucional*.

Este fenómeno puede interpretarse como una expresión de la gubernamentalidad algorítmica, donde el control social se ejerce a través de sistemas tecnológicos que operan con niveles limitados de transparencia y participación ciudadana. En este contexto, los ciudadanos no rechazan necesariamente la tecnología, pero sí cuestionan las condiciones bajo las cuales es implementada, especialmente en lo relacionado con la protección de derechos, la transparencia y la rendición de cuentas, dando lugar a un escenario caracterizado por: aceptación de la tecnología, desconfianza hacia las instituciones y demanda de control sobre los datos.

Entonces, estos resultados constituyen un aporte central de la investigación, al evidenciar que la legitimidad de la vigilancia digital no depende únicamente de su eficacia técnica, sino que al reivindicar el papel de los ciudadanos como garantes del uso que se le dan a los dispositivos tecnológicos y de los datos personales, y que también termina por articularse con principios de transparencia, confianza y derechos ciudadanos.

9 Derechos, privacidad y agencia ciudadana

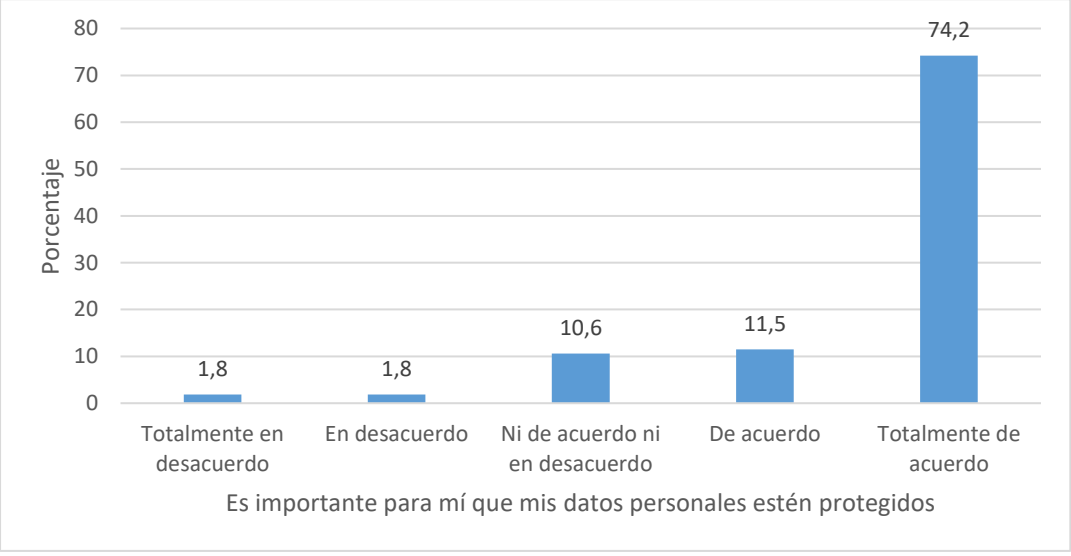
El despliegue de tecnologías de vigilancia digital en el espacio urbano no solo redefine las estrategias de seguridad, sino que introduce nuevas tensiones en torno a los derechos fundamentales, la privacidad y la capacidad de acción de los ciudadanos.

En este capítulo se examina cómo los habitantes de Medellín interpretan el uso de sus datos personales, qué preocupaciones emergen frente a posibles vulneraciones de derechos y de qué manera la presencia de tecnologías de vigilancia influye en su comportamiento cotidiano en el espacio urbano.

9.1 Centralidad de la privacidad en la percepción ciudadana

Los resultados evidencian que la proyección de los datos personales constituye una preocupación ampliamente extendida entre los ciudadanos. En la **Figura 7** el 85,7% de los encuestados considera importante que sus datos personales estén protegidos, lo que refleja un consenso casi generalizado sobre la relevancia de la privacidad en el contexto de la vigilancia digital.

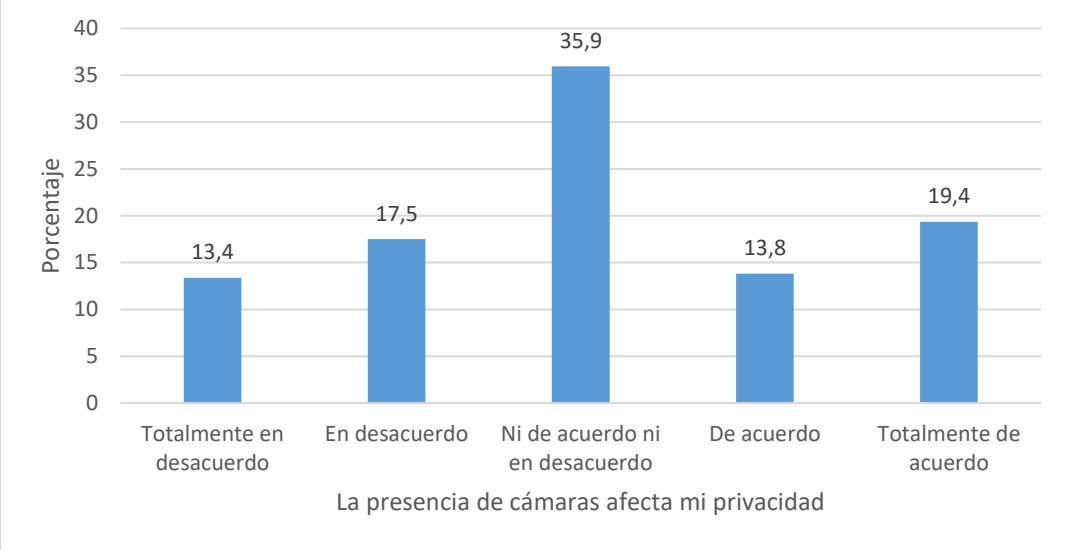
Figura 7
Importancia de la protección de los datos



Adicional a lo anterior, al indagar directamente por el impacto de las cámaras sobre la privacidad, los resultados muestran una distribución más ambivalente: el 33,2% considera que las cámaras afectan su privacidad, mientras que el 30,9% no lo percibe así, y un 35,9% se mantiene neutral, tal como se muestra en la **Figura 8**.

Figura 8

Afectación de la privacidad por presencia de cámaras de vigilancia



Este contraste es clave, ya que, aunque existe un alto consenso sobre la importancia de la privacidad, no hay una percepción homogénea sobre su vulneración directa, lo que sugiere una tensión entre principios normativos y experiencias cotidianas.

Este hallazgo puede interpretarse a partir de los planteado por David Lyon, quien afirma que “la vigilancia contemporánea se centra cada vez más en la recopilación y el procesamiento de datos personales” (Lyon, 2018, p. 5). En ese sentido, la preocupación por la privacidad no implica necesariamente una percepción clara de su afectación inmediata, sino una conciencia más amplia sobre el valor de la información personal, así también, una respuesta a la creciente centralidad de la información en los sistemas de control.

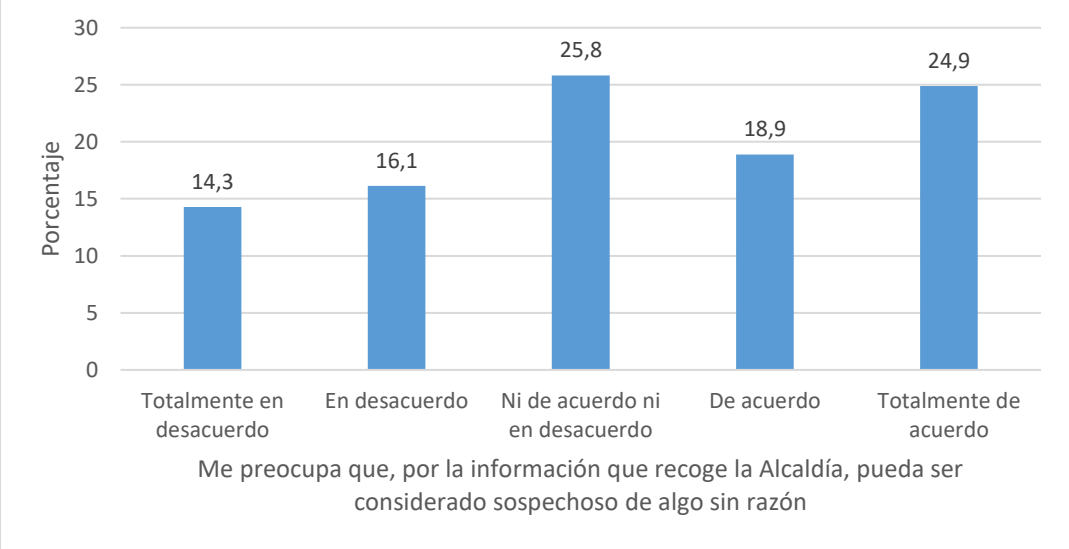
9.2 Percepción de riesgo y producción de sospecha

Más allá de la importancia atribuida a la privacidad, los datos muestran la existencia de una preocupación significativa por los efectos de la vigilancia en términos de sospecha y clasificación social. Esto además se asocia no solo con seguridad, sino también con la idea de riesgo.

El 43,8% de los encuestados, como se observa en la **Figura 9** expresa preocupación por ser considerado sospechoso injustamente, lo que evidencia la percepción de que los sistemas de vigilancia pueden producir clasificaciones erróneas o sesgadas.

