Cámaras Discretas

Análisis del fallido sistema de videovigilancia inteligente para Transmilenio

Pilar Sáenz y Ann Spanger

Fundación Karisma

PRIVACY INTERNATIONAL

Esta publicación fue realizada por la Fundación Karisma con el apoyo y financiación de Privacy International.

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: http://www.documentoaccesible.com/#que-es.

Autoras
Pilar Sáenz
Ann Spanger

Revisión
Carolina Botero
Juan Diego Castañeda
Amalia Toledo
Francisco Vera - Privacy International

Coordinación editorial
Laura Rojas Aponte
Camila Barajas Salej

Diseño gráfico y diagramación
Sergio García Casas

Imagen de portada
Spy Camera Security Video Surveillance Pigeon por Nikon D60 con licencia CC0 Dominio Público

Imagen de contraportada
Cámara Cámaras El Tráfico Ver Vigilancia Gobierno por Public-DomainPictures con licencia CC0 Dominio Público

Imagen a la derecha
Eye and finger por Leszek Leszczynski con licencia CC BY 2.0

Bogotá, Colombia
2018

contenido

resumen

Fundación Karisma hace un análisis de la fallida implementación del sistema de videovigilancia inteligente (biométrico) en Transmilenio y alerta sobre nuevas implementaciones de sistemas que utilizan cámaras de identificación biométrica en espacios públicos; a la vez, pone de manifiesto posibles afectaciones a los derechos humanos asociados con este tipo de sistemas y plantea dudas sobre su necesidad y el gasto público asociado con estos sistemas. Encontramos que a la hora de diseñar las políticas públicas para implementaciones de este tipo, se está ignorando el análisis del impacto o afectación de derechos humanos.

palabras clave

Sistemas de videovigilancia; tecnologías biométricas; reconocimiento facial; intimidad; privacidad; libertad de expresión; solucionismo tecnológico; vigilancia masiva.

introducción

La primera pregunta que surge al mirar el fallido sistema de videovigilancia inteligente (biométrico) en Transmilenio es: ¿por qué es necesario hablar de un caso que, finalmente, no sucedió? Es cierto que el sistema de cámaras que el Distrito pretendió poner en marcha en el sistema de transporte masivo de Bogotá, Transmilenio, no pasó de ser un tenebroso prospecto de cómo la institucionalidad en Colombia está proyectando un eventual uso de herramientas tecnológicas para la vigilancia masiva. Aunque se avanzó hasta la instalación y realización de pruebas de la totalidad del sistema, invirtiendo un presupuesto nada despreciable, este sistema de cámaras de vigilancia, hasta donde sabemos, no entró en operación por las trabas derivadas de la creación, gestión y manejo de una base de datos con la que se haría el cotejo de la información recolectada por las cámaras ubicadas en las estaciones de Transmilenio. Sin embargo, aun cuando el sistema nunca haya entrado en funcionamiento, sí se trata de un proyecto paradigmático de cómo se concibe la utiliza-

ción de tecnologías de vigilancia y sistemas de identificación biométrica, donde las consideraciones principales son técnicas y no se realizan estudios de impacto, necesidad y proporcionalidad o posibles afectaciones al ejercicio de derechos humanos. La realidad es que hay planes de implementar nuevos sistemas de vigilancia con las características del que se había pensado para Transmilenio y por eso también es fundamental analizarlo.

El diseño de políticas públicas, cuando se implementan sistemas de videovigilancia de semejantes dimensiones y características, no puede pasar por alto las graves afectaciones que podrían tener para los derechos de las personas.

Entre defensores de derechos humanos y algunos sectores de la ciudadanía resulta, además, un motivo de preocupación y alerta que, para el diseño y puesta en marcha de este tipo de sistemas, no se tomen en cuenta las perspectivas de quienes podrían resultar afectados ni los argumentos de los sectores que tienen una mirada crítica. El diseño de políticas públicas, cuando se implementan sistemas de videovigilancia de semejantes dimensiones y características, no puede pasar por alto las graves afectaciones que podrían tener para los derechos de las personas.

Así, este documento tiene varios propósitos: por un lado, dar una perspectiva sobre el uso del reconocimiento facial en sistemas de videovigilancia (y, de paso, mostrar los puntos críticos de la utilización de cámaras de vigilancia en general); y, por otro, mostrar los fallos que se evidencian en el diseño e implementación de este tipo de proyectos, concretamente en el sistema de transporte masivo de Bogotá.

El análisis que se presenta se basa en la información pública disponible tanto en las páginas web de las instituciones involucradas en la implementación de este proyecto (Fondo de Vigilancia y Seguridad, la Secretaría Distrital de Seguridad, Convivencia y Justicia, EMTEL), como en los medios de comunicación y otras entidades.

Si bien el Estado tiene la facultad de usar la vigilancia para evitar crímenes y proteger la seguridad nacional, sigue siendo una facultad excepcional por su posible afectación a los derechos humanos. Uno de los mecanismos que busca evitar los abusos de esta facultad es el fomento de la transparencia que obliga a las autoridades a informar sobre los objetivos, características y mecanismos de protección que garanticen el respeto a los derechos humanos. Por tanto, creemos que este tipo de investigaciones también contribuyen a la búsqueda de transparencia en las decisiones asociadas a políticas públicas.

El ejercicio de investigación que se materializa en este documento busca también establecer qué tanto puede una persona interesada saber sobre el diseño del sistema de videovigilancia de Transmilenio y su atención a los derechos humanos indagando en la información pública.

la vida en el nuevo panóptico

En suma, este es el relato de un costosísimo proyecto que nunca vio la luz y lo que deberíamos aprender de él.

Las cámaras de seguridad son una constante de nuestra vida moderna. Están por todas partes, registran nuestros tránsitos cotidianos de la casa al trabajo, al colegio o a la universidad y de vuelta a casa. Parece que las pedimos a gritos para espacios como estadios, aeropuertos, centros comerciales, festivales callejeros e incluso las pagamos y las instalamos en conjuntos residenciales y oficinas. Instalar cámaras para tener más seguridad es una promesa electoral que no distingue color o ideología. Más allá de su efectividad, las cámaras de seguridad aparentan ser un sistema de disuasión efectivo que desplaza el comportamiento sancionable del espacio vigilado hacia donde no se está haciendo el registro. Varios estudios han demostrado que, en muchos casos, las cámaras de vigilancia se encuentran en espacios privilegiados y que, en vez de reducir el crimen, lo desplazan[1] .

1 Véase: King, J. Mulligan, K. Raphael, S. 2008,

Del mismo modo, el gasto público en sistemas de videovigilancia en Colombia se ha incrementado en los últimos años. Solamente en Bogotá, en el 2017, se invirtieron 75 mil millones de pesos (25 millones de dólares) en cámaras[2]; en Medellín la cifra alcanza los 100 mil millones de pesos (35 millones de dólares).[3] En otras ciudades como Cali, Cúcuta, Riohacha, Valledupar, Pasto, Armenia, Barranquilla, Cartagena, Manizales y Quibdó, durante los años 2016 y 2017, también se han hecho inversiones millonarias en asocio con el Ministerio de Interior en el marco del programa Vive Seguro, Vive en Paz.[4]

Los programas del gobierno concuerdan con una narrativa difundida por varios medios de comunicación, que han extendido la idea de que las cámaras son una parte fundamental en la solución a los problemas de seguridad o que, incluso, son la solución ejemplar. El hecho de que los noticieros muestren con frecuencia lo que las cámaras registran y lo instrumentalicen como evidencias incuestionables para algunos crímenes, ayuda a alimentar el imaginario popular de la eficiencia e incluso de la infalibilidad de los sistemas de videovigilancia.

La inversión pública y el auge de la videovigilancia como mecanismo idóneo de seguridad, se sostiene en varias ideas acerca de su efectividad: las cámaras podrían identificar delincuentes potenciales, alertar a la policía de forma temprana, generar pruebas para la identificación de agresores o aumentar la percepción de seguridad[5]. Sin embargo, aunque es cierto que el uso de cámaras podría reducir las tasas de criminalidad en determinados lugares, su alcance no es tan amplio como se nos hace creer. Además, existe evidencia de que un uso irresponsable y la falta de regulación específica pueden dar lugar a abusos por parte de las autoridades.[6]

diciembre. *CITRIS Report: San Francisco Community Safety Camera Program.* Disponible en: https://www.wired.com/images_blogs/threatlevel/files/sfsurveillancestudy.pdf; y Kille, L. Maximino, M. 2014, febrero. *The effect of CCTV on public safety: Research roundup.* Disponible en: https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime

2 Véase: Minuto 30. 2017, Septiembre. *Una inversión superior a los 75 mil millones de pesos en el sistema de video vigilancia para la ciudad*. Disponible en: https://www.minuto30.com/secretaria-de-seguridad-de-bogota-presento-su-rendicion-de-cuentas-tras-primer-ano/487975/; y Caracol Radio. 2017, Enero. *Alcaldía de Bogotá invertirá 88 mil millones en cámaras de seguridad*. Disponible en: http://caracol.com.co/emisora/2017/01/02/bogota/1483388790_835022.html.

