

VIGILAR AL VIGILANTE: TRANSPARENCIA  
Y RENDICIÓN DE CUENTAS SOBRE LAS TECNOLOGÍAS  
DE VIGILANCIA PÚBLICA EN MÉXICO  
SOUSVEILLANCE, SURVEILLING THE SURVEILLERS:  
TRANSPARENCY AND ACCOUNTABILITY ON PUBLIC  
SURVEILLANCE TECHNOLOGIES IN MEXICO



*Lucía Carmina JASSO LÓPEZ\**

RESUMEN. El presente artículo tiene como objetivo analizar la transparencia y la rendición de cuentas sobre las tecnologías de vigilancia pública que instalan y gestionan los gobiernos locales y federal en México. A partir del análisis cualitativo, se estudian las expectativas y necesidades de transparencia que la ciudadanía ha manifestado a través de las solicitudes en el Sistema de Acceso a la Información y que pueden ser consultadas en la Plataforma Nacional de Transparencia. En total se sistematizaron y analizaron 2,264 solicitudes, que se registraron del 2008 al 2021. Estas expectativas de transparencia de la ciudadanía se contrastan con la información pública disponible en los portales de las instituciones públicas, para probar la hipótesis de investigación que sustenta que existe una brecha entre las expectativas y necesidades sociales de transparencia en la materia y la rendición de cuentas de las autoridades que ejercen vigilancia con el uso de tecnologías, y que además ésta no responde a los derechos fundamentales que potencialmente se vulneran con este tipo de dispositivos.

PALABRAS CLAVE. Transparencia, acceso a la información, rendición de cuentas, tecnologías de vigilancia, derechos fundamentales.

---

\* Doctora en Políticas Públicas. Investigadora en el Instituto de Investigaciones Sociales de la UNAM. Correo electrónico: [carmina.jasso@sociales.unam.mx](mailto:carmina.jasso@sociales.unam.mx).

Fecha de recepción: 11 de febrero de 2022.

Fecha de dictamen: 17 de mayo de 2022.

LUCÍA CARMINA JASSO LÓPEZ

32



**ABSTRACT.** *This article aims to analyze the transparency and accountability of public surveillance technologies installed and managed by local and federal governments in Mexico. Based on the qualitative analysis, the transparency expectations that citizens have expressed through requests in the Information Access System and that can be consulted in the Plataforma Nacional de Transparencia are studied. In total, 2,264 applications were systematized and analyzed, which were registered from 2008 to 2021. These expectations of citizen transparency are contrasted with the public information available on the portals of public institutions, to test the research hypothesis that supports that there is a gap between the social needs for transparency in the matter and the accountability of the authorities that exercise surveillance with the use of technologies, and that this also does not respond to the fundamental rights that are potentially violated with this type of device.*

**KEYWORDS.** *Transparency, access to information, accountability, surveillance technologies, fundamental rights.*

## I. INTRODUCCIÓN

La noción de “vigilar al vigilante” parte de la propuesta de *sousveillance* o “vigilancia desde abajo” de Mann, Nolan y Wellman (2003), quienes afirman que es fundamental vigilar a quienes poseen la autoridad y los medios para vigilar. En específico, el concepto de *sousveillance* se refiere como complementario a la vigilancia, e incluso se ha referido como un neologismo que no necesariamente debería usarse en el análisis académico (Thomsen, 2019). Sin embargo, es un concepto que se usa respecto a la vigilancia u observación de distintas actividades principalmente con dispositivos particulares, como los teléfonos inteligentes que cuentan con sus propias cámaras, con el fin de vigilar a quienes vigilan, como a la policía en manifestaciones sociales o en operativos, a las autoridades, entre otros.

En esta investigación, la *sousveillance* se propone desde la perspectiva de la transparencia y la rendición de cuentas que, en gran medida, se han constituido como una forma de limitar el control social que ejerce la autoridad. En específico, tiene como objetivo analizar la rendición de cuentas de las autoridades que gestionan y operan las tecnologías de vigilancia pública en México, así como se orienta al estudio de las expectativas y necesidades de transparencia de la sociedad que se manifiestan en las solicitudes de información, vía el

Sistema de Acceso a la Información. Lo que se busca es hacer un balance que permita comprender la relación entre la información disponible a través de las distintas formas de rendición de cuentas y las necesidades sociales de transparencia manifiestas, además de que se enuncian algunas recomendaciones de política pública que se consideran pertinentes.

Las preguntas que guían esta investigación son tres: 1) ¿cuáles son las expectativas y necesidades sociales de transparencia sobre las tecnologías de vigilancia?; 2) ¿cuál es la información pública disponible en la materia?; y 3) ¿cuál es la relación entre las expectativas y necesidades sociales y la información pública disponible?

Se plantea como hipótesis que las expectativas y necesidades sociales de transparencia en la materia están muy distantes de la rendición de cuentas de las autoridades que ejercen vigilancia con el uso de tecnologías, y que no son acordes a los derechos fundamentales que potencialmente se vulneran con este tipo de dispositivos, como los derechos a la privacidad, a la protección de datos personales, a no ser discriminado, entre otros.

Este análisis comprende que la vigilancia “se refiere a la recopilación de información acerca de un objetivo” (Thomsen, 2019: 705), y con el uso de las tecnologías puede llegar a hacerlo de manera sistemática y exhaustiva y sin la presencia *in situ* del vigilante. Se puede observar al objetivo remotamente desde un centro de control o, incluso, desde un teléfono inteligente u otro dispositivo que esté conectado a cientos de kilómetros de distancia. Las posibilidades de vigilancia con el uso de tecnologías son amplias y cada vez más innovadoras y sofisticadas (Zuboff, 2020).