Figura 9

Preocupación por el riesgo de ser señalado o parecer sospechoso



Este resultado permite evidenciar que la vigilancia no solo se percibe como un mecanismo de seguridad, sino también como un sistema potencial de producción de riesgo para el ciudadano. Desde la perspectiva de Michel Foucault, el poder disciplinario no solo vigila, sino que clasifica y produce categorías de normalidad y desviación. Como señala: “el examen combina las técnicas de la jerarquía que vigila y las de la sanción que normaliza” (Foucault, 1975, p. 184).

Es así que, la preocupación por ser considerado sospechoso refleja la internalización de un sistema donde el individuo puede ser evaluado constantemente a partir de los datos, la identificación de patrones y la forma en la que se dan los comportamientos de los individuos en el

espacio público. En ese sentido, la vigilancia no solo observa, sino que clasifica y produce categorías.

9.3 Vigilancia y percepción de exposición

El análisis de correlaciones evidenciado en la **Tabla *11*** Percepción de vigilancia vs preocupación por ser considerado sospechoso **Tabla 11** muestra que existe una relación significativa entre la percepción de mayor vigilancia y la preocupación por ser considerado sospechoso ($r = 0{,}315$; $p < 0{,}001$), lo que indica que, a mayor percepción de vigilancia, mayor percepción de riesgo.

Tabla 11

Percepción de vigilancia vs preocupación por ser considerado sospechoso

Correlaciones

		¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?	Me preocupa que, por la información que recoge la Alcaldía, pueda ser considerado sospechoso de algo sin razón
¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?	Correlación de Pearson	1	,315***
	Sig. (bilateral)		,000
	Suma de cuadrados y productos vectoriales	426,691	130,705
	Covarianza	1,975	,605
	N	217	217
Me preocupa que, por la información que recoge la Alcaldía, pueda ser considerado sospechoso de algo sin razón	Correlación de Pearson	,315***	1
	Sig. (bilateral)	,000	
	Suma de cuadrados y productos vectoriales	130,705	403,539
	Covarianza	,605	1,868
	N	217	217

***. Correlation at 0.001(2-tailed)

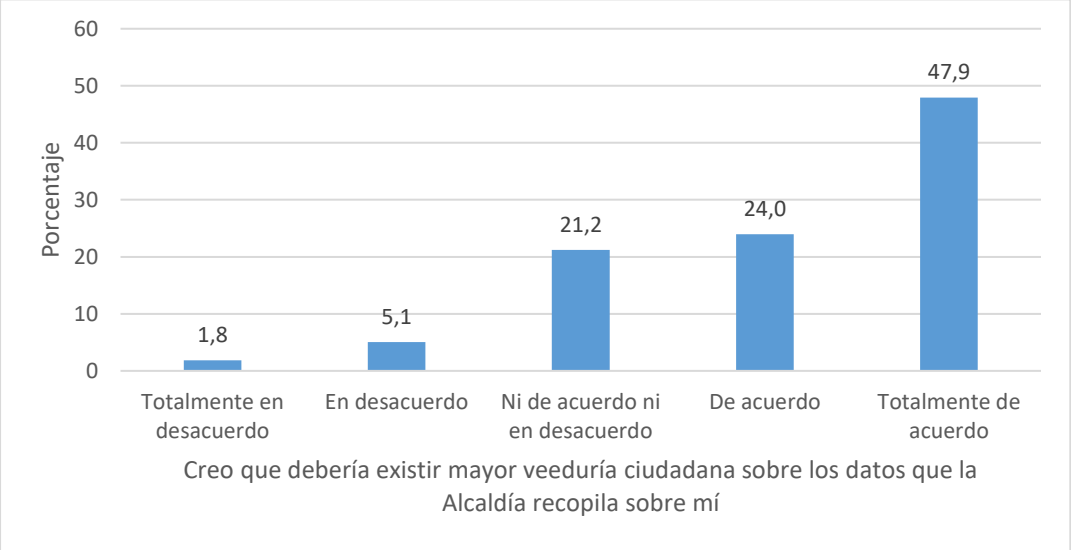
Este resultado indica que los sistemas de vigilancia no solo producen efectos de control, sino también de exposición.

Este fenómeno puede interpretarse a partir de los planteado por Byung-Chul Han, quien señala que “la sociedad de la vigilancia digital no se basa en la prohibición, sino en la exposición voluntaria de los sujetos” (Han, 2013, p. 21). Sin embargo, en el caso analizado, esta exposición no parece ser plenamente voluntaria, sino más bien percibida como parte de una infraestructura urbana de la cual no es posible sustraerse.

9.4 Demanda de control ciudadano sobre los datos

Uno de los hallazgos más contundentes del estudio es la alta demanda de mecanismos de control ciudadano sobre la información personal. El 71,9% de los encuestados considera que debería existir mayor veeduría ciudadana sobre los datos que la Alcaldía recopila.

Figura 10
Veeduría ciudadana requerida por la ciudadanía



Este resultado evidencia que los ciudadanos no solo reconocen la importancia de la privacidad, sino que también demandan participación y control en la gestión de sus datos **(Figura 10)**. Desde el enfoque de la gobernanza digital, esto se relaciona con lo planteado por Christian Katzanbach, quien señala que “la gobernanza de los datos implica disputas sobre quién tiene el control, la capacidad de decisión y la legitimidad sobre los sistemas tecnológicos” (Katzenbach, 2022, p. 7). La tecnología de vigilancia también se utiliza para ejercer controles territoriales,

permitiendo excluir a sectores considerados 'indeseables' de ciertos espacios urbanos (Palmer y Warren, 2012). Frente a esto, Arce Jiménez (2022) sostiene que la ciudadanía digital requiere una reconfiguración para proteger la identidad del individuo en un entorno donde el 'yo analógico' y el 'yo digital' conviven bajo la mediación de algoritmos. En Medellín, esto se conecta con la agencia ciudadana, donde los sujetos no son solo usuarios, sino actores capaces de desarrollar competencias críticas frente al monitoreo y la recopilación de datos (Vázquez, 2025).

9.5 Agencia ciudadana y transformación del comportamiento

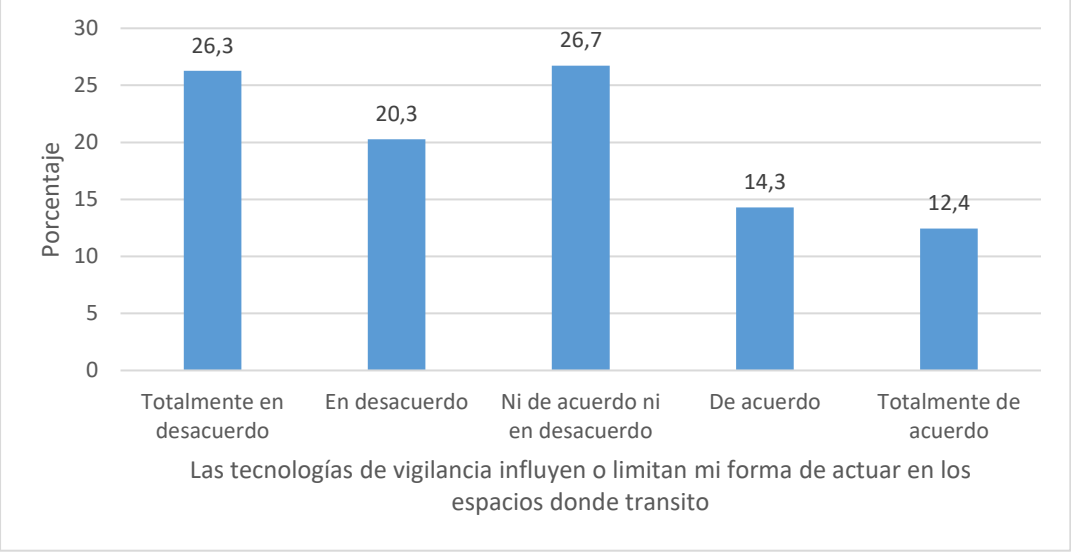
En el análisis, la capacidad de agencia ciudadana, permite identificar en qué medida la vigilancia influye en el comportamiento de los individuos. Los resultados (

Figura *11*) muestran que el 46,6% de los encuestados está en desacuerdo con la idea de que las tecnologías de vigilancia limitan su forma de actuar, mientras que el 26,7% adopta una posición neutral y el 26,7% considera que sí existe influencia o limitación.

Este hallazgo tiene valor, debido a que sugiere que la vigilancia no produce un efecto homogéneo sobre la conducta: mientras una parte de la población no percibe cambios en su comportamiento, otra sí reconoce una influencia directa. Tal como lo afirma Gilles Deleuze (1990), “los mecanismos de control funcionan mediante modulaciones continuas del comportamiento”.

Figura 11

Tecnologías de vigilancia y limitación del comportamiento



En ese sentido, la vigilancia no necesariamente impone restricciones explícitas, sino que introduce condiciones que pueden influir de manera diferenciada en los sujetos. De la misma manera, desde la perspectiva de Byung-Chul Han, "el sujeto se explica a sí mismo creyéndose libre" (Han, 2013, p. 9), lo que permite entender cómo el control puede operar sin ser plenamente percibido.

9.6 Diferencias sociodemográficas en la percepción de la privacidad y la agencia

El análisis de las tablas cruzadas permite identificar diferencias en la percepción de la privacidad y la agencia según variables sociodemográficas.