3 Periódico *El Tiempo*. 2017, Octubre. *Habrá una inversión de 100.000 millones para adquirir cámaras de seguridad para la ciudad*. Disponible en: http://www.eltiempo.com/colombia/medellin/medellin-aumenta-en-22-su-presupuesto-para-el-2018-139658.

4 Ministerio del Interior. 2017, Enero. *La estrategia ´Vive Seguro, Vive en Paz´ del Ministerio del Interior sigue cumpliendo, cuatro ciudades inician el 2017 con cobertura plena de cámaras de seguridad*. Disponible en: http://www.mininterior.gov.co/sala-de-prensa/noticias/la-estrategia-vive-seguro-vive-en-paz-del-ministerio-del-interior-sigue-cumpliendo-cuatro-ciudades-inician-el-2017-con-cobertura-plena-de-camaras-de-seguridad

5 Véase: La Vigne, Nancy G. 2013, Abril. *How surveillance cameras can help, prevent and solve crime.* Urban Institute. Disponible en: https://www.urban.org/urban-wire/how-surveillance-cameras-can-help-prevent-and-solve-crime; y Concejo de Bogotá, Distrito Capital. 2014. *Exposición de motivos del Proyecto de Acuerdo 198*. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=58799.

6 Kille, L. Maximino, M. 2014, Febrero. *The effect*

Un mundo con cámaras, registros y las respectivas bases de datos en las que se recopila una ingente cantidad de información de las personas, en realidad, es un escenario que genera muchos y crecientes problemas para la privacidad y, por tanto, se erige como una amenaza para nuestras libertades. En algunos Estados, bajo la figura de preservar la "seguridad pública", se ha llegado a monitorear y a prohibir protestas y manifestaciones públicas. Existen reportes de cómo imágenes registradas durante protestas han servido para identificar y perseguir a manifestantes con las consecuentes dudas sobre la legitimidad de tales procedimientos y las preocupaciones sobre la facilidad con que este tipo de sistemas se prestan para abusos.[7] Sirven, también, para discriminar y reforzar estigmas y prejuicios raciales, sociales, culturales y de género, especialmente cuando van en conjunto con tecnologías de seguimiento, rastreo, reconocimiento facial o corporal, o incluso sistemas de toma de decisión automatizados. No se trata de decir que las cámaras no deberían existir, sino de no tomar a la ligera las políticas públicas que las involucran.[8]

No se trata de decir que las cámaras no deberían existir, sino de no tomar a la ligera las políticas públicas que las involucran.

En Colombia, los diferentes escándalos en los que se han visto involucradas diferentes agencias de inteligencia que han abusado de los sistemas de vigilancia de las telecomunicaciones, demuestran las graves consecuencias que el abuso de sistemas de vigilancia masiva y selectiva (incluidos sistemas de videovigilancia), pueden tener para los derechos humanos si no hay veeduría, control y una legislación enfocada en la priorización de los derechos humanos a la intimidad, a la libertad de expresión y a la no discriminación y estigmatización.[9]

of CCTV on public safety: Research roundup. Disponible en: https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime

7 Algunos de los casos conocidos han sido la utilización de cámaras de videovigilancia en Brasil durante los Juegos Olímpicos. Kayyali, Dia. VICE (Motherboard). 2016, Junio. Disponible en: https://motherboard.vice.com/en_us/article/wnxgpw/the-olympics-are-turning-rio-into-a-military-state.
También en la identificación de manifestantes que protestaban tras la elección de Donald Trump en Jacksonville, Estados Unidos. Conarck, Ben. *Monitoring Dissent: How the Jacksonville Sheriff's Office spied on protesters.* 2017, Marzo. Disponible en: http://jacksonville.com/news/florida/public-safety/2017-03-17/monitoring-dissent-how-jacksonville-sheriff-s-office-spied. Y en la utilización de un software privado ligado al uso de redes sociales para la identificación de personas que participaron en protestas anti corrupción en Rusia. Meduza, 2017, Julio. *We'll find you, too' An anonymous website is identifying Russians who attended Alexey Navalny's June 12 anti-corruption protest.* Disponible en: https://meduza.io/en/feature/2017/07/09/we-ll-find-you-too

8 Véase: ACLU. Sin fecha. *What's wrong with public video surveillance.* Disponible en: https://www.aclu.org/other/whats-wrong-public-video-surveillance; Norris, Clive. *From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social contro*l en: Lyon. D (Ed.). *Surveillance as Social Sorting Privacy, risk, and digital discrimination*. 2003. New York, US: Routledge.

9 Fundación Karisma. 2015, Agosto. Un Estado en la sombra: Nuevo informe revela abusos de las agencias de inteligencia en Colombia en:

más allá de la vigilancia, identificación biométrica

La situación tiende a ser más problemática cuando hablamos de tecnología biométrica. El uso de tecnología biométrica en cámaras de vigilancia, si bien no es la regla, aumenta los problemas asociados con la videovigilancia al incorporar tecnología de reconocimiento facial y al crear bases de datos con información altamente sensible. Además, con tecnología de videovigilancia controlada y gestionada de forma remota a través de internet, se abre la posibilidad de la combinación de datos para la identificación de personas con el agravante de que la decisión sobre qué o a quién considerar sospechoso es tomada, en primera instancia, por sistemas automatizados que siguen reglas y buscan patrones preestablecidos para predecir potenciales actividades criminales.

¿Qué significa que las cámaras de vigilancia puedan tener incorporada tecnología biométrica para el reconocimiento facial? En resumen, signi-

https://karisma.org.co/un-estado-en-la-sombra-nuevo-informe-revela-abusos-de-las-agencias-de-inteligencia-en-colombia/

fica que las imágenes recogidas son procesadas para generar datos específicos sobre la identidad de las personas. Estos datos están, en general, relacionados con las medidas del rostro pero dependiendo de su uso permiten el rastreo y acumulación de información acerca de los desplazamientos, rutinas e intereses de una persona.[10]

no deberían instalarse cámaras en cualquier parte, por cualquier razón y menos aún añadir un sistema de comparación biométrica sin el debido análisis jurídico y de impacto a derechos humanos.

La vigilancia debería tener como objetivo proteger la vida y los bienes de las personas, que son fines constitucionalmente válidos. Sin embargo, por el nivel de interferencia que puede tener en los derechos de las personas solo puede plantearse en casos excepcionales cuando cumple con los requisitos de (1) legalidad, (2) objetivo imperativo, (3) necesidad, idoneidad y proporcionalidad, y (4) control judicial y debido proceso.[11] Por tanto, un sistema de vigilancia como el que analizaremos será legítimo y posible solo si consigue enmarcarse y cumplir con dichos requisitos. Sumado a esto, es necesario que la evaluación sea pública y se concrete en los documentos que sustentan la medida de instalación de cámaras en un lugar concreto. Finalmente, añadir el cotejo biométrico debería ser evaluado con el mismo estándar. De esta manera, no deberían instalarse cámaras en cualquier parte, por cualquier razón y menos aún añadir un sistema de comparación biométrica sin el debido análisis jurídico y de impacto a derechos humanos.

Con todo, es cierto que desde una perspectiva técnica la captura de información biométrica realizada por sistemas de reconocimiento facial tiene varias "ventajas" en comparación con otros sistemas de identificación biométrica. Estas "ventajas" son las mismas que se erigen como los principales riesgos de vulneración de derechos. Por ejemplo, se trata de una técnica "no intrusiva", pues no implica contacto directo con el cuerpo de la persona a quien se va a registrar. A diferencia de la huella digital o la lectura del iris, el reconocimiento facial puede hacerse a distancia y de manera encubierta.[12] En otras palabras, esto significa que tal tecnología se puede usar sin el consentimiento de la persona. Esto dificulta saber que se está siendo vigilado y, por lo mismo, afecta la capacidad de la población de limitar o cuestionar la vigilancia de la que se es objeto.

Al ser un procedimiento de rutina, es difícil tener claridad sobre la manera en que se gestiona, procesa y almacena la información. Sin procedimientos claros es difícil saber cómo se

10 Gabel Cino, J. 2017, Abril. *Facial recognition is increasingly common, but how does it work?* Disponible en: https://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354

11 Necessary and Proportionate. 2013. *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.* Disponible en: https://es.necessaryandproportionate.org/.

12 Stan Z. Li, Anil K. Jain. 2011. *Handbook of Facial Recognition.* London, England: Springer.

manejan los datos recolectados, quiénes tienen acceso a estos, durante cuánto tiempo existe un archivo, etc. Como si esto fuera poco, dentro de las desventajas reportadas, encontramos que siempre existe una probabilidad de que el sistema falle y genere falsas concordancias (cuando se identifica a una persona como otra, cuyo registro está en la base de datos) o falsas coincidencias (cuando no se logra identificar a una persona que sí está en la base de datos con la que se contrasta). Dependiendo de la luz, el ángulo, la distancia y la nitidez, los resultados de un cotejo pueden no coincidir o arrojar coincidencias equivocadas, los también llamados "falsos positivos".[13] Para que la tecnología de reconocimiento facial sea precisa, es necesario que las imágenes sean muy similares; mientras esto no pueda asegurarse, no se puede corroborar, por ejemplo, la utilidad del uso de reconocimiento facial en espacios abiertos en los que, además, transiten multitudes.