El hecho de que las tecnologías permitan vigilar sin estar en el mismo lugar que el objetivo genera la incapacidad de reciprocidad de la mirada, donde el vigilado no puede observar al que vigila (Jasso, 2021). En este sentido, podríamos decir que en la vigilancia pública hay relaciones de poder en las que regularmente la sociedad se encuentra en desventaja frente a los gobiernos que disponen de las tecnologías de vigilancia para observar extensivamente a las personas (Thomsen, 2019: 706 y 707), ver lo que hacen o no hacen, e incluso el acontecer de la vida privada, que ineludiblemente también ocurre en el espacio público.

Sin embargo, esta vigilancia se construye “no sólo como un proceso unidireccional en el que prevalece la mirada de los vigilantes sobre los vigilados sino también como un proceso sujeto a dinámicas multivalentes, abiertas y contingentes de producción, uso e interpretación” (Arteaga, 2018: 9). Entre éstas se encuentran las demandas sociales para que el uso y gestión de las tecnologías de vigilancia por parte de las instituciones públicas se transparente y se rindan cuentas.



LUCÍA CARMINA JASSO LÓPEZ

34



En las siguientes páginas se analizan la transparencia y la rendición de cuentas sobre las tecnologías de vigilancia pública en México. En la primera parte se expone el marco teórico y conceptual enfocado a la argumentación de por qué rendir cuentas y transparentar sobre estas tecnologías. Posteriormente, se presentan los resultados de la investigación, enlistando, en primera instancia, las que se han considerado buenas prácticas o prácticas relevantes en materia de transparencia y rendición de cuentas, y, después, se examinan las solicitudes de información en la materia consultadas en la sección de Datos Abiertos de Solicitudes de Información de la Plataforma Nacional de Transparencia (en adelante, PNT), con el objetivo de conocer las expectativas y necesidades sociales de transparencia en la materia. Finalmente, se discuten los resultados y se presentan las conclusiones y recomendaciones de política pública.

## II. LA TRANSPARENCIA Y LA RENDICIÓN DE CUENTAS SOBRE LAS TECNOLOGÍAS DE VIGILANCIA PÚBLICA

En torno a la transparencia y la rendición de cuentas, hay un relativo consenso en cuanto a las dificultades que existen para lograr “los cambios institucionales, los procedimientos y las prácticas”, así como generar “la transformación organizacional y cultural profunda” (Cejudo *et al.*, 2014), que hagan posible el acceso a este derecho. En particular, cuando se trata de instituciones de seguridad y justicia —que también están sujetas al marco legal de transparencia y rendición de cuentas— cuyas lógicas apuntan más a la secrecía y la discrecionalidad (Jasso, 2017), estas dificultades se agudizan.

Sin embargo, la transparencia y la rendición de cuentas se consideran parte esencial de un gobierno democrático e, incluso, se espera un impacto positivo en las gestiones y en las políticas públicas (Cejudo *et al.*, 2014), por lo que se han convertido en prácticas aceptadas, aun en aquellas instituciones donde las inercias y la cultura organizacional van en sentido contrario.

En términos sociales, también hay un reconocimiento de la relevancia de la transparencia y la rendición de cuentas, aun cuando son pocas personas las que ejercen y acceden a este derecho; es una narrativa socialmente aceptada y compartida.

Existen diferentes razones por las que la transparencia y la rendición de cuentas sobre las tecnologías de vigilancia pública son fundamentales para las sociedades contemporáneas. Por una parte, su importancia se debe al despliegue incremental en el territorio en prácticamente todas las ciudades del mundo, en las que, a través de cámaras, drones y otros dispositivos tecnológicos, los gobiernos pueden vigilar lugares públicos e, incluso, observar el acontecer

de la vida privada de las personas en el espacio público. Como afirma Zuboff (2020), estamos inmersos en la era del “capitalismo de la vigilancia”.

También su trascendencia es debido a que tienen efectos en la sociedad y potencialmente vulneran derechos fundamentales, como los derechos a la privacidad, a no ser discriminado, al libre tránsito, a la protección de datos personales, entre otros. Estos temas han sido abordados en la literatura sobre tecnologías de vigilancia que, entre otros aspectos, han develado que éstas vigilan con mayor prevalencia a “grupos socialmente descreditados” (Smith, 2004), que comparten datos con otras fuentes de análisis (Zuboff, 2020) y que atentan contra la privacidad de las personas.

Asimismo, la transparencia y la rendición de cuentas son relevantes por cuestiones mucho más pragmáticas. La adquisición y gestión de estas tecnologías puede llegar a ser onerosa y regularmente se realiza con recursos públicos que podrían destinarse a otras acciones públicas, por lo que la transparencia—cuando menos de los costos, las formas de adquisición y otros tópicos que no vulneren la seguridad del Estado— debería ser una consecuencia inmediata. Al respecto, tenemos la amenaza latente de la corrupción, particularmente en la fase de adquisición de bienes o servicios con empresas privadas, que es donde aparecen asuntos como “sobrecostos en adquisición y mantenimiento, adjudicaciones directas injustificadas, fraude, entre otros” (Chipuli, 2019: 10), y también se ha encontrado evidencia de la “presión de proveedores” que, “con frecuencia, buscan vender equipos que no corresponden con las necesidades” (Vizcaíno, 2021: 19).

Quienes tienen el control de las tecnologías de vigilancia, además de proveer el servicio de prevención del delito, investigación de las violencias e incidencia delictiva, pueden ejercer distintas formas de control social, así como pueden incurrir en prácticas distópicas o discriminatorias (Abu-Laban, 2015). Al respecto, hay evidencia de que estas tecnologías se pueden usar para monitorear a ciertos grupos “rebeldes” (Smith, 2004: 378).