En relación con la edad, se observa en la **Tabla 12** que los grupos entre 19 y los 30 años, y 31 y 59 años concentran mayor diversidad de percepciones, con una alta presencia de respuestas neutrales y distribuciones relativamente equilibradas entre acuerdo y desacuerdo.

Tabla 12

Diferencias entre percepción de privacidad según variable de edad

		La presencia de cámaras afecta mi privacidad					Total
		Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo	
Selecciona el rango de edad en el que te encuentras	60 años en adelante	0	0	0	1	0	1
	Entre 12-18 años	1	0	1	1	0	3
	Entre 19-30 años	13	22	47	13	20	115
	Entre 31-59 años	15	16	30	15	22	98
Total		29	38	78	30	42	217

Por otro lado, el cruce entre nivel educativo y percepción de limitación del comportamiento muestra que la percepción de influencia de la vigilancia se distribuye en todos los niveles educativos, aunque con ligeras variaciones en la intensidad de las respuestas.

Tabla 13

Relación del nivel educativo con la capacidad de agencia

		Las tecnologías de vigilancia influyen o limitan mi forma de actuar en los espacios donde transito					Total
		Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo	
¿Cuál es tu nivel educativo?	Posgrado	10	6	6	3	3	28
	Pregrado	20	15	28	16	12	91
	Secundaria	9	5	6	2	3	25
	Técnico/Tecnológico	18	18	18	10	9	73
Total		57	44	58	31	27	217

Estos resultados indican que la percepción de vigilancia no está determinada de manera directa por factores sociodemográficos, sino que responde a una combinación de experiencias, niveles de información y posicionamientos individuales frente a la tecnología.

9.7 Discusión: derechos, vigilancia y ciudadanía en tensión.

El análisis de los resultados, permiten identificar que la vigilancia digital en Medellín configura un escenario complejo en el que los derechos ciudadanos se encuentran en constante tensión. En primer lugar, se evidencia un alto consenso sobre la importancia de la privacidad, acompañado de una percepción heterogénea sobre su afectación directa.

En segundo lugar, la vigilancia es asociada no solo con seguridad, sino también con riesgo, clasificación y posible vulnerabilidad, especialmente en relación con el uso de datos personales. En tercer lugar, la agencia ciudadana se presenta de manera diferenciada: mientras algunos individuos no perciben cambios en su comportamiento, otros reconocen que la vigilancia influye en sus prácticas cotidianas.

En conjunto, estos elementos configuran una ciudadanía que no es pasiva frente a la vigilancia, sino que se encuentra en un proceso de negociación constante entre seguridad, derechos y autonomía.

10 Tipologías ciudadanas frente a la vigilancia digital

Los análisis descriptivos y correlacionales desarrollados en los capítulos anteriores evidencian que la percepción ciudadana frente a la vigilancia digital en Medellín no es homogénea. Por el contrario, se identifican tensiones entre aceptación tecnológica, desconfianza institucional y preocupación por los derechos.

Con el fin de avanzar hacia una comprensión más profunda de estas diferencias, se implementó un análisis de conglomerados (cluster análisis), que permite identificar perfiles o tipologías de ciudadanos a partir de patrones similares de respuesta en las variables analizadas. Este enfoque permite superar la descripción general de tendencias y avanzar hacia la identificación de formas diferenciadas de relación con la vigilancia digital, lo cual constituye el aporte central de la investigación.

10.1 Metodología de análisis de clusters

El análisis de conglomerados se realizó a partir de los índices construidos en el procesamiento de datos en SPSS (**Tabla 13**):

- Índice de Desarrollo Tecnológico
- Índice de Gobernabilidad Algorítmica
- Índice de Ciudadanía

Tabla 14

Medias por cluster

	N	Mínimo	Máximo	Media	Desv. estándar
Indice_DesarrolloTecnológico	217	1,00	5,00	2,7889	,83880
Indice_GobernabilidadAlgorítmica	217	1,43	5,00	3,2462	,78085
Indice_Ciudadanía	217	2,00	5,00	3,3065	,67485
N válido (por lista)	217				

Se utilizó un método de clasificación K-medias, agrupando los casos en función de su proximidad en estas dimensiones. Este tipo de análisis permite identificar estructuras latentes en los datos, agrupando individuos con características similares en conjuntos interpretables sociológicamente.

Con el fin de profundizar en la comprensión de las diferencias entre las tipologías ciudadanas identificadas mediante análisis de clúster, se implementaron técnicas de análisis bivariado, específicamente tablas cruzadas acompañadas de la prueba de chi-cuadrado de Pearson.

Las tablas cruzadas permitieron examinar la distribución de las respuestas en variables clave —como la confianza institucional, la percepción de vigilancia y la afectación a la privacidad— en función de los distintos tipos de ciudadanía. Este tipo de análisis es ampliamente utilizado en estudios de enfoque cuantitativo para identificar patrones de asociación entre variables categóricas, facilitando una lectura comparativa entre grupos (Hernández Sampieri et al., 2014).

No obstante, más allá de la descripción de frecuencias y porcentajes, se recurrió a la prueba de chi-cuadrado con el propósito de evaluar la existencia de asociaciones estadísticamente significativas entre las variables analizadas. De acuerdo con Andy Field, esta prueba permite determinar si existe una relación entre variables categóricas al contrastar la hipótesis nula de independencia, es decir, si las diferencias observadas pueden atribuirse al azar o si responden a una estructura subyacente en los datos (Field, 2013).

En este sentido, la hipótesis nula plantea que no existe relación entre las tipologías ciudadanas y las percepciones analizadas, mientras que la hipótesis alternativa sostiene que sí existe una asociación significativa entre estas variables. La interpretación de los resultados se realizó a partir del valor de significación (p-valor), considerando como criterio de decisión un nivel de significancia de 0,05, tal como es estándar en investigaciones sociales (Hernández Sampieri et al., 2014).

Los resultados obtenidos evidenciaron niveles de significación inferiores a 0,001 en los cruces analizados, lo que indica una asociación estadísticamente significativa entre el tipo de ciudadanía y variables como la confianza en el uso institucional de los datos, la percepción de afectación a la privacidad y la intensificación de la vigilancia. En consecuencia, se rechaza la

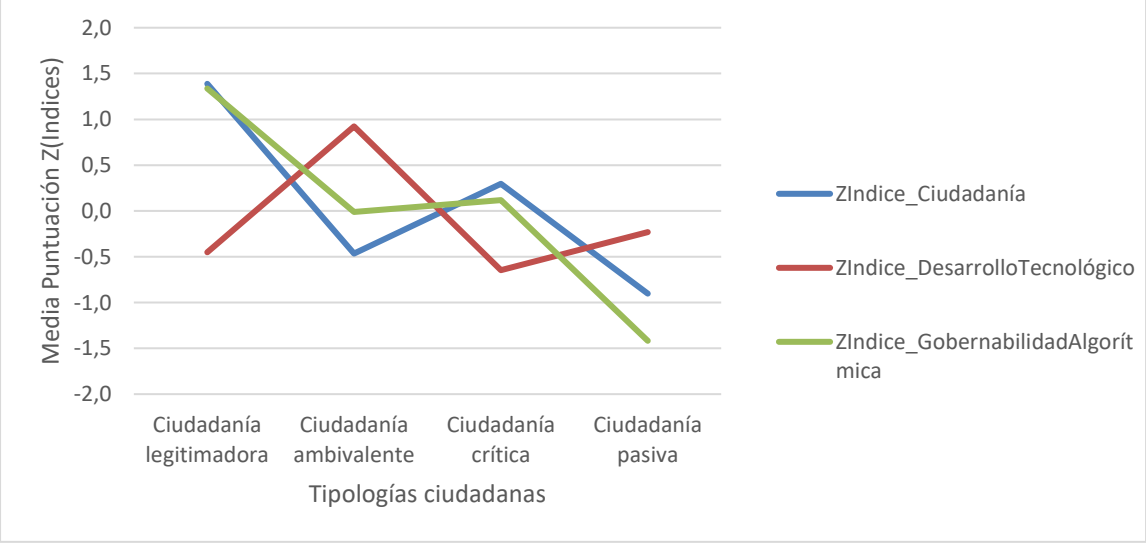
hipótesis nula de independencia, confirmando que las diferencias observadas entre los clústeres no son aleatorias.

Adicionalmente, como señala Andy Field, es importante considerar las frecuencias esperadas en cada celda de la tabla, ya que valores muy bajos pueden afectar la robustez de la prueba. En el presente estudio, aunque se identificaron algunas celdas con frecuencias esperadas menores a cinco, esta situación no compromete la validez global del análisis, dado que representa un porcentaje reducido del total y se mantiene la consistencia en los niveles de significación obtenidos (Field, 2013). Por lo que este análisis permite afirmar que las tipologías ciudadanas identificadas no solo constituyen agrupaciones estadísticas, sino que se asocian de manera significativa con percepciones diferenciadas sobre el uso de tecnologías de vigilancia.

10.2 Caracterización de las tipologías ciudadanas desde una perspectiva teórica.

A partir del análisis realizado, se identificaron cuatro tipologías (**Figura 12**) ciudadanas frente a la vigilancia digital.