El uso de tecnologías biométricas puede funcionar tanto para la autenticación como para la identificación, pero se trata de dos modalidades con características distintas.

El uso del reconocimiento facial para la autenticación, en la que de antemano se ha tomado una imagen con la autorización y conocimiento de la persona, se puede utilizar para verificar que una persona sea la misma que está accediendo a un servicio, a un sistema, a una aplicación, etc. Contra la imagen capturada previamente, se cotejan las medidas del rostro que se toman en el momento real. En el reconocimiento facial para la identificación, se extraen las medidas de todos los rostros a las que tiene acceso un sistema y se comparan con las medidas presentes en una base de datos específica, buscando similitudes.

El primer uso suele ser el que se realiza en los puntos de control de migración de los aeropuertos, el segundo es el que podrían emplear las autoridades policiales a la hora de buscar a una "persona sospechosa" en un espacio público. En el caso de los sistemas que son empleados en un espacio público, todas las personas transeúntes son tratadas como sospechosas.

En cualquiera de los dos escenarios, es necesario tener una base de datos contra la cual se hacen las comparaciones. Plantear la construcción de esas bases de datos no es un problema menor. Precisar a quienes se pretende buscar debería ser un elemento central en el análisis de la viabilidad de un sistema de identificación biométrica. Esto permitiría saber si se justifica o no chequear diariamente a millones de personas buscando tan solo a cientas. Recordemos acá que el estándar en materia de derechos humanos de un sistema de este tipo, pasa por responder si cumple con los principios de legalidad, objetivo imperativo, necesidad, idoneidad y proporcionalidad, y control judicial y debido proceso.

Ahora bien, la base de datos debería tener solo la información que responda a una búsqueda específica que se quiere hacer. Si se quiere

13 Ibíd.

buscar a prófugos de la justicia o personas que tengan orden de captura pero que no hayan comparecido ante las autoridades, por ejemplo, es necesario tener una base de datos con su información biométrica de identificación facial. Es contra esta base de datos que se prueba a todas las personas cuya imagen es capturada por el sistema.

Como ya lo mencionamos, la implementación de sistemas de vigilancia requiere de un profundo análisis sobre sus capacidades, el marco legal que le aplica y la forma como se puede controlar su abuso. Esto es especialmente cierto si se trata de sistemas de vigilancia públicos que usan el poder del Estado. Sin embargo, en el momento en que se formuló el sistema de vigilancia con cámaras biométricas de Transmilenio, que se describirá con mayor detalle más adelante, nunca se precisó a quienes se quería buscar. El proyecto se encargó de explicar los aspectos técnicos (tipos de cámaras, capacidad de análisis realizados por minuto, tipo de conectividad, etc.) pero no profundizó en establecer su necesidad ni mucho menos su alcance. Jamás se habló de la base de datos necesaria para su funcionamiento. Nunca se aclaró de quién era esa responsabilidad y que implicaba. Mucho menos se miró cuales podrían ser los problemas, en términos de privacidad de una base de datos de este tipo. No hubo análisis de necesidad, idoneidad y proporcionalidad, ni de afectación a derechos humanos.

En la presentación del sistema que realizó la Alcaldía Mayor de Bogotá en marzo de 2015, y de la que hicieron eco diferentes medios locales y nacionales, el foco estaba en un deslumbre con los aspectos tecnológicos.[14] En su momento se presentó como una gran novedad que haría más segura a la capital y que era capaz de identificar a un periodista, ¡incluso con sombrero y unas gafas oscuras![15] Si bien este ejemplo habla de lo avanzados que pueden ser estos sistemas, no podemos dejar de lado que siempre existe la probabilidad de generar falsas correspondencias y que en la práctica se trata de un equipo que automáticamente, siguiendo unas reglas predeterminadas, nos trata a todas las personas como sospechosas.

En este contexto, la recolección de datos personales (como imágenes obtenidas mediante cámaras de vigilancia) en un espacio público constituye una clara interferencia al derecho a la intimidad, que aunque disminuido, no se pierde por el solo hecho de transitar por las

14 Alcaldía Mayor de Bogotá. 2015, Marzo. *Nuevo Sistema de Videovigilancia Inteligente para Transmilenio.* Disponible en: http://www.bogota.gov.co/content/nuevo-sistema-de-video-vigilancia-inteligente-para-transmilenio

15 Véase: W Radio. 2015, Marzo. *Transmilenio pone en marcha este martes cámaras de reconocimiento biométrico.* Disponible en: http://www.wradio.com.co/noticias/bogota/transmilenio-pone-en-marcha-este-martes-camaras-de-reconocimiento-biometrico/20150316/nota/2676753.aspx; El Espectador (Redacción Bogotá). 2015, Marzo. *$12.500 millones invirtió Distrito en cámaras de alta tecnología para Transmilenio.* Disponible en: https://www.elespectador.com/noticias/bogota/12500-millones-invirtio-distrito-camaras-de-alta-tecnol-articulo-549842; y Noticias RCN. 2015, Marzo. *Así funciona el sistema de reconocimiento facial que se implementa en Transmilenio.* Disponible en: http://www.noticiasrcn.com/nacional-bogota/asi-funciona-el-sistema-reconocimiento-facial-se-implementa-transmilenio

calles. No es lo mismo documentar potenciales crímenes cometidos en público, que identificar a personas indiscriminadamente en la vía pública. Dentro de este panorama, el Estado es el primer obligado a garantizar los derechos de las personas.

No es lo mismo documentar potenciales crímenes cometidos en público, que identificar a personas indiscriminadamente en la vía pública. Dentro de este panorama, el Estado es el primer obligado a garantizar los derechos de las personas.

Hay que considerar que en un sistema de videovigilancia con identificación biométrica no es solo la imagen lo que se está capturando sino que se está tratando esta información para extraer información biométrica, que ante la ley colombiana tiene un tratamiento especial. Incluso, esto es algo que nos hace cuestionar si es legal hacer un registro de este tipo de las personas que utilizan el sistema de transporte masivo de Transmilenio[16].

En Colombia los datos biométricos se consideran datos sensibles por la Ley de Protección de Datos (Título III, artículo 5). Este tipo de datos requiere un tratamiento especial que pasa por la autorización explícita del tratamiento de dicha información y la imposibilidad de que estos datos se suministren a terceros sin autorización. Teniendo en cuenta estas garantías consagradas en la ley, es entendible la dificultad que representa asumir la responsabilidad por el manejo de la información biométrica que es necesaria para la operación de este sistema. La implementación de una base de datos, al afectar derechos fundamentales, obliga en primer lugar a su creación mediante una ley.

Recordemos, entonces, que un sistema de vigilancia como el que se planteaba para Transmilenio se justifica tan solo en la medida en que se trate de una afectación necesaria, proporcional y adecuada; acreditando que no existen otros medios menos gravosos para mejorar la seguridad de la población que la implementación de un oneroso sistema de vigilancia, que, por lo demás, no solo afecta la intimidad, sino también el derecho a reunión, expresión, culto, protesta, entre otros.

16 El informe de Gestión del Fondo de Vigilancia y Seguridad Enero – Diciembre 2015 contiene en su cuerpo el detalle de los pagos realizados por los conceptos de los convenios 782 de 2014, 880 de 2014 y 885 de 2014 relacionados con el proyecto de implementación, diseño y puesta en funcionamiento de un sistema integrado de video vigilancia inteligente para Transmilenio. Fondo de Vigilancia y Seguridad, Alcaldía de Bogotá. 2015. Informe de gestión. Disponible en: http://www.fvs.gov.co/sites/default/files/planeacion/Informe%20de%20gesti%C3%B3n%202015.pdf.

el sistema que nunca existió

El sistema dejó instaladas 24 cámaras de reconocimiento facial, 120 cámaras IP fijas y 20 cámaras PTZ[17], además de un sistema que funciona con una base de pruebas de 96 registros. El propósito del sistema era "garantizar la seguridad de los ciudadanos y ciudadanas, en el sistema de transporte masivo de Bogotá".[18] No obstante, al igual que en otros sistemas similares, los estudios apuntan a que el verdadero propósito termina siendo vigilar áreas geográficas específicas, siguiendo patrones de discriminación y estigmatización a poblaciones marginales.[19] De hecho, llama la atención que entre los puntos del sistema de transporte masivo donde se

17 Pan, Tilt and Zoom: paneo, inclinación y ampliación.

18 Fondo de Vigilancia y seguridad, Alcaldía de Bogotá. 2016, Junio. *Situación del sistema integrado de videovigilancia biométrico de Transmilenio.* Disponible en: http://www.fvs.gov.co/noticias/situaci%C3%B3n-del-sistema-integrado-v%C3%ADdeovigilancia-biom%C3%A9trico-transmilenio-c%C3%A1maras-aportadas

19 Journalist's Resource. 2014, Febrero. *The effect of CCTV on public safety: Research roundup*. Disponible en: https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime

instalaron las cámaras de identificación biométrica no esté incluido el Portal Norte, que según las estadísticas oficiales de Transmilenio, históricamente es el que tiene la mayor demanda de todo el sistema[20] y una de las estaciones donde se presentan más robos.[21]

El sistema debió entrar en operación el 20 de marzo de 2015, pero para septiembre de ese mismo año aún no estaba en funcionamiento. En una entrevista radial, Jairo Osorio, quien era el gerente administrativo del Fondo de Seguridad y Vigilancia, manifestó: "[las cámaras] ni siquiera dejan registro archivado de lo que muestran".[22] Y añadió:

"[...] en el centro de monitoreo no hay grabación de lo que se está mirando con esas cámaras, usted ve en tiempo real lo que está sucediendo pero no hay posibilidad de hacer la grabación ni hay la conectividad directa [...]" [23]

También mencionó que el Fondo de Seguridad y Vigilancia no contaba con alguien que recibiera las cámaras; ni siquiera la Policía podía hacerlo porque no tenían conectividad y no iban a ninguna agencia de despacho.[24] Es decir que la Policía se lamentaba de que la señal no se conectaba directamente a sus oficinas. Además, al usar la expresión "agencias de despacho" también se hacía extensiva el acceso a este sistema por parte de otras autoridades, como Bomberos, para que pudieran analizar estas imágenes de manera centralizada.