Con la vigilancia se genera una cantidad enorme de datos e información, y mucha de ésta se utiliza para “mejorar productos o servicios”, como podría ser la prevención del delito, la regulación del tránsito vehicular, entre otros temas sociales. Pero también “se fabrican productos predictivos que prevén lo que cualquiera de ustedes hará ahora, en breve y más adelante” (Zuboff, 2020: 21). Esta situación se agudiza con las cada vez más innovadoras formas de las tecnologías de vigilancia, que se interconectan a otras fuentes de información masiva, como las redes sociales, o los motores de búsqueda de información o productos, como Google o Amazon.

En este sentido, el papel de la sociedad como contrapeso y límite es imprescindible, aunque paradójicamente parte de la sociedad se ha vuelto insensible a la videovigilancia (Jasso, 2021). Pero también hay personas, grupos y



LUCÍA CARMINA JASSO LÓPEZ

organizaciones que se mantienen alerta sobre los riesgos de las tecnologías de vigilancia en la sociedad y se organizan para realizar acciones al respecto. Como argumenta Arteaga (2018):

...la videovigilancia impone lógicas de control de la población, y cómo los actores ubicados en una posición de subordinación resisten, pugnan y cuestionan dichas lógicas, y a veces son capaces de producir lazos de solidaridad a través de procesos propios de vigilancia, autovigilancia y contravigilancia, incluso mediante la apropiación de los sistemas que operan bajo el control de entidades públicas y privadas (Arteaga, 2018: 16).

36

●  
○  
● En el mundo han surgido discursos críticos, principalmente, por la vulneración a la privacidad, e incluso algunos son apoyados por organismos independientes. En Reino Unido, organizaciones como Privacy International, Liberty, entre otras, han acompañado temas sobre la regulación de la vigilancia, y “les preocupa en gran medida la eliminación de la privacidad, la naturaleza insidiosa de las cámaras, y la amenaza general a las libertades civiles y los derechos humanos” (Smith, 2004: 380). Inclusive, han surgido grupos más extremos que convocan a la destrucción de las tecnologías de vigilancia.

En Europa, destaca que la transparencia y la rendición de cuentas en la materia fueron consideradas como parte de los siete principios fundacionales —que son complementarios entre sí— de la “Carta para el uso democrático de la vigilancia por video”, que se elaboró en el Foro Europeo para la Seguridad Urbana (FESU, 2010). En la Carta se sostiene la necesidad de la transparencia, que garantice “una política clara y transparente en cuanto al funcionamiento de su sistema”; de la legalidad, que refiere que los sistemas de videovigilancia deberán apegarse y cumplir con la ley; de la responsabilidad, que atañe el derecho de vigilancia del espacio público a las autoridades que son responsables de estos sistemas, y de la supervisión independiente, que consiste en los “frenos y contrapesos al funcionamiento de los sistemas de vigilancia por video que deben aplicarse a través de un proceso de control independiente” (FESU, 2010).

En torno al derecho a la protección de datos personales, una constante de las tecnologías de vigilancia son los datos que sistemáticamente éstas recopilan en los espacios públicos, e incluso de actividades privadas que ineludiblemente también ocurren de manera cotidiana en el ámbito público. Actividades, rostros, rutas, entre otros tantos datos, son compilados y están al escrutinio de quienes gestionan estas tecnologías.

Este tema ha llegado a ser polémico, y aunque se han generado marcos normativos en torno a la vigilancia en algunos ámbitos —por ejemplo, en los centros de trabajo se usan estas tecnologías para fiscalizar a los empleados—, generalmente el uso de estos dispositivos se considera una violación al derecho a la intimidad y a la protección de datos personales, así como “una im-

portante intromisión en su vida privada” (Taléns, 2018: 62). Esto es aún más cuestionable cuando se trata de la vigilancia en espacios públicos.

En América Latina también hay evidencia de estos discursos críticos. Algunos de ellos se construyen desde las instituciones, como el Centro de Protección de Datos Personales y la Defensoría del Pueblo de Buenos Aires, que en 2018 organizó el conversatorio titulado “Tecnologías de vigilancia en Argentina. Alcances, implementación y viabilidad de estas tecnologías para la prevención del delito y la protección de los derechos humanos” (Defensoría del Pueblo, 2018). Otros más se hacen desde otras trincheras, como el arte o la misma tecnología, pero apelando al balance entre la vigilancia y los derechos humanos.

En este contexto, la transparencia y la rendición de cuentas se configuran como una forma de control a las autoridades públicas que ejercen el poder de vigilar con distintos dispositivos tecnológicos. Coincido en que se trata de “un principio democrático que apela en última instancia a establecer mecanismos para vigilar a los que vigilan” (Arteaga, 2016: 224).

37



### III. METODOLOGÍA

La metodología de investigación es principalmente cualitativa y se fundamenta en el análisis documental de las solicitudes de información y sus respectivas respuestas disponibles al 4 de enero de 2022 en la PNT (<https://www.plataformadetransparencia.org.mx/>). En la sección de Datos Abiertos de Solicitudes de Información se consultó la palabra “videovigilancia” y en total el sistema encontró 2,264 solicitudes del 2008 al 2021 y 509 solamente en 2021, que principalmente muestran información sobre cámaras de videovigilancia, pero también de drones y de centros de control, cómputo y comando (C4 o C5), así como otros dispositivos auxiliares o complementarios.

Del 2008 al 2021 se analizó con estadística descriptiva las frecuencias de las variables: año de registro, entidad de registro, institución a la que se dirigió la solicitud y tipo de respuesta. Este análisis longitudinal permite conocer las características generales de las solicitudes de información en un periodo de catorce años. Por su parte, las solicitudes registradas en 2021 se revisaron con mayor profundidad y se analizó su contenido para conocer los requerimientos de información y las respuestas a las mismas.

Respecto a las solicitudes de 2021, es pertinente señalar que, como ocurre en otros casos, hay peticionarios que registran la misma solicitud, incluso con la misma redacción, y la dirigen a distintas instituciones, por lo que algunas de éstas se repetían decenas de veces cuando, por ejemplo, eran enviadas a las instituciones homologas de todas las entidades federativas o de los municipios de un estado. En este caso, se priorizó en analizar la solicitud para co-

LUCÍA CARMINA JASSO LÓPEZ

nocer la demanda de información y se revisaron tres distintas respuestas para explorar cómo responden las diferentes instituciones, aunque la comparación de las respuestas no se considera el centro de esta investigación.