Figura 12
Perfiles de las tipologías ciudadanas según índices estandarizados



El gráfico anterior permite visualizar la configuración estructural de las tipologías ciudadanas identificadas, evidenciando que la relación entre desarrollo tecnológico, gobernabilidad algorítmica y ciudadanía no es homogénea, sino que se distribuya en patrones diferenciados. Esta diferenciación empírica se corresponde con lo que Michel Foucault denominó una dispersión de las formas de subjetivación, en donde los individuos no responden de manera uniforme a los dispositivos de poder, sino que los internalizan, resisten o ignoran de formas diversas.

10.2.1 Ciudadanía legitimadora

La ciudadanía legitimadora se caracteriza por una alta aceptación del uso de tecnologías de vigilancia, incluso cuando reconoce su presencia de manera intensiva. Este grupo presenta una aparente paradoja que resulta central para comprender la relación contemporánea entre ciudadanía y vigilancia. Aunque concentra altos niveles de percepción de vigilancia, como se observa en la **Tabla 17** (71,4% afirma sentirse "mucho" más vigilado), no traduce esta experiencia en una desconfianza hacia las instituciones, sino que indica una clara conciencia de los dispositivos de monitoreo. Por el contrario, como se observa en la **Tabla 16**, el 68,8% se ubica en "Totalmente en desacuerdo" frente a la afirmación de desconfianza, lo que indica una aceptación tácita del uso institucional de los datos.

Esta aparente contradicción se profundiza cuando se analiza la dimensión de privacidad, tal como se evidencia en la **Tabla 15**, donde se identificó una relación estadísticamente significativa entre las tipologías ciudadanas y la percepción de afectación a la privacidad ($\chi^2 = 143{,}770$; $p < 0{,}001$), lo que sugiere que la manera en que los individuos experimentan la vigilancia tecnológica varía significativamente según el tipo de ciudadanía al que pertenecen.

Tabla 15

Relación entre tipologías ciudadanas y percepción de afectación a la privacidad

Tabla cruzada Número de caso de clúster*La presencia de cámaras afecta mi privacidad

		La presencia de cámaras afecta mi privacidad					Total
		Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo	
Ciudadanía legitimadora	Recuento	0	1	1	6	27	35
	% dentro de Número de caso	0,0%	2,9%	2,9%	17,1%	77,1%	100,0%
Ciudadanía ambivalente	Recuento	14	16	37	8	0	75
	% dentro de Número de caso	18,7%	21,3%	49,3%	10,7%	0,0%	100,0%
Ciudadanía crítica	Recuento	2	7	32	13	15	69
	% dentro de Número de caso	2,9%	10,1%	46,4%	18,8%	21,7%	100,0%
Ciudadanía pasiva	Recuento	13	14	8	3	0	38
	% dentro de Número de caso	34,2%	36,8%	21,1%	7,9%	0,0%	100,0%
Total	Recuento	29	38	78	30	42	217
	% dentro de Número de caso	13,4%	17,5%	35,9%	13,8%	19,4%	100,0%

Esta combinación sugiere una forma de ciudadanía que naturaliza la vigilancia como condición de seguridad, incluso cuando es plenamente consciente de su presencia. En términos analíticos, no se trata de ignorancia, sino de una legitimación consciente del control, donde la seguridad justifica la exposición.

Sin embargo, esta legitimación no elimina tensiones: el 77,1% reconoce que las cámaras afectan su privacidad tal como se evidencia en la **Tabla 15**. Esto evidencia una forma de subjetividad que acepta la pérdida de privacidad como un costo necesario, lo que puede leerse como una internalización de las lógicas de gobierno algorítmico.

Desde una perspectiva foucaultiana, esto puede interpretarse como una forma de internalización del poder disciplinario, en la que el control no se impone únicamente desde afuera, sino que es asumido como legítimo por los propios sujetos. En palabras de Michel Foucault, "el poder produce realidad; produce dominios de objetos y rituales de verdad" (Foucault, 1975, p. 194). En este caso, la vigilancia se constituye como una verdad aceptada en nombre de la seguridad.

Por su parte, David Lyon plantea que en las sociedades contemporáneas la vigilancia se normaliza a través de procesos de legitimación social, donde los ciudadanos aceptan ser observados a cambio de beneficios percibidos, Como afirma el autor, "la vigilancia se ha vuelto una característica rutinaria de la vida cotidiana" (Lyon, 2007, p. 14). En este caso, la tecnología es percibida principalmente como una herramienta de seguridad, sin que se evidencie una preocupación significativa por sus implicaciones en términos de derechos.

10.2.2 Ciudadanía crítica

La ciudadanía crítica constituye el grupo que articula de manera más clara la relación entre vigilancia, poder y riesgo. Como se evidencia en la **Tabla 16**:

Tabla 16

Relación entre tipologías ciudadanas y niveles de confianza institucional en el uso de datos

Tabla cruzada Número de caso de clúster*Confío en que la Alcaldía use bien la información que recolecta y que esto no me pone en riesgo

		Confío en que la Alcaldía use bien la información que recolecta y que esto no me pone en riesgo					Total
		Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo	
Ciudadanía legitimadora	Recuento	24	4	4	0	3	35
	% dentro de Número de caso	68,6%	11,4%	11,4%	0,0%	8,6%	100,0%
Ciudadanía ambivalente	Recuento	7	10	32	13	13	75
	% dentro de Número de caso	9,3%	13,3%	42,7%	17,3%	17,3%	100,0%

Ciudadanía crítica	Recuento	39	20	9	1	0	69
	% dentro de Número de caso	56,5%	29,0%	13,0%	1,4%	0,0%	100,0%
Ciudadanía pasiva	Recuento	10	13	9	2	4	38
	% dentro de Número de caso	26,3%	34,2%	23,7%	5,3%	10,5%	100,0%
Total	Recuento	80	47	54	16	20	217
	% dentro de Número de caso	36,9%	21,7%	24,9%	7,4%	9,2%	100,0%

Los resultados evidencian una relación estadísticamente significativa entre las tipologías ciudadanas y la confianza institucional en el uso de los datos ($\chi^2 = 85{,}887$; $p < 0{,}001$), como ya se ha indicado, estas responden a patrones diferenciados en la forma en que los ciudadanos interpretan el uso institucional de la información.

En la **Tabla 16,** se muestra que el 85,5% se ubica entre el desacuerdo y el total desacuerdo frente a la confianza institucional, lo que refleja una postura claramente desconfiada frente al uso de los datos por parte de la Alcaldía. A diferencia del grupo legitimador, aquí la percepción de vigilancia sí se traduce en una problematización política.

Este grupo presenta además una alta percepción de vigilancia (62,3% entre "bastante" y "mucho" más vigilado), indicando que la experiencia de monitoreo no es neutral, sino interpretada como potencialmente problemática. Asimismo, aunque hay presencia de respuestas neutrales en privacidad, se observa una tendencia creciente hacia el reconocimiento de afectaciones.

En este sentido, la ciudadanía crítica no rechaza necesariamente la tecnología en sí misma, sino su uso sin garantías claras. Se configura así como una ciudadanía que articula vigilancia, poder y riesgo, en línea con marcos analíticos de control social.

Desde la perspectiva de David Lyon, esto puede interpretarse como una forma de conciencia vigilante, donde los sujetos reconocen que los sistemas de monitoreo no son neutrales, sino que implican relaciones de poder y posibles formas de clasificación social.

En esta misma línea, Michel Foucault plantea que el poder moderno opera a través de dispositivos que permiten observar, clasificar y normalizar a los individuos. La ciudadanía crítica, en este sentido, no solo experimenta la vigilancia, sino que la interpreta como un mecanismo de control, quien además sostiene que el poder no solo se ejerce, sino que también es objeto de

resistencia. Como señala: “allí donde hay poder, hay resistencia” (Foucault, 1975, p.95). Adicionalmente, Byung-Chul Han sugiere que en la sociedad contemporánea el control ya no se ejerce únicamente mediante la coerción, sino a través de la autoexposición y la gestión de los datos. Entonces, esta ciudadanía parece resistirse parcialmente a esta lógica, al mantener una postura de sospecha frente al uso institucional de la información, lo que permite clasificarla también como una ciudadanía reflexiva, capaz de problematizar los efectos de la vigilancia en la vida cotidiana.

10.2.3 Ciudadanía ambivalente

La ciudadanía ambivalente se configura como un grupo caracterizado por la indecisión y la falta de posicionamiento claro frente a la vigilancia. Como se evidenció previamente (**Tabla 16**), el 42,7% presenta respuestas neutrales en relación con la confianza institucional, mientras que el 49,3% se mantiene en posiciones intermedias frente a la afectación de la privacidad.

Este patrón sugiere la existencia de una zona de indeterminación cognitiva o incertidumbre cognitiva y política, en la que ls sujetos no cuentan con los elementos suficientes para evaluar críticamente el impacto de las tecnologías. Más que apatía, se trata de una forma de incertidumbre estructural frente a sistemas complejos y opacos.

En ese sentido, Byung-Chul Han advierte que en la sociedad digital contemporánea el exceso de información no produce necesariamente mayor comprensión, sino nuevas formas de confusión. Como señala: “la transparencia no ilumina, sino que puede cegar” (Han, 2013, p. 23). Esta ciudadanía se mueve precisamente en ese espacio de ambigüedad.

Asimismo, esta ambivalencia puede leerse a la luz de David Lyon, quien plantea que los sujetos contemporáneos participan en sistemas de vigilancia sin comprender plenamente sus implicaciones, lo que genera una aceptación pasiva o no reflexiva.