Para mediados de 2016, y con el sistema aún sin operar, se informó que "[...] A pesar de ya estar instalados y conectados al Centro de Control, 24 de los dispositivos no están enlazados con bases de datos para comparar fotografías y detallar información".[25] No existía la base de datos de registros biométricos con la que se deberían cotejar los rostros de los millones de personas que usan el sistema de Transmilenio diariamente.

20 Servicio de Transporte Público *Transmilenio*. 2016, Septiembre. *Estadísticas de oferta y demanda del sistema integrado de transporte - SITP*. Disponible en: http://www.transmilenio.gov.co/Publicaciones/la_entidad/transparencia_y_acceso_a_la_informacion_publica_transmilenio/2_informacion_de_interes/estadisticas_de_oferta_y_demanda_del_sistema_integrado_de_transporte_publico_sitp

21 Publimetro Colombia. 2017, Septiembre. *Las 10 estaciones de Transmilenio donde más roban.* Disponible en: https://www.publimetro.co/co/bogota/2017/09/05/estaciones-de-transmilenio-donde-mas-roban.html

22 BLU Radio. 2015, Septiembre. *Cámaras de seguridad en Bogotá, que costaron $387 millones cada una, no graban.* Disponible en: https://www.bluradio.com/108994/camaras-de-seguridad-en-bogota-que-costaron-387-millones-cada-una-no-graban

23 Ibíd.

24 Las Agencias de Despacho, incluyen el Centro Automático de Despacho de la Policía Metropolitana de Bogotá - CAD-, la Dirección para la Prevención y Atención de Emergencias -DPAE-, el Cuerpo de Bomberos de Bogotá, el Centro Regulador de Urgencias -CRU-, la Policía de Tránsito y las demás instituciones que deseen adherirse, mediante Convenios, al Sistema integrado de seguridad y emergencias Número Único -123-. Disponible en: http://www.123bogota.gov.co/index.php/normatividad/decreto-451-de-2005/8-decreto-451-de-2005

25 Periódico *El Espectador* (Redacción Bogotá). 2016, Junio. *Aún en veremos cámaras de reconocimiento facial para Transmilenio.* Disponible en: https://www.elespectador.com/noticias/bogota/aun-veremos-camaras-de-reconocimiento-facial-transmilen-articulo-637688.

Según el reporte de la Secretaría Distrital de Gobierno: "[...] la Policía Metropolitana de Bogotá [...] no fue consultada antes de la compra y no cuenta con una base de datos necesaria para poder usarla con toda su capacidad en la seguridad de los usuarios [sic] de Transmilenio".[26]

¿Qué pasa hoy con todos esos equipos? Si no se usan para identificar rostros de "personas sospechosas", en todo caso ¿están funcionando? Si el sistema se usa para recolectar información de personas que transitan en las estaciones, ¿a dónde van a parar los datos?, ¿están todavía en prueba?

En el mismo comunicado, dicen que han realizado mesas de trabajo con la participación de:

[...] la Secretaría de Gobierno, el Fondo de Vigilancia y Seguridad, Transmilenio, Policía Nacional, Sijín, Dijín Registraduría Nacional y Seccional Bogotá, Fiscalía Seccional Bogotá y el Centro de Comando y Control (C4) para hallar una alternativa interinstitucional que permita la puesta en funcionamiento del sistema de vigilancia a través de estas cámaras.[27]

Y se dio un plazo máximo de seis meses para poner a funcionar el sistema. Después de haber invertido millones de pesos de nuestros impuestos, vieron que no era todo lo que querían y que, aunque tenían todos los juguetes, les faltaba lo más importante: ¡la base de datos!

¿Qué pasa hoy con todos esos equipos? Si no se usan para identificar rostros de "personas sospechosas", en todo caso ¿están funcionando? Si el sistema se usa para recolectar información de personas que transitan en las estaciones, ¿a dónde van a parar los datos?, ¿están todavía en prueba? En suma, a finales de 2017, no sabemos si hay planes realistas para su puesta en funcionamiento o si se trabaja en su eventual desmantelamiento.

26 Secretaría Distrital de Gobierno, Alcaldía de Bogotá. Sin fecha. *Administración distrital, comprometida con la seguridad en Transmilenio.* Disponible en: http://wwwold.gobiernobogota.gov.co/prensa/93-noticias/2038-administracion-distrital-comprometida-con-la-seguridad-en-transmilenio

27 Ibid.

del dicho al hecho

El sistema de cámaras biométrico de Transmilenio se basaba en la instalación de 24 cámaras repartidas entre 6 de las principales estaciones y portales del sistema (4 en el Portal Américas, 4 en el Portal 80, 6 en la estación Avenida Jiménez, 6 en la estación Ricaurte y 4 en la estación Héroes). En el sistema, las 24 cámaras biométricas se complementan con otras 140 cámaras (120 cámaras IP fijas y 20 cámaras PTZ), de forma tal que las cámaras de reconocimiento facial registran las imágenes, las procesan y extraen la información biométrica (medidas de los rostros), mientras que las restantes sirven para hacer seguimiento a una persona una vez es identificada.

Entre los requerimientos con los cuales se proyectó el sistema, nunca se habla de la construcción de la base de datos, siempre se da por hecho que la base existe o que se puede hacer. Los requerimientos se centran en los aspectos técnicos.

De acuerdo con el Fondo de Vigilancia y Seguridad, entidad que hizo el contrato, la información

En realidad, cuando se formuló el proyecto nunca se precisó a quienes se quería buscar y, por tanto, nunca se pensó en quien debería aportar la base de datos necesaria para operar el sistema. Nunca se aclaró de quién era esa responsabilidad y qué implicaba.

biométrica que recogen las 24 cámaras con esta tecnología, se debía comparar con una base de datos de "personas condenadas".[28] Cuando se produjera una coincidencia entre un rostro y la información de la base de datos, se generaría una alerta que activaría el seguimiento de la persona identificada con las cámaras cercanas. La alerta facilitaría la acción correspondiente por parte de la Policía Nacional.

Sin embargo, la expresión "base de datos de personas condenadas" aparece por primera vez en el comunicado del Fondo de Vigilancia y Seguridad cuando se explica porque el sistema no había entrado en operación en el momento. Aunque en un principio el proyecto proclamaba garantizar la seguridad de los ciudadanos y ciudadanas en el sistema de transporte masivo de Bogotá, una vez hechas las pruebas, el sistema no puede operar por la inexistencia de la base de datos contra la cual hacer las búsquedas; fue así que se empezó a hablar de la necesidad de construir aquella base de datos de "condenados". En realidad, cuando se formuló el proyecto nunca se precisó a quienes se quería buscar y, por tanto, nunca se pensó en quien debería aportar la base de datos necesaria para operar el sistema. Nunca se aclaró de quién era esa responsabilidad y qué implicaba. Esto nos permite concluir que el sistema se montó sin un análisis sobre el marco jurídico relacionado con el uso de información biométrica y por tanto sin analizar mecanismos para garantizar los derechos de las personas.

Ubicación	Biométricas (Rec. Facial)	IP Fijas	PTZ	Total
Portal Américas	4	24	5	33
Portal 80	4	18	5	27
Estación Jiménez	6	23	3	32
Estación Ricaurte	6	27	1	34
Estación Héroes	4	14	3	21
Estación Calle 26	0	10	2	12
Estación Las Aguas	0	4	1	5
TOTAL DE CÁMARAS	**24**	**120**	**20**	**164**

Tabla No.1. Ubicación y funcionalidades de las cámaras de seguridad aportadas por el Fondo de Vigilancia y Seguridad a Transmilenio[29]

28 Esto es lo que decía la página del Fondo de Vigilancia y Seguridad: *"El FVS viene adelantando gestiones con la Policía, la Dijin, la Registraduría, la Fiscalía, para construir una verdadera base de datos con registros de personas condenadas para que estas cámaras puedan prestar a cabalidad el servicio de reconocimiento facial".* Fondo de Vigilancia y Seguridad (en liquidación), Alcaldía Mayor de Bogotá. 2016, Junio. *Situación actual del Sistema Integrado de Videovigilancia Biométrico para Transmilenio. Cámaras aportadas por el Fondo de Vigilancia y Seguridad de Bogotá.* Disponible en: http://www.fvs.gov.co/noticias/situaci%C3%B3n-del-sistema-integrado-v%C3%ADdeovigilancia-biom%C3%A9trico-transmilenio-c%C3%A1maras-aportadas

29 Ibid.

Sabemos, por los comunicados de prensa y las noticias que han hecho cubrimiento de los avances, que la instalación de las cámaras, y la puesta en funcionamiento del sistema de identificación se realizó, pero solo con una base de datos de prueba.