38 Sobre la metodología de revisión y el análisis de solicitudes de acceso a la información, es relevante señalar que hay una larga lista de estudios empíricos que han recurrido a este análisis, como el de Fox, Haight y Palmer, que se enfoca, entre otros aspectos, en “evaluar tanto la completud como la calidad de las respuestas de los organismos a las solicitudes de información pública” (2011: 9). Asimismo, tenemos el trabajo de Filipini y Selwood (2021), donde se estudian “casos difíciles” en el acceso a la información, o el de Jasso (2021), que analiza las solicitudes de información sobre inteligencia militar.

● Además, a partir de la revisión de las páginas de Internet y de los portales de transparencia de los gobiernos locales y del gobierno federal, se realizó la búsqueda de información pública disponible que pudiera considerarse como una práctica relevante de rendición de cuentas. Respecto a esta parte de la investigación, se reconoce que puede ser más limitada que el análisis sistemático de solicitudes de acceso a la información, ya que en gran parte se fundamenta en la agenda propia de investigación y los hallazgos en la materia durante los últimos años. Sin embargo, se considera que es relevante porque aporta referencias para contrastar con las expectativas y necesidades sociales de transparencia.

#### IV. LA RENDICIÓN DE CUENTAS

Paulatinamente, la rendición de cuentas sobre las tecnologías de vigilancia pública en México se ha incrementado. No obstante, es pertinente decir que ha tenido algunos retrocesos, pues se ha dejado de actualizar información o, incluso, se ha eliminado información que ya era pública. En las siguientes páginas se presenta un listado abreviado de ciertas prácticas que se han considerado relevantes en materia de transparencia y rendición de cuentas, así como algunos de los retrocesos identificados.

Al respecto, es imprescindible señalar que en México “las leyes en la materia obligan a los sujetos obligados a poner en Internet un conjunto de datos relacionados con el ejercicio de los recursos públicos y otros aspectos vinculados a la gestión, programas, trámites y servicios” (Cejudo *et al.*, 2014). Así, los gobiernos de los distintos órdenes han creado espacios virtuales para compartir datos por temas y, en específico, las instituciones cuentan con unidades de transparencia que publicitan la información, según les corresponda, para la consulta de la sociedad.

En cuanto a las tecnologías de vigilancia, a nivel nacional destaca el Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales, que se nutre de los datos proporcionados por los gobiernos estatales, y nos permite saber que en 2019 se contaba con 99,912 cámaras de vigilancia en vía pública; 41 centros de control, comando, cómputo, comunicaciones y coordinación (C5); 85 centros de control, comando, cómputo y comunicaciones (C4), y 93,308 botones de pánico (INEGI, 2020). Sin embargo, en esta información hay algunos vacíos, como el caso de Coahuila, que “reportó no contar con el tipo de infraestructura” al INEGI, cuando en distintos medios de comunicación existe evidencia de que sí cuentan con estas tecnologías.

Asimismo, en el Censo Nacional de Gobiernos Municipales y Demarcaciones Territoriales de la Ciudad de México se contabilizan las tecnologías de vigilancia que administran y gestionan en ese orden de gobierno. Hasta 2019 se reportaba la presencia de 34,491 cámaras de vigilancia y 340,196 botones de pánico (INEGI, 2019a).

Si bien los censos del INEGI permiten conocer los datos absolutos sobre las tecnologías de vigilancia de las demarcaciones que reportan desde hace varios años, hay más información que resulta relevante para la sociedad.

Entre las prácticas relevantes que transparentan la información sobre las tecnologías de vigilancia pública, podemos destacar las del gobierno de la Ciudad de México. Este gobierno, además de ser pionero en la implementación de sistemas de videovigilancia a nivel nacional e incluso regional y contar con el mayor despliegue de estas tecnologías en el territorio, también ha sobresalido por la información que ha publicitado.

En el Portal de Datos Abiertos de la CDMX era posible consultar la ubicación de cada una de las cámaras de videovigilancia pública; sin embargo, a la fecha de consulta (7 de enero de 2022) esta información ya no está disponible. Algo similar ocurrió en Morelos, donde la organización no gubernamental Morelos Rinde Cuentas refirió que “En 2020 la información sobre el estado de las cámaras de video vigilancia sí era información pública para la Comisión Estatal de Seguridad Pública. En 2021 ya no. Es información reservada” (Díaz, 2021).

En el caso de la Ciudad de México, desde enero de 2021 se difundieron los datos del programa “Mi Calle”, que consiste en la instalación de tótems en los domicilios de 333 colonias determinadas como prioritarias, en donde se incluyen cámaras de videovigilancia, alertas (sonoras y visuales) y botones de auxilio (ADIP, 2022). Asimismo, está disponible la ubicación del Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano (C5) y de los centros de comando y control (C2) de la Ciudad de México.

De igual forma, el Portal de Datos Abiertos de la CDMX publicita la ubicación de los dispositivos del Programa de Fotomultas, que de 2015 a 2018



LUCÍA CARMINA JASSO LÓPEZ

dispuso cámaras y radares para el control de velocidad y otras faltas administrativas. Posteriormente, este programa se denominó Fotocívicas. Desde el punto de vista de Thomsen, esta vigilancia es del tipo “moralmente bueno”, porque el propósito de las cámaras de tráfico móviles es crear una amenaza disuasoria contra la velocidad, suponiendo plausiblemente que los límites de velocidad benefician a la sociedad (2019: 710).