Esta interpretación se refuerza con la percepción de vigilancia distribuida, es decir, aunque una parte significativa reconoce sentirse vigilada, no hay una traducción consistente en términos de confianza o rechazo. Esto configura una ciudadanía que oscila entre la aceptación y la sospecha, sin consolidar una postura definida.

Desde la perspectiva de Gilles Deleuze, las sociedades contemporáneas se caracterizan por transformaciones continuas que dificultan la consolidación de posiciones estables. Como plantea: “los controles son modulaciones, como un molde que cambia continuamente” (Deleuze, 1990, p.

4). Este perfil es particularmente relevante, ya que representa una ciudadanía en proceso de formación de opinión frente a la vigilancia digital.

10.2.4 Ciudadanía pasiva

Este grupo representa el nivel más bajo de implicación frente a la vigilancia digital. Se caracteriza por una baja percepción de vigilancia y una escasa problematización de sus implicaciones. Como se evidencia en la **Tabla 17** El 89,5% se ubica entre "nada" y "poco" en percepción de vigilancia, lo que indica una baja conciencia sobre la presencia de dispositivos de monitoreo.

Tabla 17

Relación entre tipologías ciudadanas y percepción de intensificación de la vigilancia

Tabla cruzada Número de caso de clúster*¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?

		¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?					Total
		Nada	Poco	Neutral / Algo	Bastante	Mucho	
Ciudadanía legitimadora	Recuento	0	0	5	5	25	35
	% dentro de Número de caso de clúster	0,0%	0,0%	14,3%	14,3%	71,4%	100,0%
Ciudadanía ambivalente	Recuento	9	7	25	18	16	75
	% dentro de Número de caso de clúster	12,0%	9,3%	33,3%	24,0%	21,3%	100,0%
Ciudadanía crítica	Recuento	6	8	12	26	17	69
	% dentro de Número de caso de clúster	8,7%	11,6%	17,4%	37,7%	24,6%	100,0%
	Recuento	19	15	3	1	0	38

Ciudadanía pasiva	% dentro de Número de caso de clúster	50,0%	39,5%	7,9%	2,6%	0,0%	100,0%
Total	Recuento	34	30	45	50	58	217
	% dentro de Número de caso de clúster	15,7%	13,8%	20,7%	23,0%	26,7%	100,0%

En los resultados anteriores se muestra una asociación estadísticamente significativa entre las tipologías ciudadanas y la percepción de intensificación de la vigilancia en los últimos años ($\chi^2 = 122{,}688$; $p < 0{,}001$), evidenciando que la experiencia subjetiva de ser observado no es homogénea, sino que se distribuye de manera diferenciada entre los distintos grupos analizados.

Este grupo no presenta una postura clara frente a la confianza o la privacidad, lo que sugiere una forma de desconexión más que de ambivalencia, aquí no hay duda ni tensión, sino ausencia de problematización. Entonces, es una ciudadanía que no se posiciona, lo que puede implicar menor capacidad de agencia frente a sistemas de control. Esto no debe interpretarse únicamente como indiferencia, sino como una forma de desconexión estructural, donde la vigilancia no se percibe como un problema relevante.

Desde una lectura foucaultiana, esta ciudadanía podría interpretarse como aquella que se encuentra plenamente inmersa en los dispositivos de poder sin reconocerlos como tales. Como señala Michel Foucault, “el poder es más efectivo cuando no es percibido como poder”. Por su parte, Byung-Chul Han advierte que en la sociedad del rendimiento, los sujetos pueden participar activamente en sistemas de control sin percibirlos como tal ,lo que genera una forma de dominación silenciosa. En palabras del autor: “el sujeto de rendimiento se somete a sí mismo sin coacción externa” (Han, 2013, p. 12).

En conjunto, estas tipologías evidencian que la relación entre ciudadanía y vigilancia en Medellín no puede entenderse de manera homogénea. Por el contrario, se configura a través de múltiples formas de subjetivación que oscilan entre la legitimación, la crítica, la ambivalencia y la pasividad. Este hallazgo refuerza la idea de que el gobierno algorítmico no solo opera a nivel técnico, sino también en el plano de las percepciones, creencias y prácticas sociales.

10.3 Discusión teórica: tipologías y gobernabilidad algorítmica

Las tipologías identificadas permiten comprender la vigilancia digital como un fenómeno social complejo, en el que coexisten distintas formas de relación entre ciudadanía, tecnología y poder.

Desde el enfoque de la gubernamentalidad algorítmica, estas tipologías reflejan cómo los sistemas tecnológicos no producen efectos homogéneos, sino que son interpretados y apropiados de manera diferenciada por los sujetos.

Como señalan Christian Katzenbach y Lena Ulbricht, la gobernanza algorítmica implica nuevas formas de mediación entre Estado y ciudadanía, donde el control se ejerce a través de sistemas técnicos que no siempre son visibles o comprensibles. En este contexto, algunos ciudadanos legitiman, otros cuestionan, otros permanecen indecisos y otro no se involucran.

11 Aporte de la investigación

El principal aporte de esta tesis consiste en demostrar que la relación entre ciudadanía y vigilancia digital no puede ser comprendida únicamente desde la dicotomía aceptación y rechazo, sino que debe ser analizada como un campo complejo de tensiones donde convergen múltiples dimensiones: tecnologías, políticas y subjetivas.

Asimismo, la construcción de tipologías ciudadanías permite avanzar hacia una comprensión más profunda de cómo los individuos se posicionan frente a la vigilancia, aportando una mirada explicativa que complementa los enfoques descriptivos predominantes en este campo de estudio. Es así que, el análisis de dichas tipologías permite comprender que la vigilancia digital no es un fenómeno uniforme, sino un campo de tensiones donde se articulan distintas formas de relación con la tecnología , el Estado y los derechos. Casos internacionales como el escándalo de Cambridge Analytica (Pérez Lagos, 2019) y experiencias locales de comunicación transmedia (Ramírez López, 2019) refuerzan la idea de que Medellín requiere fortalecer la agencia ciudadana y la transparencia para evitar que el habitante sea un usuario pasivo y se convierta en un actor consciente de sus derechos digitales (Vázquez, 2025). Por otro lado, el análisis de clusters permite afirma que, la ciudadanía en Medellín no responde de manera homogénea a la vigilancia digital, sino que se configura en tipologías diferenciadas que combinan aceptación tecnológica, desconfianza institucional y preocupación por los derechos.

Este hallazgo constituye un aporte relevante, ya que permite superar visiones simplificadas de la relación entre tecnología y sociedad. Por lo que los resultados sugieren que la implementación de tecnologías de vigilancia debe considerar niveles diferenciados de confianza, percepciones de riesgo y demandas de participación. En ese sentido, la legitimidad de estos sistemas no depende únicamente de su eficacia técnica, sino de su capacidad para articularse con las expectativas y preocupaciones de la ciudadanía.

Es por eso que, a través del análisis empírico de la investigación, se evidencia que la gobernabilidad algorítmica no produce una ciudadanía homogénea, sino múltiples formas de posicionamiento frente al control tecnológico.

12 Conclusiones

Esta investigación tuvo como propósito analizar la relación entre ciudadanía, tecnologías de vigilancia y gobernabilidad algorítmica en Medellín, con el fin de comprender cómo los ciudadanos perciben, interpretan y responden al despliegue de sistemas de monitoreo basados en inteligencia artificial y reconocimiento facial.

A partir del análisis de los datos recolectado mediante encuesta y datos procesados en SPSS, se evidencia que la vigilancia digital no es un fenómeno percibido de manera homogénea, sino que configura un campo de tensiones donde convergen la aceptación tecnológica, la desconfianza institucional y la preocupación los derechos.

En primer lugar, los resultados muestran una alta aceptación de las tecnologías de vigilancia como herramientas para la seguridad, especialmente en lo relacionado con el uso de inteligencia artificial en el actuar policial. Este hallazgo se alinea con lo planteado por David Lyon, quien sostiene que "la vigilancia se ha convertido en una característica rutinaria de la vida cotidiana" (Lyon, 2018, p. 3). En este sentido, la tecnología es incorporada por amplios sectores de la ciudadanía como parte legítima del entorno urbano.

No obstante, esta aceptación coexiste con una profunda desconfianza institucional, evidenciada en la percepción de que la Alcaldía no utiliza adecuadamente la información recolectada ni comunica de manera clara el funcionamiento de los sistemas de vigilancia. Esta tensión revela una fractura entre el desarrollo tecnológico y su legitimación política, lo que sugiere que la eficacia técnica no garantiza la confianza ciudadana.

En segundo lugar, la investigación evidencia una alta valoración de la privacidad y los datos personales, acompañada de una significativa preocupación por los riesgos asociados al uso de la información. La percepción de que los ciudadanos pueden ser considerados sospechosos injustamente, así como la demanda de mayor veeduría sobre los datos, indica que la vigilancia no solo es interpretada como un mecanismo de seguridad, sino también como un potencial dispositivo de clasificación y control.

Este resultado puede comprenderse a la luz de Michel Foucault, quien afirma que "el examen combina las técnicas de la jerarquía que vigila y las de la sanción que normaliza" (Foucault, 1975, p. 184). En este sentido, los sistemas de vigilancia contemporáneos no solo observan, sino

que producen categorías de normalidad y desviación, generando efectos en la forma en que los individuos se perciben a sí mismo dentro del orden social.