De la información técnica suministrada sobre el sistema para su implementación, podemos inferir como debería haber sido su funcionamiento.[30] La infraestructura que requiere este sistema no termina en las cámaras, de hecho, cada una de estas se conectaría con un sistema de procesamiento presente en los portales y estaciones en donde están instaladas. Cada uno de estos sistemas debería tener una copia de la base de datos contra la que haría el contraste para identificar a quienes se esté buscando. Las bases de datos en los portales y estaciones deberían sincronizarse con la base de datos ubicada en el centro de control y monitoreo. Así, en cada estación se debería hacer la confrontación automática de la información biométrica de los rostros capturados por la cámara, con la información biométrica consignada en la base de datos.

El centro de control y monitoreo se encontraría en el centro de gestión de Transmilenio. Es el lugar donde se encuentra el sistema centralizado de información, la versión primaria de la base de datos para cotejo de datos biométricos, el sitio web, el sistema de alertas y una gran pantalla de visualización donde se podrían ver las imágenes generadas por las cámaras que componen el sistema.

Este gran sistema de vigilancia debería estar a cargo de una sola persona, la operadora del sistema. A este personaje le correspondería estar pendiente del sistema de alertas generado automáticamente por las cámaras de reconocimiento biométrico. Para hacer el seguimiento remoto de la persona sospechosa, en caso de ser necesario, la persona operaria debería controlar remotamente las demás cámaras o enviar la información de la alerta a los diez dispositivos móviles que también harían parte del sistema y que estarían en manos de personas encargadas de la respuesta en los portales y estaciones.

Tal como se concibió, la idea era manejar tres tipos de actuaciones diferentes dependiendo del nivel de coincidencia de la identificación. Si el sistema encontraba una coincidencia plena, se generaba una alerta que llegaría a los celulares de aquellos encargados de la seguridad en cada estación. El sistema también podía actuar ante identificaciones parciales o dudosas, caso en el que se activaba un protocolo de seguimiento para realizar una comparación visual con el fin de obtener una identificación más exacta y poder definir una acción.

30 Empresa de telecomunicaciones de Popayán S.A. EMTEL E.S.P. 2015, Enero. *Informe estudio de propuestas.* Disponible en: https://tinyurl.com/ybt9vzto

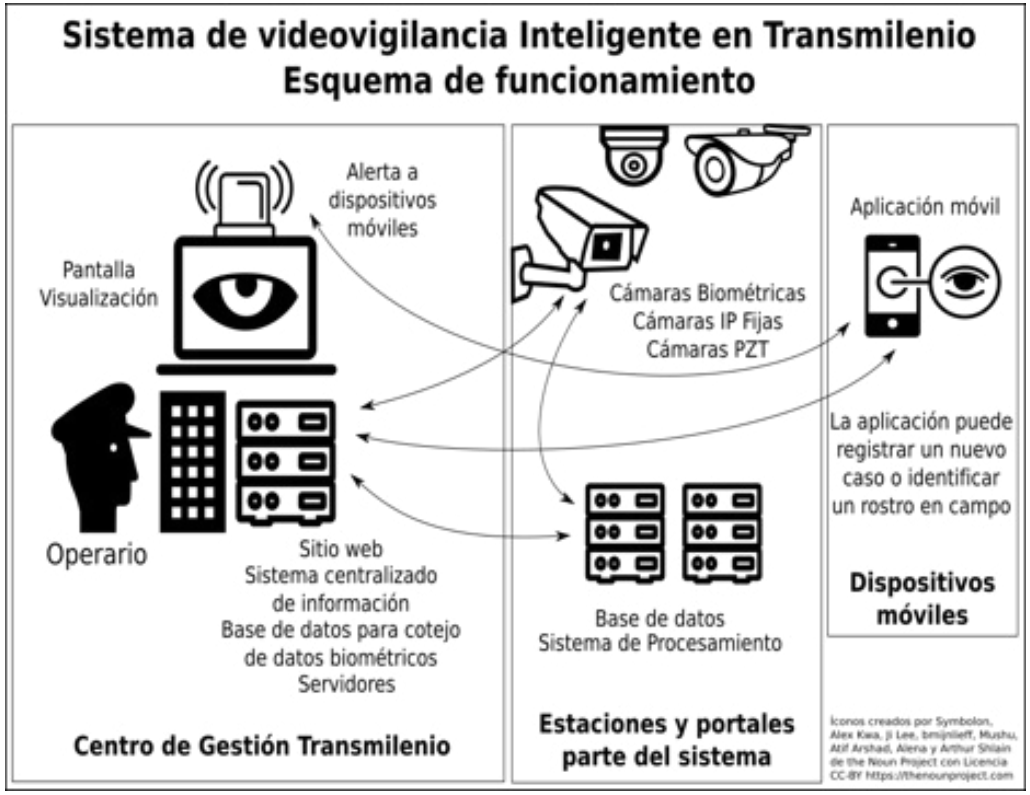

Imagen No. 1. Esquema de funcionamiento del Sistema de videovigilancia Inteligente en Transmilenio. Construido con información del Informe Estudio de Propuestas de EMTEL.[31]

No hay información sobre hasta dónde quedó operando el sistema. Sabemos, por los comunicados de prensa y las noticias que han hecho cubrimiento de los avances, que la instalación de las cámaras, y la puesta en funcionamiento del sistema de identificación se realizó, pero solo con una base de datos de prueba[32]. Es la falta de la base de datos y el problema que implica su construcción lo que genera el retraso en la entrada en funcionamiento completo del sistema.

Aun cuando la atención de este tipo de sistemas se centra en la capacidad de identificación que tienen las cámaras de reconocimiento biométrico, el corazón de este sistema, en particular, es la base de datos contra la que se deben hacer todos los cotejos, esta es la base que no existe.

31 Ibid.

32 Fondo de Vigilancia y Seguridad (en liquidación), Alcaldía Mayor de Bogotá. 2016, Junio. *Situación actual del Sistema Integrado de Videovigilancia Biométrico para Transmilenio. Cámaras aportadas por el Fondo de Vigilancia y Seguridad de Bogotá.* Disponible en: http://www.fvs.gov.co/noticias/situaci%C3%B3n-del-sistema-integrado-v%C3%ADdeovigilancia-biom%C3%A9trico-transmilenio-c%C3%A1maras-aportadas

la ‘letra chiquita’ del sistema

Cualquier sistema de reconocimiento facial precisa un software que sea capaz de identificar automáticamente a una persona en una imagen digital. Para que esto sea posible se deben analizar las características faciales de la persona extraídas de una imagen, ya sea desde una fotografía o un fotograma de un video, y compararlas con la información existente en una base de datos.

El análisis de la imagen parte de la detección del rostro y su alineación para localizar los componentes del rostro y la transformación de esa información siguiendo un estándar preestablecido mediante transformaciones geométricas. Hay diferentes reglas para extraer el patrón como la distancia entre ojos, posición y geometría de la boca, distancia entre las cejas, etc. Una vez obtenido el patrón se compara con los contenidos en la base de datos que se haya seleccionado para hacer el cotejo. El resultado de la comparación es un porcentaje de similitud.

el sistema de reconocimiento falla si el rostro que se quiere reconocer no está en un ángulo apropiado, si no se tiene la iluminación apropiada, si se utilizan objetos que impidan la medición de las características del rostro y en general los algoritmos de reconocimiento no siempre son capaces de distinguir un rostro si la expresión facial es diferente a la almacenada en la base de datos.

En el proceso de identificación propuesto para el sistema de Transmilenio, el sistema debía tomar el patrón extraído de la imagen de video en vivo y compararlo contra cada uno de los patrones registrados en la base de datos, buscando aquellos que tuvieran un nivel de similitud suficiente para generar una alerta de identificación. Estos niveles de similitud se configurarían en el sistema. La idea era tener un proceso de identificación de alta velocidad y efectividad, que pudiera realizar la identificación en cuestión de segundos sobre una base de datos de más de un millón de registros.[33]

La gran ventaja de este tipo de sistemas, supuestamente, es la posibilidad que brinda de realizar identificaciones no invasivas, en movimiento, a distancia, sin que las personas se den cuenta (ni consientan ni puedan negarse, por cierto) que su imagen se está capturando, procesando, analizando, comparando y posiblemente almacenando. Sin embargo, son bien conocidas las limitaciones del proceso.

Como ya lo habíamos mencionado, el sistema de reconocimiento falla si el rostro que se quiere reconocer no está en un ángulo apropiado, si no se tiene la iluminación apropiada, si se utilizan objetos que impidan la medición de las características del rostro y en general los algoritmos de reconocimiento no siempre son capaces de distinguir un rostro si la expresión facial es diferente a la almacenada en la base de datos.