40 Sobre la gestión y los resultados de las tecnologías de vigilancia, el Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano de la Ciudad de México (C5) integró como parte de su política de transparencia a los reportes estadísticos, que contenían datos sobre “incidentes captados por cámara, botón, radio y llamada al 911 en la Ciudad de México”. Estos reportes se publicaban trimestralmente y se elaboró un reporte anual del 2010 al 2017; sin embargo, posterior a este año, tales reportes ya no están disponibles para la consulta de la ciudadanía.

En cuanto al uso de los recursos, los anexos técnicos de los fondos y subsidios federales han publicitado cada año el desglose de los recursos públicos convenidos con los estados y municipios, y entre ellos están los destinados a las tecnologías de vigilancia, como cámaras de video, centros de control, cámaras de solapa, entre otras. Asimismo, durante algunos años, estos datos se sistematizaron para su consulta en el Mecanismo de Evaluación y Transparencia de Recursos Federales (MET) del SESNSP, y es posible saber que de 2016 a 2020 se destinaron 10,667 millones de pesos para videovigilancia en los estados y municipios (Vizcaíno, 2021: 22).

En los estados también hay algunas prácticas interesantes. Por ejemplo, el Aviso de Privacidad del Sistema de Videovigilancia Urbana del Estado de México promueve el carácter obligatorio o facultativo de la entrega de los datos personales y refiere a la sociedad: “Si usted se percata de que se obtuvo una imagen suya que no desea que sea difundida, por favor, solicítele directamente que la elimine, en su defecto, acuda ante la Unidad de Transparencia, indicando la fecha y lugar del evento” (Gobierno del Estado de México, 2018).

Igualmente, en 2020 se realizó en el Estado de México una audiencia pública en el C5, a la que asistieron distintos representantes de la sociedad civil, empresarios, instituciones educativas, organizaciones vecinales y académicos. En el periódico *El Universal* (2020) se convocó a “todos los habitantes del Estado de México” para asistir al C5 “donde se monitorean las cámaras de videovigilancia, para dar recomendaciones a los operadores sobre cómo podrían mejorar el funcionamiento”.

Asimismo, es de destacar la labor de los institutos estatales y el nacional de transparencia que han atendido los recursos de revisión de la ciudadanía, dando acceso a la información sobre tecnologías de vigilancia. Esto es fundamental, porque muchas veces existen resistencias por parte de las autoridades

para negar, simular u omitir la información que debería ser pública, debido a que “una de las falacias con las que se sataniza la transparencia desde los centros de poder es que con ello se reivindica una cierta voluntad panóptica que puede fácilmente derivar en totalitaria, cuando en la práctica ocurre lo contrario” (Díaz y Talens, 2013: 71).

## V. LAS SOLICITUDES DE INFORMACIÓN

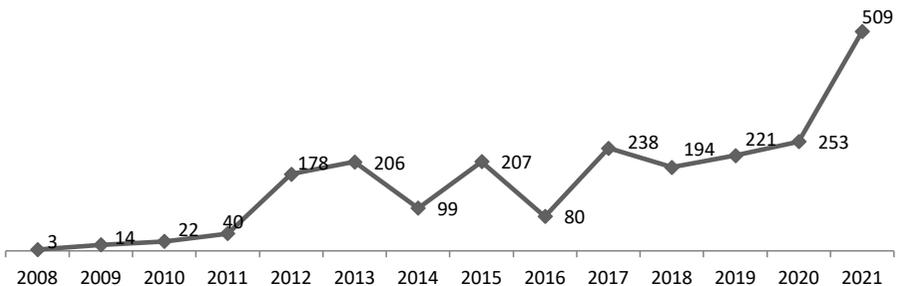
41

Se comprende que el acceso a la información es un “derecho humano comprendido en la libertad de expresión que reconoce la prerrogativa de la persona a informarse sobre asuntos públicos” (Filipini y Selwood, 2021: 63). Las solicitudes de información son una forma de acceder a este derecho humano y en México es posible consultarlas desde la PNT, que se define como la “Plataforma electrónica que permite cumplir con los procedimientos, obligaciones y disposiciones establecidas en las leyes en materia de transparencia, atendiendo a las necesidades de accesibilidad de los usuarios”.

En la PNT se registraron 2,264 solicitudes de información del 2008 al 2021 sobre tecnologías de vigilancia. ¿Esto es mucho o poco? Considerando que en 2019 se recibieron a nivel nacional 102,044 solicitudes de acceso a la información (INEGI, 2021) y que las correspondientes a tecnologías de vigilancia en ese mismo año son 221, éstas representan apenas el 0.21%, lo cual es un porcentaje bajo.

Sin embargo, en el tiempo, se observa una tendencia de crecimiento respecto a éstas, particularmente en los últimos cinco años (2017-2021), donde se concentra el 62.5% de las solicitudes en la materia (gráfica 1). Probablemente, esta tendencia se mantendrá en los siguientes años ante el incremento de estas tecnologías en las ciudades.

GRÁFICA I. SOLICITUDES DE INFORMACIÓN  
SOBRE TECNOLOGÍAS DE VIGILANCIA EN MÉXICO 2008-2021



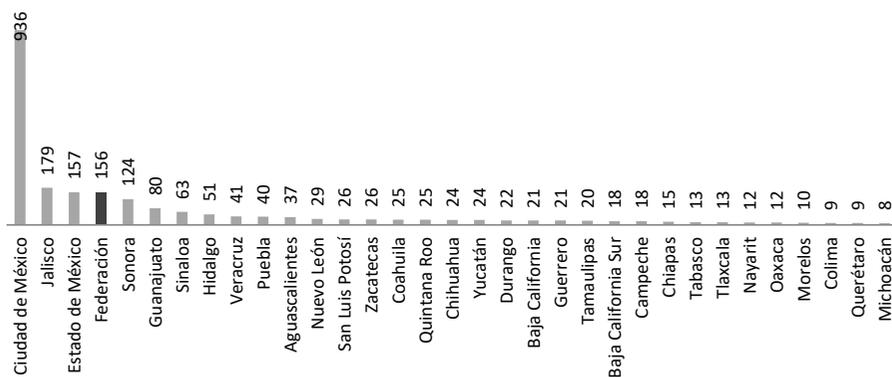
FUENTE: elaboración propia con datos de la Plataforma Nacional de Transparencia.