En tercer lugar, el análisis de la agencia ciudadana revela que la vigilancia tiene efectos diferenciados sobre el comportamiento. Mientras una parte de la población no percibe cambios en su forma de actuar, otra reconoce que la presencia de tecnologías de monitoreo influye en sus prácticas cotidianas. Lo que sugiere que el control no opera de manera uniforme, sino que se modula según las percepciones y disposiciones individuales.

Desde la perspectiva de Byung-Chul Han, "el sujeto de rendimiento se somete a sí mismo sin coacción externa" (Han, 2013, p. 12), entonces, permite entender cómo los mecanismos de control pueden internalizarse sin necesidad de coerción explícita, esto quiere decir que la vigilancia digital puede producir formas de autocontrol que no siempre son plenamente reconocidas por los ciudadanos.

Uno de los aportes Más relevantes de la investigación se deriva del análisis de conglomerados, a partir del cual se identificaron cuatro tipologías ciudadanas frente a la vigilancia digital: ciudadanía legitimadora, crítica, ambivalente y pasiva. Estas tipologías evidencian que la relación entre ciudadanía y tecnología no es uniforme, sino que responde a configuraciones diferenciadas de sentido.

La existencia de estos perfiles confirma que la gobernabilidad algorítmica no produce una ciudadanía homogénea, sino múltiples formas de posicionamiento frente al control tecnológico. Como señalan Christian Katzenbach y Lena Ulbricht (2022), la gobernanza algorítmica implica nuevas formas de mediación entre Estado y sociedad, donde los sistemas tecnológicos reconfiguran las dinámicas de poder y participación.

Entonces, los hallazgos permiten afirmar que la vigilancia digital en Medellín se configura como un fenómeno ambivalente: es simultáneamente acepta como herramienta de seguridad, cuestionada en términos de confianza institucional y problematizada desde la perspectiva de los derechos. En síntesis, la vigilancia digital en Medellín no solo transforma la seguridad urbana, sino que redefine las relaciones entre ciudadanía, Estado y tecnología. En este proceso, los ciudadanos no se configuran únicamente como objetos de control, sino como actores que interpretan, negocian y, en algunos casos, cuestionan bajo las cuales se ejerce la vigilancia.

Este hallazgo invita a repensar la gobernabilidad algorítmica no como un sistema cerrado, sino como un campo abierto de disputa, donde el futuro de la relación entre tecnología y sociedad

dependerá de la capacidad de construir formas más trasparentes, participativas y orientadas a la protección de los derechos.

Finalmente, los hallazgos en Medellín confirman la denominada paradoja de la videovigilancia identificada por Vizcaíno Zamora (2021): el hecho de vivir en una de las sociedades más monitoreadas de la historia no se traduce automáticamente en una reducción de la incidencia delictiva ni en una mejora de la percepción de seguridad. Como señala el autor, esta saturación tecnológica a menudo produce una adicción a la seguridad que, lejos de tranquilizar, refuerza una cosmovisión basada en la ubicuidad del peligro y la sospecha constante.

13 Recomendaciones

A partir de los hallazgos de esta investigación, se proponen las siguientes líneas de análisis futuras:

En primer lugar, se sugiere desarrollar estudios que evalúen el impacto real de la videovigilancia, contrastando la instalación de tecnologías de monitoreo con la variación de las tasas de criminalidad y la percepción de inseguridad en Medellín, con el fin de profundizar en la relación entre seguridad objetiva y subjetiva.

En segundo lugar, resulta pertinente investigar la opacidad de los sistemas algorítmicos utilizados en la gestión de la seguridad, analizando sus criterios de funcionamiento, procesos de toma de decisiones y posibles sesgos asociados a variables socioeconómicas. Asimismo, se recomienda incorporar un enfoque interseccional que permita examinar cómo la vigilancia tecnológica afecta de manera diferenciada a distintos grupos sociales, especialmente poblaciones vulnerables.

Finalmente, en el ámbito normativo, se sugiere analizar la viabilidad de marcos regulatorios locales que orienten el uso de tecnologías de vigilancia, garantizando derechos como la autodeterminación informativa.

Referencias

Alcaldía de Medellín. (s. f.). *Transición a Distrito Especial de Ciencia, Tecnología e Innovación*. https://www.medellin.gov.co/es/departamento-administrativo-de-planeacion/transicion-a-distrito-especial-de-ciencia-tecnologia-e-innovacion/

Arce Jiménez, C. (2022). *Desafíos para la ciudadanía y el sistema de derechos fundamentales en la era digital. Derechos y Libertades*, (46), 241-272. https://doi.org/10.20318/dyl.2022.6520

Arteaga Botello, N. (2010). *Videovigilancia del espacio urbano: tránsito, seguridad y control social. Andamios*, *7*(14), 263-286.

Badillo Mendoza, M. E., & Marta-Lazo, C. (2019). Medios digitales y ciberciudadanía ambiental: análisis del Blog "noalacolosahorrorosa". En M. E. Badillo Mendoza, C. Pérez Lagos, N. J. Medranda Morales, & M. I. Cortés Cortés (Eds.), *Ciudadanías digitales: Perspectivas desde los medios, el periodismo y la educomunicación* (pp. 55-82). Editorial Politécnico Grancolombiano.

Bañuelos, J. (2003). *Videovigilancia en la sociedad panóptica contemporánea. Razón y Palabra*, (31).

Barcelona Llop, J. (2012). *Videovigilancia, seguridad ciudadana y derechos fundamentales* [Recensión del libro de Xabier Arzoz Santisteban]. *Revista de Administración Pública*, (189), 497-521.

Bonilla Gutiérrez, J. C. (2024). *IA y privacidad: Protegiendo la autodeterminación informativa en la era digital. Revista de la Facultad de Derecho de México*, *74*(290). https://doi.org/10.22201/fder.24488933e.2024.290.89719

Caracol Radio. (2022, 4 de julio). *Alcaldía no ha definido qué pasará con datos de Medellín Me Cuida*. https://caracol.com.co/emisora/2022/07/04/medellin/1656952747_024498.html

Castro Orellana, R. (2009). *La ciudad apestada: Neoliberalismo y postpanóptico. Revista de Ciencia Política*, *29*(1), 165-183. https://doi.org/10.4067/S0718-090X2009000100009

Cazau, P. (2006). *Introducción a la investigación en ciencias sociales*. (3.ª ed.). Buenos Aires. 26

De la Garza Montemayor, D. J., La Rosa, A., Barredo Ibáñez, D., & Freundt-Thurne, Ú. (2019). *Medios sociales, capital social y sentimiento de eficacia política: Un estudio comparativo entre las juventudes de México y Perú.* En M. E. Badillo Mendoza, C. Pérez Lagos, N. J. Medranda Morales, & M. I. Cortés Cortés (Eds.), *Ciudadanías digitales: Perspectivas desde los medios, el periodismo y la educomunicación* (pp. 133-154). Editorial Politécnico Grancolombiano.

De la Serna Bilbao, M. N. (2016). *Seguridad ciudadana y los sistemas de videovigilancia: Límites, garantías y regulación. Vniversitas*, (132), 129-163. http://dx.doi.org/10.15332/s1900-0448.2016.0045.06

Deleuze, G. (1990). *Conversaciones, 1972-1990*. Pre-Textos. 4-5.

Departamento Administrativo Nacional de Estadística. (2025). *Proyecciones de población por sexo y grupos de edad, Medellín*, 2018–2035 [Base de datos]. https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/proyecciones-de-poblacion

Domínguez González, D. J., & Domínguez Sánchez-Pinilla, M. (2023). *Panoptismo digital y gubernamentalidad algorítmica. Una mirada desde la teoría social*. *Las Torres de Lucca: Revista Internacional de Filosofía Política, 12*(2), 261–277. https://doi.org/10.5209/ltdl.83864

El Colombiano. (2023, 3 de marzo). *Secretario de Seguridad habló sobre polémico contrato del sistema de reconocimiento facial*. https://www.elcolombiano.com/medellin/alcaldia-medellin-responde-sobre-polemico-contrato-de-reconocimiento-facial-FA20649491

e-Residency of Estonia. (s. f.). *e-Residency of Estonia*. https://www.e-resident.gov.ee/

Feldstein, S., Ferreyra, E., & Krivokapić, D. (2022). *La lucha global ante la vigilancia con IA: Nuevas tendencias y respuestas democráticas* (B. Kerley, Ed.). National Endowment for Democracy.

Feenberg, A. (1999). *Questioning technology*. Routledge.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4.ª ed.). SAGE Publications. 171-172

Foucault, M. (1975). *Vigilar y castigar: Nacimiento de la prisión*. Siglo XXI Editores. 194.

Fundación Karisma. (2020). *¿Qué dice que hace y qué es lo que realmente hace Medellín Me Cuida? Karisma.org.co.* https://karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-medellin-me-cuida/

Galdon-Clavell, G. (2015). *Si la videovigilancia es la respuesta, ¿cuál era la pregunta? Cámaras, seguridad y políticas urbanas. EURE (Santiago)*, *41*(123), 81-101.

García Martín, L. (2017). *Vigilar y corregir: el Trabajo Social en las obras de Michel Foucault y Jacques Donzelot. Cuadernos de Trabajo Social*, *30*(2), 357-367. http://dx.doi.org/10.5209/CUTS.54585

Gil Márquez, T. (2004). *El sistema de seguridad pública en la Constitución española de 1978* [Tesis doctoral, Universitat Abat Oliba CEU].