Por eso, la forma como la Alcaldía y los medios presentaron la noticia no deja de ser una forma de ampliar la leyenda. La posibilidad de que el sistema reconozca a alguien con sombrero es remota (posiblemente se dé bajo condiciones de laboratorio) pero es difícil en medio de una multitud en una estación de Transmilenio en hora pico. No obstante, parece que cuestionamos muy poco la infalibilidad de la tecnología. Bajo la premisa de que la tecnología puede resolver todos los problemas sociales de manera fácil y a bajo costo, terminamos implementando soluciones sin hacer un diagnóstico serio de los problemas que queremos resolver, ni de formas de resolverlos que puedan ser más eficientes y respetuosas de nuestros derechos.

33 Empresa de telecomunicaciones de Popayán S.A. EMTEL E.S.P. Op. cit., p. 8.

¿y dónde está la base de datos?

A lo largo de este documento hemos hecho énfasis en que para justificar y poner a funcionar un sistema de identificación biométrica es necesario definir a quienes se quiere buscar. Construir una base de datos con la cual se contrasten los rostros de millones de personas es realmente el meollo del asunto, tanto desde el punto de vista técnico, como desde el jurídico y hasta el administrativo. Para que este sistema opere se requiere una base de datos centralizada, sincronizada con cada una de las estaciones que albergue la información biométrica de los rostros de las personas que quiere reconocer, a las que están buscando. Es una base de datos que no se definió para la compra del sistema y que el Fondo de Vigilancia y Seguridad llegó a señalar como de personas "condenadas". Cuántas personas entran en esa categoría es algo que se desconoce.

El sistema se pensó para revisar millones de registros, pero si al final el propósito del sistema es buscar a quienes se escapen del sistema penal, se tendría que considerar que según da-

tos del 2015, en el país se dieron 51.000 condenas[34] y se lograron cerca de 260.000 capturas de las que 50.000 se realizaron en Bogotá.[35] En ninguna parte se ha encontrado información específica sobre cuántos registros, y extraídos de dónde, se iban a utilizar para construir la base de datos por lo que hablar de buscar "personas condenadas" es ambiguo.

Hasta donde se sabe, todas las pruebas de funcionamiento del sistema instalado en Transmilenio se realizaron con un base de pruebas de 96 registros.[36] En todo caso, tanto en el comunicado del Fondo de Vigilancia y Seguridad sobre la situación del sistema integrado de videovigilancia biométrico para Transmilenio, como en las diferentes noticias que hicieron eco del tema, se fue conociendo cómo esa base de datos era lo que hacía falta para que el sistema entrara en operación plena.[37]

En junio de 2016, tras un cambio en la administración del Fondo de Vigilancia y Seguridad, en el mismo comunicado sobre la situación del sistema integrado de videovigilancia biométrico para Transmilenio, se indicó que el Fondo de Vigilancia y Seguridad estaba "adelantando gestiones con la Policía, la Dijin, la Registraduría, la Fiscalía, para construir una verdadera base de datos con registros de personas condenadas para que estas cámaras puedan prestar a cabalidad el servicio de reconocimiento facial"[38].

Explican, además, que "desde que se compraron e instalaron las cámaras biométricas no ha existido una base de datos completa"[39]. También afirman que su objetivo es "que en un plazo máximo de 6 meses esta base de datos esté construida para solucionar este inconveniente"[40]. Sin embargo, hasta la fecha no hay información de la creación de tal base de datos.

Obviamente, la construcción de una base de

34 Segun cifras del 2015 sobre la impunidad en Colombia dice el Fiscal General de la Nación que: "extrapolando el número de denuncias el año anterior con la base de criminalidad oculta, en el 2015 se habrían cometido en el país 3.5 millones de delitos, es decir que las 51 mil condenas representan escasamente el uno por ciento de los mismos". Monsalve Gaviria, Ricardo. 2016, Agosto. *99% de los delitos quedan en la impunidad: Fiscal.* El Colombiano. Disponible en: http://www.elcolombiano.com/colombia/99-de-los-delitos-quedan-en-la-impunidad-fiscal-JI4785092

35 Estos datos se extrajeron del Sistema de Estadísticas en Justicia, del ministerio de Justicia: http://sej.minjusticia.gov.co/PoliticaCriminalYPenitenciaria/Paginas/Capturas.aspx

36 *Administración distrital, comprometida con la seguridad en Transmilenio* en: http://www.fvs.gov.co/noticias/situaci%C3%B3n-del-sistema-integrado-v%C3%ADdeovigilancia-biom%C3%A9trico-transmilenio-c%C3%A1maras-aportadas

37 Caracol Radio. 2016, Junio. *En seis meses estará lista la conexión entre las cámaras de seguridad de Transmilenio.* Disponible en: http://caracol.com.co/emisora/2016/06/14/bogota/1465908618_604389.html, http://www.eldiariobogotano.com/controversia-por-fallas-en-camaras-de-vigilancia-en-estaciones-de-transmilenio/

38 Fondo de Vigilancia y Seguridad (en liquidación), Alcaldía Mayor de Bogotá. 2016, Junio. *Situación actual del Sistema Integrado de Videovigilancia Biométrico para Transmilenio. Cámaras aportadas por el Fondo de Vigilancia y Seguridad de Bogotá.* Disponible en: http://www.fvs.gov.co/noticias/situaci%C3%B3n-del-sistema-integrado-v%C3%ADdeovigilancia-biom%C3%A9trico-transmilenio-c%C3%A1maras-aportadas

39 Ibid.

40 Ibid.

En todo caso, el análisis precisamente olvidaba lo más importante y es que la construcción de la base de datos requiere de una consagración legal porque, como ya dijimos, en Colombia los datos biométricos se consideran datos sensibles por la Ley de Protección de Datos y su tratamiento pasa por la autorización explícita y la imposibilidad de entregarlos a terceros sin autorización.

este tipo no es una responsabilidad que pueda asumir el Fondo de Vigilancia y Seguridad o Transmilenio, entidades que no tienen facultades para hacerlo. Tal como el Distrito explicó en su momento, se requiere un trabajo interinstitucional:

En las mesas de trabajo convocadas desde febrero han participado la Secretaría de Gobierno, el Fondo de Vigilancia y Seguridad, Transmilenio, la Policía Nacional, la Sijín, la Dijín, la Registraduría Nacional, la Fiscalía y el Centro de Comando y Control (C4) para hallar una alternativa interinstitucional que permita la puesta en funcionamiento del sistema de vigilancia a través de estas cámaras.[41]

En todo caso, el análisis precisamente olvidaba lo más importante y es que la construcción de la base de datos requiere de una consagración legal porque, como ya dijimos, en Colombia los

41 Ibid.

datos biométricos se consideran datos sensibles por la Ley de Protección de Datos[42] y su tratamiento pasa por la autorización explícita y la imposibilidad de entregarlos a terceros sin autorización. Por lo tanto, la implementación de una base de datos, al afectar derechos fundamentales, obliga a su creación por ley.

Tras estos anuncios de junio de 2016, en los cuales se decía que el trabajo continuaba, poco se ha vuelto a conocer sobre el estado actual del sistema. En marzo de 2017, el concejal de Bogotá, Julio César Acosta, denunció que "[e]l sistema de video vigilancia biométrica para Transmilenio, terminó siendo un monumento al despilfarro, sin ningún beneficio real para la seguridad de todos los bogotanos [sic]".[43]

Además, el Concejal aseguró:

[...] el sistema de video vigilancia biométrica de Transmilenio, sigue siendo un adorno en estaciones y portales, porque aún se está tratando de poner en funcionamiento el centro de monitoreo y las bases de datos para el reconocimiento facial siguen sin estar listas.[44]

42 Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

43 Caracol Radio. 2017, agosto. *Cámaras instaladas en Transmilenio y en entornos escolares no funcionan.* Disponible en: http://caracol.com.co/emisora/2017/03/08/bogota/1489002031_640175.html, http://www.elnuevosiglo.com.co/articulos/03-2017-en-bogota-no-funciona-el-37-de-camaras-para-vigilancia

44 Gente Noticias. 2017, noviembre. "*Cámaras de vigilancia en Bogotá, un fiasco y un monumento al*

Si bien concordamos con el Concejal en que el sistema ha sido un despilfarro y no llegó a ser más que un adorno en las estaciones, se equivoca al señalar que ese es su único problema. Como se ha expuesto a lo largo del documento, el supuesto beneficio a la seguridad de las personas que habitan la ciudad está en entre dicho. Más allá del problema de gasto estamos ante un sistema que posiblemente atentaría contra la intimidad de millones de personas al tratar a cualquiera que utilice el sistema masivo de transporte como un eventual sospechoso. Un sistema que no fue diseñado pensando en quienes se quería buscar y que, por tanto, nunca fue dimensionado objetivamente. De hecho hay literatura que sugiere que los primeros en adaptarse a la presencia de sistemas de vigilancia son quienes delinquen[45], mientras que quienes sufren más sus consecuencias son las personas marginadas y vulnerables, que suelen ser estigmatizadas solo por su apariencia.[46]

hay literatura que sugiere que los primeros en adaptarse a la presencia de sistemas de vigilancia son quienes delinquen, mientras que quienes sufren más sus consecuencias son las personas marginadas y vulnerables, que suelen ser estigmatizadas solo por su apariencia.