LUCÍA CARMINA JASSO LÓPEZ

Las primeras solicitudes de información fueron registradas en 2008, lo que coincide con la instalación de los primeros sistemas de videovigilancia pública en México con el Proyecto Bicentenario “Ciudad Segura” en el entonces Distrito Federal. En este tenor, resulta interesante señalar que la mayor parte de las solicitudes se realizaron en la Ciudad de México con 41.3% y, además, 241 solicitudes (10.6%) se dirigieron directamente al Centro de Comando, Control, Cómputo, Comunicaciones y Contacto Ciudadano de la Ciudad de México (C5CDMX), que es la institución responsable de la gestión de la vigilancia pública en la ciudad.

Después de la Ciudad de México, el mayor número de solicitudes de información se realizaron en Jalisco y Estado de México, donde también coincide que son las entidades federativas en las que se concentra el mayor número de tecnologías de vigilancia pública declaradas por los respectivos gobiernos estatales (INEGI, 2020). En cuarto lugar, las solicitudes se dirigieron hacia la Federación (gráfica 2).

GRÁFICA 2. SOLICITUDES DE INFORMACIÓN  
 SOBRE TECNOLOGÍAS DE VIGILANCIA EN MÉXICO,  
 POR ENTIDAD FEDERATIVA Y LA FEDERACIÓN (2008-2021)



FUENTE: elaboración propia con datos de la Plataforma Nacional de Transparencia.

En la mayor parte de las entidades federativas, las solicitudes de información sobre tecnologías de vigilancia no han sido tan relevantes. En efecto, en más de la mitad de las entidades federativas se han recibido menos de veinticinco solicitudes, y en estados como Colima, Querétaro y Michoacán se han registrado menos de una decena en el periodo. Particularmente, nos llama la atención que en entidades como Nuevo León, donde la ciudad de Monterrey o San Pedro Garza García también cuentan con sistemas de videovigilancia

públicos con gran despliegue en el territorio, éste no sea un tema de interés de la ciudadanía; de esta manera, en la consulta realizada únicamente se registraron veintinueve solicitudes en esta entidad.

Sobre las dependencias hacia las que se dirigen las solicitudes, después del C5 de la CDMX, al que se dirigieron una de cada diez solicitudes, le siguen cuatro instituciones del gobierno de la Ciudad de México: la Secretaría de Seguridad Ciudadana (163), el Sistema de Transporte Colectivo (44), la Secretaría de Obras y Servicios (29), y la Jefatura de Gobierno de la Ciudad de México (25). Posteriormente, se enlistan los ayuntamientos de Guadalajara (25) y Zapopan (23) en Jalisco y, a su vez, la Fiscalía estatal (21) de esa misma entidad.

En cuanto al tipo de respuesta, sobresale que en 625 solicitudes se entregó la información vía Infomex; en 236 casos se notificó que la solicitud correspondía a otro ente, y en 111 se entregó la información por un medio electrónico. Por otro lado, en 37 solicitudes se estableció la incompetencia del sujeto obligado; en diecinueve se refirió al acceso restringido en modalidad confidencial o reservada, y en diez casos se determinó una negativa por tratarse de información reservada o confidencial.

Respecto a la información que se declaró confidencial o reservada, diez correspondieron a la Federación. En varios de los casos se solicitó información sobre los arcos detectores de metales, las cámaras de videovigilancia, las bandas de rayos X y los aparatos de rayos gamma con que contaban instituciones públicas, como el Consejo de la Judicatura de la Federación (Folio 0320000153921), la Secretaría de Turismo (Folio 0002100034713), la Secretaría de Educación Pública (Folio 0001100290513), la Secretaría de Energía (Folio 0001800034813), la Secretaría de Agricultura (Folio 0000800071313) y la Secretaría de Gobernación (Folio 0000400169313).

Aunque la persona solicitante no requirió la ubicación, sino sólo el número, las respectivas dependencias determinaron la reserva y confidencialidad de la información. Incluso, se argumentó que

...podría ocasionarse un menoscabo en los procedimientos de seguridad llevados a cabo en las instalaciones del edificio... como la infraestructura... para garantizar la seguridad de las personas que en ella laboran, así como de la gente que ingresa al edificio diariamente, máxime que se corre el riesgo del mal uso que pudiera darse a la información, con lo que se pondrían en peligro vidas humanas, recursos materiales y, en consecuencia, la seguridad de las personas (Folio 0001800034813).

En este tenor, también destaca la negativa de información respecto a la solicitud de información de los contratos en materia de videovigilancia. De



LUCÍA CARMINA JASSO LÓPEZ

manera específica, un par de solicitudes requirieron información sobre el Servicio de Videovigilancia Administrada Integral VIVA-I, que presuntamente se instaló en el Servicio de Administración Tributaria (SAT), y también solicitaban los nombres de las empresas subcontratadas por el licitante ganador Six-sigma Networks México, S. A. de C. V. (Folio 0610100086709).

44 En las entidades federativas sobresale un conjunto de trece solicitudes de información realizadas al gobierno de Guanajuato y a distintos gobiernos municipales. La solicitud requería datos sobre el estado de fuerza e infraestructura para la seguridad pública y, en específico, consultaba sobre el “total de cámaras de videovigilancia conectadas al C4 o C5 de seguridad”.