Goldmann, L. (1971). *Sociología de la creación literaria* (H. Acevedo, Trad.). Ediciones Nueva Visión. (Obra original publicada en 1967).

Haggerty, K., & Ericson, R. (2000). *The surveillant assemblage. The British Journal of Sociology, 51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Han, B.-C. (2013). *La sociedad de la transparencia* (R. Gabás Pallas, Trad.). Herder, 12-64.

Hernández-Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Ibarreche, X., Martínez Elebi, C., & Di Lorenzo, C. (2025). *Reconocimiento facial y tecnologías de vigilancia en América Latina: Casos, proveedores y dinámicas comerciales*. Al Sur. https://www.alsur.lat/sites/default/files/2025-07/Reporte%20reconocimiento%20facial.pdf

Isin, E. F. (2009). *Citizenship in flux: The figure of the activist citizen. Subjectivity, 29*(1), 367-388. https://doi.org/10.1057/sub.2009.25

Jasso López, L. C. (2018). *Hacia la transterritorialización de la política pública de videovigilancia en México. Anuario de Espacios Urbanos, Historia, Cultura y Diseño*, (25), 199-222. https://doi.org/10.24275/BAER1762

Juri, Y. E. (2023). *La gobernanza de los datos de la soberanía territorial a la soberanía digital. Revista Quaestio Iuris*, *16*(2), 802-820.

Katzenbach, C., & Ulbricht, L. (2022). *Gobernanza algorítmica.* Revista Latinoamericana de Economía y Sociedad Digital, (Especial 1). https://doi.org/10.53857/CWYI6959

Lema-Taday, N. V., & Alvaracín-Jarrín, A. A. (2022). *Big Data: Automatización, vigilancia y control. Una crítica desde los derechos humanos.* Revista Arbitrada Interdisciplinaria Koinonía, *7*(2), 450-474. http://dx.doi.org/10.35381/racji.v7i2.2012

Lío, V. (2020). La efectividad puesta a prueba: *Funciones y limitaciones de la videovigilancia del espacio público. Ciencia, Docencia y Tecnología*, *31*(60), 71-105. https://doi.org/10.33255/3160/632

Londoño Osorio, I. S., & Guerrero-C, J. (2024). *El teatro de la vigilancia: Las cámaras de vigilancia en Medellín. Sociología y Tecnociencia*, *14*(1), 66-87. https://doi.org/10.24197/st.1.2024.66-87

Lozano Jiménez, J. L. (2013). *La influencia del panóptico de Jeremy Bentham en el proyecto Tracking Transience de Hasan Elahi. AUSART Journal for Research in Art*, *1*(1), 201-212.

Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press, 14. https://doi.org/10.4000/communication.11962

Malamud Herrera, S. (2018). *Videovigilancia y privacidad: Consideraciones en torno a los casos "Globos" y "Drones".* Revista Chilena de Derecho y Tecnología, 7(2), 137-162. https://doi.org/10.5354/0719-2584.2018.49097

Noain Sánchez, A. (2016). Byung-Chul Han, *La sociedad de la transparencia [Reseña del libro]. CIC. Cuadernos de Información y Comunicación*, (21), 265-266. http://dx.doi.org/10.5209/CIYC.52976

Noelle-Neumann, E. (1993). *La espiral del silencio. La opinión pública y los efectos de los medios de comunicación. Communication & Society*, *6*(1-2), 9-28. https://doi.org/10.15581/003.6.35558.

Osaba, J. (2015). *La distopía ya está aquí: Vigilancia estatal, de Orwell a Snowden y El Guardián. Dixit*, (23), 4-15.

Pain, R. (2000). *Place, social relations and the fear of crime: A review. Progress in Human Geography*, *24*(3), 365-387.

Palmer, D., & Warren, I. (2012). *Tecnología de vigilancia y controles territoriales: Gobernanza y el pulso de la privacidad. Novática*, (217), 15-20.

Parrilli, F. A. (2013). *Ingeniería y sociedad de control: sobre diseño y videovigilancia pública. Tecnología & Sociedad*, *1*(2), 11-37.

Pérez Esquivel, A. (2021). *Desafíos de la videovigilancia automatizada. Anales de la Facultad de Ciencias Jurídicas y Sociales de la UNLP*, (24), 100-122.

Pérez Lagos, C. (2019). *El caso Cambridge Analytica en el periódico francés "Le Figaro": enfoque pragmatista y discursivo del estudio de los acontecimientos.* En M. E. Badillo Mendoza, C. Pérez Lagos, N. J. Medranda Morales, & M. I. Cortés Cortés (Eds.), *Ciudadanías digitales: Perspectivas desde los medios, el periodismo y la educomunicación* (pp. 37-54). Editorial Politécnico Grancolombiano.

Pew Research Center. (2019). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf

Ragnedda, M. (2011). *Internet y control social: entre rizoma y Gran Hermano. Perspectivas de la Comunicación*, *4*(1), 42-52.

Ramírez López, S. (2019). *Comunicación transmedia y ciudad: El caso de La Candelaria de Bogotá, Colombia.* En M. E. Badillo Mendoza, C. Pérez Lagos, N. J. Medranda Morales, & M. I. Cortés Cortés (Eds.), *Ciudadanías digitales: Perspectivas desde los medios, el periodismo y la educomunicación* (pp. 95-114). Editorial Politécnico Grancolombiano.

Rouvroy, A., & Berns, T. (2013). *Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation?* Réseaux, 177(1), 163–196. https://doi.org/10.3917/res.177.0163

Sabater, C. (2008). *Vidas de cristal: análisis del derecho a la intimidad en la sociedad de la información. Intersticios: Revista Sociológica de Pensamiento Crítico*, *2*(1), 43-55.

Selwyn, N. (2004). *Reconsidering political and popular understandings of the digital divide. New Media & Society*, *6*(3), 341-362. https://doi.org/10.1177/1461444804042519

Silva Arriola, L. (2009). *Seguridad, territorio, población*. *Revista INVI, 24*(66), 193–196. https://www.revistas.uchile.cl/index.php/INVI/article/view/62194

Ull Salcedo, M. V. (2005). *El derecho a la intimidad como límite de la videovigilancia. Revista de Derecho Político*, (63), 191-201.

Vázquez, M. (2025). *No digan cómo vivo, díganme cómo vivir: El movimiento Do It Yourself y el capitalismo de vigilancia. InMediaciones de la Comunicación*, *20*(1), 205-231. https://doi.org/10.18861/ic.2025.20.1.3992

Venturini, J., & Garay, V. (2021). *Reconocimiento facial en América Latina: Tendencias en la implementación de una tecnología perversa*. Consorcio Al Sur.

https://estudio.reconocimientofacial.info/reports/ALSUR-Reconocimiento_facial_en_Latam-ES.pdf

Vizcaíno Zamora, Á. (2021). *Videovigilancia e inteligencia artificial: entre la utopía y la distopía. Revista Mexicana de Ciencias Penales*, (14), 8-38.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Anexos

Anexo 1. Instrumento de investigación – Encuesta estructurada

El levantamiento de información de la presente investigación se llevará a cabo a través de una encuesta estructurada, que, si bien mide percepciones de momentos concretos, porque está influida por el contexto social presente (por ejemplo, estar en época electoral o por un pico de inseguridad de algún tipo en un lugar específico) y por la forma en la que están formuladas preguntas. No devuelve la verdad objetiva sino indicios, pulsos sociales que requieren triangulación y controles para interpretarse correctamente.

Debido a lo anterior se plantea como estrategia para minimizar problemas de análisis y obtener del mismo resultados robustos, tener en cuenta la contextualización de la encuesta, es decir, se registrará la fecha exacta, se tomará en cuenta los eventos relevantes y con relación al contexto se incluirá preguntas sobre exposición reciente a noticias. Para evitar el establecimiento de sesgos, se usará preguntas tipo *vignettes* para plantear escenarios que permitan explorar percepciones y/o creencias.

Se plantea un pilotaje de la encuesta con una muestra de 20 a 30 para detectar si hay sesgos o ambigüedades relacionadas con la redacción, además de controlar el contexto a través de la inclusión de variables que permitan medir el clima político, la exposición a noticias y datos de caracterización como la comuna, el estrato socioeconómico, entre otros.

Durante la elaboración del informe se contrastará y documentará cuándo se realizó la encuesta, que pasaba en la ciudad durante ese mismo periodo de tiempo y que limitaciones se presentaron que infieren en los resultados.

Tipos de preguntas

Esta exploración considera los siguientes tipos de preguntas:

- Preguntas de caracterización
- Uso de escalas tipo Likert (1 al 5)
- Preguntas para conocimiento/experiencia (Si/No/No sabe)
- Vignettes para medir aceptación ante escenarios concretos

Bloques de la encuesta

1. Consentimiento informado y protección de datos

a. **Protección de datos:** El componente ético de esta investigación se fija a partir de los derechos fundamentales de protección de datos personales o habeas data, bajo los criterios establecidos en la Ley Estatutaria de 1581 del octubre 17 de 2012 de Colombia. En concordancia con esto y, con la técnica y el instrumento de medición, se presentará el siguiente consentimiento informado al inicio del cuestionario digital:

b. **Consentimiento informado:**

El presente estudio es realizado por un estudiante del programa de Sociología de la Universidad de Antioquia como parte de los requisitos para optar al título de Sociólogo. La investigación, titulada "La vigilancia digital en Medellín: percepción ciudadana frente al uso de dispositivos y tecnología en el espacio urbano", tiene como objetivo conocer cómo perciben los habitantes de Medellín el uso de tecnologías de vigilancia en la ciudad y qué implicaciones consideran que esto tiene para sus derechos y su vida cotidiana.