A la fecha no se ha vuelto a hablar de si algún día entrará en operación el sistema que ya está, en todo caso, instalado en Transmilenio.

despilfarro": Concejal Julio Cesar Acosta. Disponible en: https://webcache.googleusercontent.com/search?q=cache:RBjJEIxVo_oJ:www.gentenoticias.com/index.php%3Foption%3Dcom_k2%26view%3Ditem%26id%3D1374:camaras-de-vigilancia-en-bogota-un-fiasco-y-un-monumento-al-despilfarro-concejal-julio-cesar-acosta%26Itemid%3D121+&cd=1&hl=es-419&ct=clnk&gl=co

45 Bowe, Rebecca. 2012, Septiembre. *Freedom Not Fear: CCTV Surveillance Cameras In Focus. Electronic Frontier Foundation.* Disponible en: https://www.eff.org/es/deeplinks/2012/09/freedom-not-fear-cctv-surveillance-cameras-focus

46 Patel, Tina G. 2012. *Surveillance, Suspicion and Stigma: Brown Bodies in a Terror-Panic Climate. Surveillance & Society 10(3/4): 215-234.* Disponible en: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/download/stigma/stigma/

biometría para rato, el caso de los estadios del país

La posibilidad de la existencia de una base datos con información biométrica que permita la utilización de sistemas de reconocimiento facial, como el que se quería poner a funcionar en Transmilenio, vuelve a aparecer cuando se escucha de otros posibles proyectos que involucran sistemas de vigilancia con identificación biométrica. Actualmente, en Colombia se trabaja en un sistema de vigilancia biométrica para los estadios del país que también debería preocuparnos.

Ya se ha anunciado la utilización de cámaras biométricas en los estadios del país[47] y para ese efecto se encuentra en marcha un programa piloto de carnetización de los hinchas de la Liga Colombiana de Fútbol, con los aficionados de Cali, Medellín, Bogotá y Barranquilla.[48]

47 Periódico El Colombiano. 2016, Mayo. *Gobierno colombiano implementará biometría en los estadios*. Disponible en: http://www.elcolombiano.com/deportes/futbol-colombiano/gobierno-colombiano-implementara-biometria-en-los-estadios-XM4086101

48 Prensa DIMAYOR. 2017, junio. *La carnetización de los hinchas en Colombia es una realidad.* Disponible en: http://www.eltiempo.com/deportes/futbol-colombiano/

Como en el caso del sistema de identificación biométrica de Transmilenio, la idea de utilizar un sistema de identificación biométrica en los estadios cuenta con los mismos problemas.

Inicialmente se está haciendo un reconocimiento manual de los aficionados que van a los estadios, pero se espera que el proceso sea automatizado cuando:

[...] los entes gubernamentales se encarguen de instalar la infraestructura tecnológica en los estadios: torniquetes con control biométrico y dispositivos de reconocimiento de huella digital [...][49]

Así, se espera poder "verificar los antecedentes judiciales de quienes ingresen a los partidos de fútbol".[50]

En Medellín, ya están en funcionamiento más de 170 cámaras en sitios estratégicos del estadio Atanasio Girardot. Esto, junto con un proceso de enrolamiento en el cual toman la fotografía de la persona e ingresan los datos personales a través del código de barras de la cédula de ciudadanía, ha permitido "crear la base de datos de los hinchas y amantes del fútbol que acuden a los estadios y poder luego identificarlos tanto en el ingreso, como durante el partido y fuera de él".[51]

Más allá de esta base de datos que se está construyendo, y de acuerdo a la misma nota de prensa sobre la modernización del estadio de Medellín, la idea es que:

[cuando] la Policía identifica una persona que haya realizado alguna acción no permitida dentro del estadio se ingresa a una lista [negativa], que permite que al ser reconocido por alguna cámara se genere una alerta en el sistema que puede ser enviada a un correo electrónico o a un celular y la persona sea capturada y procesada. [52]

Como en el caso del sistema de identificación biométrica de Transmilenio, la idea de utilizar un sistema de identificación biométrica en los estadios cuenta con los mismos problemas. Si bien en este caso hay una base de datos clara, la de los hinchas que se enrolan de forma voluntaria, la construcción de la lista negativa carece de las mismas garantías que la base de condenados de la que hablamos en el caso del sistema de transporte en Bogotá. En todo caso, parece que padecemos de un exceso de optimismo sobre las capacidades de la tecnología y no tenemos inconveniente en gastar millones en la implementación de tales sistemas sin tener idea sobre su efectividad y sin considerar las afectaciones en materia de derechos humanos que puedan estar asociadas con su puesta en marcha.

proceso-de-carnetizacion-de-los-hinchas-del-futbol-profesional-colombiano-101994

49 Fútbol Red. 2017, julio. *Así es el proceso de carnetización de los hinchas de la Liga Águila II.* Disponible en:http://www.futbolred.com/liga-aguila/proceso-para-la-carnetizacion-de-los-hinchas-de-liga-2017+16858281

50 Ibid.

51 Contreras, Nicolás. 2016, mayo. *Cómo funcionaría el reconocimiento facial en los estadios.* Caracol Radio. Disponible en: http://caracol.com.co/radio/2016/05/20/tecnologia/1463776971_227801.html

52 Ibid.

legislación de los sistemas de video-vigilancia en Colombia

En la actualidad existen en Colombia dos leyes vigentes sobre sistemas de videovigilancia: la Ley 1843 del 2017, que regula los sistemas de detección de infracciones de tránsito, más conocida como "fotomultas", y el artículo 237 del Código Nacional de Policía, que establece que toda la información contenida en sistemas de vigilancia que se encuentran en el espacio público es información pública y de libre acceso para las autoridades policiales. No hay ninguna ley que hable de biometría en sistemas de vigilancia.

Tampoco hay proyectos de ley relacionados con biometría. Pero, sí hay al menos tres proyectos de ley sobre video vigilancia: (1) un proyecto que busca crear un programa comunal de apoyo y conexión de cámaras de seguridad en Bogotá (Proyecto de Acuerdo 198 de 2014)[53]; (2) un proyecto de ley, propuesto por el Centro Democrático, para implementar sistemas de vigilancia y monitoreo donde cooperen

53 Consulta de la norma en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=58799

No hay ninguna ley que hable de biometría en sistemas de vigilancia.

En todo caso debemos resaltar que ninguno de esos proyectos ha sido respaldado con evidencia de la efectividad de la vigilancia con cámaras.

la Policía Nacional y las empresas de seguridad privada[54]; y (3) un proyecto de ley con el que se pretendía hacer obligatorio el uso de cámaras de vigilancia en las entradas y salidas de todas las instituciones educativas del país.[55]

La legislación general sobre los sistemas de videovigilancia se sostiene sobre las ideas de que se puede "mejorar la prevención y reacción frente al delito de manera más eficaz"[56], además de que "la grabación opera como prueba reina para iniciar los procesos contra hechos delictivos que se presentan en la ciudad".[57] En todo caso debemos resaltar que ninguno de esos proyectos ha sido respaldado con evidencia de la efectividad de la vigilancia con cámaras.

Por lo tanto, en Colombia no hay una ley que regule comprensiva y sistemáticamente la instalación y uso de cámaras de vigilancia. Sin embargo, la Corte Constitucional ha abordado el tema en diversas ocasiones y ha reconocido que "[l]os derechos que se pueden afectar en el espacio público por la presencia de cámaras, incluyen la libertad de expresión, de manifestación y reunión, así como el derecho a la intimidad y a la protección de la persona "en su capacidad de decidir cómo presentarse al mundo".[58] Este reconocimiento impone la necesidad de evaluar si la instalación de cámaras en un espacio cualquiera supera el test de proporcionalidad, en el cual se evalúa que el fin buscado sea legítimo, que su búsqueda sea imperiosa, que la intervención sea adecuada, conducente y necesaria, es decir, que no haya una alternativa menos lesiva. Finalmente, incluye un juicio de proporcionalidad estricto en el que debe evaluarse si la medida es clara-

54 Centro Democrático (partido político). 2016. *Proyecto de ley mediante el cual se adoptan medidas tendientes a fortalecer la seguridad ciudadana urbana en las capitales, distritos y municipios de primera y segunda categoría, así como aquellos de categoría especial.* Disponible en: http://www.centrodemocratico.com/sites/default/files/p.l._fortalecimiento_seguridad_urbana-_art._y_expo.pdf

55 Artículo 20, Congreso de la República. *Proyecto de Ley busca fortalecer el sistema de video vigilancia en colegios.* Disponible en: http://www.articulo20.com.co/contenidos/detalle/proyecto-de-ley-busca-fortalecer-el-sistema-de-video-vigilancia-en-colegios.php

56 Cámara de representantes de la República de Colombia. *Informe de ponencia para primer debate al Proyecto de Ley 182 de 2016.* Disponible en: http://www.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=22&p_numero=182&p_consec=47327

57 Proyecto de Acuerdo 198 de 2014. "Por medio del cual se crea el programa comunal de apoyo y conexión de cámaras de seguridad en el Distrito Capital" Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=58799

58 Corte Constitucional. Sentencia T-407 de 2012. Magistrado Ponente Gabriel Eduardo Mendoza Martelo. Disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2012/T-407-12.htm

mente superior a las restricciones que impone a los derechos fundamentales afectados.[59]

Debido a la ausencia de una norma jurídica que señale claramente las condiciones en las que es legítimo instalar un sistema de vigilancia, se impone la necesidad de justificar con más transparencia las razones por las que un sistema de cámaras puede solucionar un problema de seguridad concreto. Sin información, por ejemplo, sobre cuántas personas son judicializadas a través del material recopilado por este tipo de sistemas, la justificación de la vigilancia es muy difícil. Lo anterior aplica por extensión y en mayor medida a temas de biometría debido a que, como ya vimos, la posible interferencia en los derechos humanos es todavía mayor.