● Asimismo, en otra solicitud al gobierno de Guanajuato se le consultó sobre el Programa Escudo de Videovigilancia (Folio 01407716), y al peticionario se le notificó que el Programa se encuentra clasificado por cinco años y se le compartió el Acuerdo de Clasificación,<sup>1</sup> en el que se argumenta que

...hacer pública la información de las especificaciones y características inherentes a la realización de acciones en materia de seguridad pública puede afectar a ésta de manera importante, inclusive alertar a la delincuencia organizada... restándole eficacia al actuar del gobierno en detrimento de la seguridad pública (Gobierno del Estado de Guanajuato, 2016: 5 y 6).

Una solicitud similar se realizó al C5 de Jalisco, al cual se le preguntó acerca del Escudo Urbano C5 (Folio 01318821); pero en este caso se entregó la información sobre el número de cámaras instaladas en once municipios, que en total suman 6,340.

Con relación a los tipos de solicitudes de información y con el objetivo de responder a las preguntas sobre ¿qué información solicita la ciudadanía respecto a las tecnologías de vigilancia en México?, ¿cuáles son las expectativas sociales de transparencia?, se trabajó con las solicitudes presentadas en 2021, las cuales ascienden a 509, y se elaboró una tipología de la información solicitada en la materia.

El tipo de solicitud más común es aquella orientada a saber si existen o no tecnologías de vigilancia en instituciones o espacios específicos, como en los municipios; en instalaciones concretas, como los vagones de los trenes

---

<sup>1</sup> El Acuerdo de Clasificación refiere que “el proyecto va dirigido a los 46 municipios del Estado de Guanajuato. Está compuesto por áreas vertebrales para su operación: las cámaras de video-vigilancia urbana, el blindaje de fronteras y carreteras con arcos detectores, la identificación vehicular por radiofrecuencia, el sistema de radiocomunicación y el sistema de inteligencia de emergencias 066 y 089. Toda esa tecnología estará en conexión con un moderno C-4, Centro de Comunicaciones, Cómputo, Control y Comando” (Gobierno del Estado de Guanajuato, 2016).

del Sistema de Transporte Colectivo Metro en la Ciudad de México (Folio 00453521), o en instalaciones estratégicas, como la solicitud de la ubicación de las cámaras en el Centro de Reinserción Social para Varones El Llano, Aguascalientes<sup>2</sup> (Folio 00195821).

También están las solicitudes que piden conocer los costos de adquisición e implementación de las tecnologías de vigilancia. Esto es relevante, porque, como refieren Filipini y Selwood, el acceso a la información es “un derecho que asiste a la lucha contra la corrupción” (2021: 67). Por ejemplo, destaca una petición a la Secretaría de Seguridad Pública de Quintana Roo, a quien se le solicitó información sobre el gasto de mantenimiento de las cámaras de videovigilancia (Folio 00017121).

Otras más solicitan los contratos para la adquisición u operación de las tecnologías de vigilancia pública. En algunos casos hasta especifican los nombres de las empresas con las que se realizaron los contratos, como la solicitud que pedía la “versión pública del contrato celebrado entre el Gobierno de la Ciudad de México y las empresas Thales, Telmex y Cisco para la modernización del sistema de videovigilancia e implementación de herramientas de inteligencia artificial” (Folio 0303100035319). En este caso, la persona peticionaria se fundamentó en una nota periodística, y aunque se le entregó respuesta vía Infomex, la respuesta refiere que el gobierno “no ha celebrado contratos” con las empresas en referencia.

También son recurrentes las solicitudes sobre los distintos tipos de tecnologías de vigilancia. En Yucatán, un peticionario solicitó información a la Secretaría General de Gobierno acerca de la existencia del “sistema, software o tecnología para el reconocimiento facial”, y en el caso de que existiera, aquél solicitaba conocer el objetivo de éste y “si es utilizado en espacios públicos”,<sup>3</sup> así como requería la información sobre proveedores, monto del contrato, etcétera (Folio 00453521). A esta solicitud se le respondió que la información es inexistente, y así ocurrió también en otras entidades y dependencias a las que se remitió la misma solicitud.

En este tenor, también destacan las solicitudes realizadas al municipio de Santiago, Nuevo León, respecto a las “cámaras de solapa recibidas o compradas” y “en uso”, así como la fuente y el monto del financiamiento (Folio 191116621000018). Como respuesta, se estableció que se trataba de “información reservada y, por lo tanto, no [era] susceptible para su entrega”. Asimismo, sobresale la solicitud de contratos por parte del gobierno de Guanajuato

<sup>2</sup> En la respuesta se señala que proporcionar esta información “representa un riesgo real”, “toda vez que de darse a conocer se pudiera incurrir en graves riesgos que pueden culminar en la fuga masiva de internos, procesados o sentenciados”.

<sup>3</sup> Esta solicitud se envió con la misma redacción a los 32 gobiernos estatales.



LUCÍA CARMINA JASSO LÓPEZ

para “la adquisición de drones o aeronaves no tripuladas destinadas para la videovigilancia aérea” (Folio 00591121).

46 En otros casos, las solicitudes piden información más específica sobre la infraestructura de las tecnologías de vigilancia, como los tipos de fibras e hilos, la arquitectura de la red, los nodos de conmutación, las antenas, los repetidores, las bandejas de empalme, etcétera; además, solicitan información respecto a los usuarios públicos de la red y la capacidad utilizada (Folio 232579700001521). Este tipo de solicitudes muestran el conocimiento por parte de los peticionarios, que esperan información muy específica y especializada.

● En particular, una solicitud de información requirió al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública conocer “sobre la aprobación y/o solicitud, oficio relacionado con el proyecto de ampliación de las videocámaras de vigilancia y geolocalización en el municipio de Macuspana, Tabasco” (Folio 2210300006721). En respuesta, el Secretariado Ejecutivo envió los oficios correspondientes en los que el presidente municipal solicitaba la validación del proyecto, argumentando que “fue prevalidado por el titular del centro de mando y comunicaciones del Estado de Tabasco”, así como el dictamen FORTASEG 2020 procedente, en el que se emite la opinión técnica y validación por parte del Centro Nacional de Información. Este tipo de solicitud podría relacionarse con la contraloría ciudadana para garantizar que las tecnologías de vigilancia pública cuenten con el aval o autorización correspondiente.