Su participación en esta encuesta es completamente voluntaria. La información que usted proporcione será recolectada de manera anónima: no se solicitará ni registrará ningún dato personal que permita identificarle.

Los datos serán utilizados exclusivamente con fines académicos para el análisis de este proyecto de investigación. Usted puede retirarse o dejar de responder en cualquier momento, sin ninguna consecuencia.

Al continuar y responder este cuestionario, usted manifiesta haber leído esta información y estar de acuerdo en participar de manera voluntaria.

2. Caracterización (captura de datos sociodemográficos y territoriales.
    a. Edad
    b. Género
    c. Educación
    d. Comuna
    e. …
3. Experiencia directa con inseguridad: permite comprender si es ciudadano encuestado a sido víctima o testigo de alguna situación de inseguridad en los últimos (x) meses.
4. Conocimiento y exposición: permite conocer si el ciudadano reconoce en el entorno dispositivos de videovigilancia o si ha recibido comunicaciones por parte de la institucionalidad respecto a vigilancia y seguridad.

5. Percepción de seguridad/privacidad medida a través de preguntas tipo Likert con escala de 1 a 5 para identifica como se siente el ciudadano.
6. Confianza institucional: permite conocer cual es la percepción de confianza con instituciones como la policía, la alcaldía, empresas tecnológicas que operan en la ciudad, etc)
7. Gobernabilidad algorítmica / transparencia: para identificar el conocimiento ciudadano sobre el uso de algoritmos en el ejercicio de vigilancia y si se debería explicar el funcionamiento de los mismos.
8. Actos de ciudadanía: permite saber si el ciudadano estaría dispuesto a participar en procesos de veeduría o si presentaría una queja.
9. Vignettes: para conocer las percepciones del ciudadano frente al planteamiento de una situación o acción especifica, pone en situación al ciudadano para dar una respuesta cerrada.
10. Medios y clima con respecto a la exposición a noticias, clima electoral, percepción política de polarización).
11. Preguntas abiertas: Para tener una mirada cualitativa.

Cuestionario:

Estudio: Percepciones ciudadanas sobre la vigilancia digital en Medellín

Aplicación: Habitantes del Valle de Aburrá y ciudadanos que transitan Medellín

Tipo de instrumento: Encuesta estructurada.

Consentimiento informado:

El presente estudio es realizado por un estudiante del programa de Sociología de la Universidad de Antioquia como parte de los requisitos para optar al título de Sociólogo. La investigación, titulada "La vigilancia digital en Medellín: percepción ciudadana frente al uso de dispositivos y tecnología en el espacio urbano", tiene como objetivo conocer cómo perciben los habitantes de Medellín el uso de tecnologías de vigilancia en la ciudad y qué implicaciones consideran que esto tiene para sus derechos y su vida cotidiana.

Su participación en esta encuesta es completamente voluntaria. La información que usted proporcione será recolectada de manera anónima: no se solicitará ni registrará ningún dato personal que permita identificarle.

Los datos serán utilizados exclusivamente con fines académicos para el análisis de este proyecto de investigación. Usted puede retirarse o dejar de responder en cualquier momento, sin ninguna consecuencia.

Al continuar y responder este cuestionario, usted manifiesta haber leído esta información y estar de acuerdo en participar de manera voluntaria.

Bloque Filtro

1. **¿Vive o transita regularmente por Medellín (mínimo 3 veces por semana)?**
   - Sí
   - No → *Fin de la encuesta*

Bloque de preguntas sociodemográficas/caracterización

2. Edad:
   - Entre 12-18 años
   - Entre 19-30 años
   - Entre 31-59 años
   - 60 años en adelante
3. Género:
   - Mujer
   - Hombre
   - No binario
   - Prefiere no responder
4. Nivel educativo alcanzado:
   - Primaria
   - Secundaria
   - Técnico/Tecnológico
   - Pregrado
   - Posgrado
5. Ocupación principal:
   - Estudiante
   - Empleado/a
   - Independiente
   - Desempleado/a
   - Hogar
   - Otro: _____

6. Estrato socioeconómico: (desplegable)
    - 1
    - 2
    - 3
    - 4
    - 5
    - 6
7. ¿Con qué frecuencia visita/transita por zonas donde hay cámaras de vigilancia (calles, estaciones, parques)?
    - A diario
    - Varias veces a la semana
    - Ocasionalmente
    - Casi nunca
    - No sabe

Bloque de preguntas conocimiento y cercanía con tecnologías de vigilancia

8. ¿Cómo valora que el gobierno tenga acceso a datos personales (incluidos datos sensibles)?
    - Muy riesgoso
    - Riesgoso
    - Neutral
    - Aceptable
    - Necesario
9. ¿Qué tanto percibe que usted aparece en cámaras de vigilancia en Medellín?

Escala Likert 1–5: Nada – Mucho.

10. ¿Reconoce alguno de estos dispositivos en Medellín? (Seleccione los que conozca)
    - Cámaras LPR (reconocimiento de placas)
    - Cámaras de reconocimiento facial
    - Cámaras “Salva Vidas” (fotodetección)
    - Cámaras PTZ
    - Software de monitoreo predictivo
    - Ninguno
11. ¿Se siente más vigilado en los últimos años debido al aumento de cámaras y tecnologías de monitoreo?

Escala Likert 1–5: Nada – Mucho.

12. ¿Qué tanta información personal comparte usted voluntariamente en plataformas digitales (redes sociales, aplicaciones comerciales, servicios públicos o privados)?
    Escala Likert 1–5.

Bloque de preguntas confianza institucional

Escala Likert 1 a 5 (1 = muy en desacuerdo, 5 = muy de acuerdo)

13. Considero que las cámaras ayudan a mejorar la seguridad en Medellín.
14. El uso de tecnologías como inteligencia artificial y reconocimiento facial mejora el actuar de la Policía Nacional.
15. Creo que la seguridad en Medellín es cada vez más automática y depende menos de personas y más de computadores.
16. La Alcaldía explica claramente cómo funcionan los dispositivos de vigilancia que utiliza.
17. Confío en que la Alcaldía use bien la información que recolecta y que esto no me pone en riesgo.
18. Creo que la videovigilancia se usa para fines distintos a los declarados oficialmente.

Bloque de preguntas Gobernabilidad algorítmica (decisiones basadas en datos)

Escala Likert 1 a 5 (1 = muy en desacuerdo, 5 = muy de acuerdo)

19. Creo que las decisiones de seguridad en Medellín dependen cada vez más de sistemas automatizados o algoritmos.
20. Me preocupa que estas tecnologías puedan cometer errores o generar falsas alarmas.
21. Entiendo bien cómo funcionan los sistemas de reconocimiento facial.
22. Creo que debería existir mayor control ciudadano sobre estas tecnologías.
23. Me preocupa que, por la información que recoge la Alcaldía, pueda ser considerado sospechoso de algo sin razón.
24. Considero que es necesario regular estrictamente el uso de sistemas de vigilancia digital.

Bloque de preguntas Ciudadanía, privacidad y derechos

Escala Likert 1 a 5 (1 = muy en desacuerdo, 5 = muy de acuerdo)

25. La presencia de cámaras afecta mi privacidad.
26. Las tecnologías de vigilancia influyen o limitan mi forma de actuar en los espacios donde transito.
27. Me siento observado/a en zonas donde hay muchas cámaras.
28. Creo que la videovigilancia podría usarse para fines distintos a los declarados oficialmente.
29. Creo que debería existir mayor veeduría ciudadana sobre los datos que la Alcaldía recopila sobre mí.
30. Es importante para mí que mis datos personales estén protegidos.

Bloque de preguntas Agenda pública y clima de opinión

Medición del clima político

31. He visto debates o polémicas recientes en redes sociales sobre vigilancia digital en Medellín.

    - Sí
    - No

32. ¿Con qué frecuencia habla usted con otras personas sobre temas de seguridad o vigilancia?

- Frecuentemente
- A veces
- Rara vez
- Nunca

33. ¿Diría abiertamente su opinión sobre la vigilancia digital en público o redes sociales?
    - Sí
    - Tal vez
    - No, evitaría hacerlo
34. En su opinión, ¿la mayoría de la gente en Medellín apoya estas tecnologías?
    - Sí
    - No
    - No sabe
35. ¿Cree que expresar preocupación sobre la vigilancia podría generar críticas o burlas?
    - Sí
    - No
    - No sabe
36. ¿Estaría dispuesto(a) a participar en una entrevista o grupo focal para profundizar en este tema?
    - Sí
    - No
37. Si su respuesta fue "Sí", por favor deje un medio de contacto (correo o número).
    Nota: este ítem debe ir separado del consentimiento anónimo y advertir explícitamente que este dato será almacenado solo para contacto y no se usará en el análisis.

Bloque de agradecimiento

Gracias por participar. Sus respuestas contribuirán al análisis sociológico de la vigilancia digital en Medellín y a la comprensión de sus impactos en la ciudadanía.