En contraste con la ausencia de un marco jurídico para este tipo de proyectos, el Foro Europeo de Seguridad Urbana elaboró la Carta de uso democrático de la videovigilancia[60], que buscaba poner a la persona en el centro de las preocupaciones en estos sistemas, y lograr el respeto al derecho a la intimidad. Este documento presenta unos principios que deben guiar la elaboración, funcionamiento y desarrollo de los sistemas públicos de vigilancia por video. Entre ellos está el de legalidad, necesidad y proporcionalidad. Difícilmente puede decirse que Bogotá tiene un programa de videovigilancia necesario y proporcional cuando uno de sus objetivos es cubrir toda la ciudad con estos dispositivos.[61] La Carta también trae los principios de transparencia, responsabilidad, supervisión independiente y participación ciudadana.

59 Ibid.

60 Botero, C. Castañeda, J. Toledo, A. 2016, marzo. *En los ojos de Bogotá está su inteligencia: cámaras de vigilancia y la idea de ciudad inteligente.* Disponible en: https://antivigilancia.org/es/2016/03/en-los-ojos-de-bogota-esta-su-inteligencia-camaras-de-vigilancia-y-la-idea-de-ciudad-inteligente/

61 Alcaldía Mayor de Bogotá, Secretaría General. 2018, enero *Bogotá ya cuenta con más de 1.500 cámaras de seguridad en funcionamiento*. Disponible en: http://www.bogota.gov.co/temas-de-ciudad/gobierno-seguridad-y-convivencia/bogota-ya-cuenta-con-mas-de-1500-camaras-de-seguridad-en-funcionamiento

conclusiones

El aumento del gasto público en cámaras de seguridad en Colombia está directamente vinculado con un imaginario sobre su eficacia, que ha sido alimentado por los medios de comunicación a través de la instrumentalización de algunos casos donde las cámaras son funcionales. Estos han sido, además, muy bien aprovechados por los políticos como justificación para la inversión de miles de millones de pesos.

Ahora bien, no se trata de decir que las cámaras no deberían existir, pues efectivamente sirven para resolver crímenes, pero no se deben tomar a la ligera las políticas públicas que las involucran pues está en juego el ejercicio de derechos humanos como la intimidad y la libertad de expresión. Es necesario pensar en la construcción de indicadores sobre la efectividad de su uso que ayuden a justificar o no, la necesidad, idoneidad y proporcionalidad de estas medidas.

La tecnología biométrica incrementa los problemas asociados con los sistemas de video-

vigilancia al incorporar tecnología de reconocimiento facial y requerir bases de datos con información altamente sensible. Para la formulación e implementación del sistema de vigilancia con cámaras biométricas de Transmilenio no hubo análisis de proporcionalidad, ni necesidad, ni de afectación a derechos humanos. Debido a la ausencia de una norma jurídica que señale claramente las condiciones en las que es legítimo instalar un sistema de vigilancia, se impone la obligación de justificar con detalle la necesidad de un sistemas de este tipo con más transparencia. Se recomienda para futuros proyectos incluir dentro de sus justificaciones el resultado de un análisis de impacto en derechos humanos, considerando los principios mínimos de (1) legalidad, (2) objetivo imperativo, (3) necesidad, idoneidad y proporcionalidad, y (4) control judicial y debido proceso.

El aumento del gasto público en cámaras de seguridad en Colombia está directamente vinculado con un imaginario sobre su eficacia, que ha sido alimentado por los medios de comunicación a través de la instrumentalización de algunos casos donde las cámaras son funcionales.

En el diseño de este tipo de sistemas, es necesario además, explicar las razones por las que un sistema de cámaras puede solucionar un problema de seguridad concreto, pues como lo dijo la Corte Constitucional "[l]os derechos que se pueden afectar en el espacio público por la presencia de cámaras, incluyen la libertad de expresión, de manifestación y reunión, así como el derecho a la intimidad y a la protección de la persona "en su capacidad de decidir cómo presentarse al mundo".[62]

Dada la necesidad de construir bases de datos con información biométrica para la puesta en marcha de sistemas de videovigilancia con identificación biométrica, y teniendo en cuenta la experiencia fallida del sistema de Transmilenio (donde al parecer la formulación del proyecto no incluyó pensar realmente a quiénes se quería buscar y, por tanto, nunca se dimensionó las implicaciones de la construcción, gestión y manejo de tal base de datos), es necesario, para futuros proyectos de este tipo, identificar claramente quien va a ser la población objeto de búsqueda, quien debería aportar la información para construir la base de datos necesaria para operar el sistema y quien tiene la autoridad y los permisos de ley para acceder, gestionar y almacenar dicha información.

En el caso del sistema de videovigilancia con identificación biométrica de Transmilenio, al parecer nunca se analizó si en su alcance se violaban los derechos de quienes usaban el sistema ni se planteó la forma como se debería incorporar controles para evitar que esto sucediera.

62 Corte Constitucional. Sentencia T-407 de 2012. Magistrado Ponente Gabriel Eduardo Mendoza Martelo. Disponible en: http://www.corteconstitucional.gov.co/RELATORIA/2012/T-407-12.htm

En el caso del sistema de videovigilancia con identificación biométrica de Transmilenio, al parecer nunca se analizó si en su alcance se violaban los derechos de quienes usaban el sistema ni se planteó la forma como se debería incorporar controles para evitar que esto sucediera.

En suma, como no lo miraron de forma integral, la ausencia de base de datos hizo que el complejo sistema ya diseñado, financiado y funcional para pruebas, no pudiera operar. Creemos que los responsables de este proyecto olvidaron lo más importante y es que la construcción de una base de datos de este tipo requiere, como ya vimos, de consagración legal porque, como ya dijimos, en Colombia los datos biométricos se consideran datos sensibles por la Ley de Protección de Datos[63] y su tratamiento pasa por la autorización explícita y la imposibilidad de entregarlos a terceros sin autorización.

Bajo la premisa de que la tecnología puede resolver todos los problemas sociales de manera fácil y a bajo costo, se implementan soluciones sin hacer un diagnóstico serio de los problemas que se quieren resolver, ni de formas de resolverlos que puedan ser más eficientes y respetuosas de nuestros derechos. Por lo tanto, más allá de suponer que este tipo de sistemas es necesario para la seguridad de todas las personas, hay preguntas que quedan abiertas sobre la existencia, efectividad, manejo, gestión y utilización de bases de datos de identificación biométrica en el país.

De este análisis, quedan una serie de preguntas abiertas.

Si vamos a seguir adoptando medidas de este tipo (porque la moda es invertir en tecnología y justificar inversiones millonarias), por lo menos deberíamos evaluar antes su posible efectividad. ¿Con qué criterios se plantean estos proyectos? ¿Cuándo son efectivos y cuándo no? ¿Hay estudios o indicadores que nos permitan evaluar estas propuestas frente a otras alternativas?

¿Hasta qué punto es legal que el sistema de transporte masivo de una ciudad o cualquier otro, recabe la información biométrica de millones de personas? Los principios de necesidad, idoneidad y proporcionalidad de una medida de este tipo deberían ser parte fundamental de un análisis de impacto en derechos humanos, el cual tendría que hacerse antes de plantearse la creación de este tipo de iniciativas y debería hacerse público, para el conocimiento de cualquiera.

63 Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Teniendo en cuenta que las bases de datos están fuertemente reguladas y mucho más aquellas que contienen información personal sensible, como lo es todo dato biométrico, ¿sobre quién recaen las responsabilidades de formular y evaluar los riesgos para la intimidad que plantea la creación de estas bases de datos?

¿Tiene sentido gastar miles de millones de pesos en sistemas que no operen como debe ser, que no tiene los controles adecuados o que nos ponen en más riesgo? ¿Acaso el remedio, así, no es peor que la enfermedad?

Finalmente, aunque para algunas personas la presente investigación puede tener el limitante de que no se conocen la totalidad de los documentos que debieron servir de soporte para el diseño de este proyecto, precisamente partimos de la base de que la legitimidad y legalidad del mismo solo es posible evaluarse con base en los documentos públicos, con fundamento en lo que cualquier persona pueda saber de la iniciativa.

¿Tiene sentido gastar miles de millones de pesos en sistemas que no operen como debe ser, que no tiene los controles adecuados o que nos ponen en más riesgo? ¿Acaso el remedio, así, no es peor que la enfermedad?

Un informe de

Fundación
Karisma

Con el apoyo de

PRIVACY
INTERNATIONAL