Los peticionarios también utilizan el acceso a la información pública para conocer sobre la instalación de tecnologías de vigilancia privadas. En la Ciudad de México se le consultó a la Secretaría de la Contraloría General lo siguiente: “si para instalar un circuito cerrado de videovigilancia y usar los postes públicos y el suministro de alumbrado público para que se alimenten las cámaras se necesitan permisos y ante quién se tienen que tramitar” (Folio 090161821000505). En este caso, la consulta no era de la competencia de la Secretaría y —probablemente, en consecuencia— el peticionario solicitó la información a otras dependencias, incluyendo el C5.

De igual forma, en la Ciudad de México se le consultó al C5 respecto al “proceso o trámite” para “entregar videos que son captados por las cámaras de videovigilancia instaladas en la ciudad”. Una persona peticionaria solicitó una explicación “de manera clara y en lenguaje sencillo”, y pidió los oficios o formatos que se deben utilizar tanto por un particular como por el Ministerio Público (Folio 0303100041021). Este tipo de solicitud muestra que existen necesidades sobre una cuestión fundamental, que es el acceso a los videos cuando una persona es víctima de un delito o violencia, y que además se re-

quiere que esta información sea clara y sencilla para evitar la impunidad y la posible revictimización.

En esta misma lógica, es de interés de la ciudadanía conocer sobre la grabación de imágenes de cámaras específicas, probablemente con relación a un hecho en concreto. Por ejemplo, se le solicitó la grabación al Instituto Mexicano del Seguro Social (IMSS) de una cámara ubicada en la sede delegacional en San José, Puebla, especificando el día y el rango de horario (Folio 330018021005543). Ante esta solicitud se respondió que “la información requerida pone en riesgo y vulnera el derecho a la privacidad” y, por lo tanto, es confidencial. Solicitudes similares se realizaron a otras instituciones sobre cámaras identificadas en días y horarios específicos.

47



## VI. DISCUSIÓN

Ineludiblemente, hay información “susceptible de lesionar otros derechos también fundamentales o intereses estatales legítimos, tales como la seguridad pública” (Filipini y Selwood, 2021: 63) o la seguridad nacional. En este sentido, la Ley General de Transparencia y Acceso a la Información Pública (2015) refiere que la información “podrá ser clasificada excepcionalmente como reservada de forma temporal por razones de interés público y seguridad nacional o bien, como confidencial”.

Desde luego, en la información relativa a las tecnologías de vigilancia pública existe aquella que puede vulnerar la seguridad pública nacional y, por lo tanto, se clasifica como reservada o confidencial. Tal es el caso de instalaciones estratégicas o de seguridad, como los centros de reinserción social, que están sujetos a una constante vigilancia y donde la revelación de su ubicación, infraestructura o características de las tecnologías vulneraría la seguridad de las instituciones y de la sociedad.

Sin embargo, hay información que debidamente sistematizada sí podría ser publicitada para consulta abierta de la sociedad. Por ejemplo, la ubicación de las cámaras de videovigilancia que se han instalado en la vía pública, que incluso bajo la premisa de la prevención situacional del delito, podría contribuir a disuadir la violencia y las incivildades en sus áreas de influencia. En contraparte, esta información no se encuentra disponible para todas las entidades federativas o municipios que en su mayoría han decidido instalar este tipo de dispositivos. Incluso, en la Ciudad de México ya se contaba con esta información y fue retirada del Portal de Datos, lo cual representa un retroceso importante en materia de rendición de cuentas.

También está la información relativa a la adquisición de estas tecnologías, tanto sobre la forma de adquisición —licitación, invitación restringida o adju-

LUCÍA CARMINA JASSO LÓPEZ

dicación directa— como con lo relacionado a los proveedores, que en algunos casos presionan a las autoridades (Vizcaíno, 2021) o pueden representar prácticas monopólicas. Desde luego, es fundamental que la ciudadanía conozca los costos y las formas de adquisición, porque generalmente este tipo de dispositivos se adquieren con recursos públicos.

48 Respecto a la información disponible, es decir, la que es pública en los portales de transparencia y la que se comparte a través de las solicitudes de información, hay varios aspectos a discutir. El primero de ellos está relacionado a la siguiente falacia: “los datos son públicos, de manera que siempre es posible comprobar su veracidad” (Díaz y Talens, 2013: 59). En principio, no todos los datos públicos son asequibles para toda la población, pues algunos requieren *expertise* tanto para encontrarlos como para comprenderlos, y aún más para analizarlos y verificarlos. Como lo refiere el 48.4% de los mexicanos, “obtener la información gubernamental es difícil o muy difícil” (INEGI, 2019b).

En cuanto a las solicitudes de información, el que estén disponibles para su consulta en la PNT hace asequible comprender diversos aspectos sobre las expectativas de la sociedad respecto a distintos temas, entre ellos las tecnologías de vigilancia pública que, si bien no son de los principales intereses de la ciudadanía, sí resultan relevantes para algunos.

Se advierte que, aunque se le responda a los peticionarios y se les entregue información vía Infomex, es recurrente que se argumente que la información es inexistente,<sup>4</sup> replicando los resultados de estudios en la materia que se realizaron desde los primeros años de implementación del Sistema de Acceso a la Información y que encontraron la tendencia hacia la negativa oficial de la “existencia” de la información solicitada, lo que, desde el punto de vista de las personas expertas, “deja mayor espacio a la opacidad” (Fox *et al.*, 2011: 19).

Hay varias solicitudes que se replican y fueron enviadas a distintos entes. Es probable que los peticionarios sean proveedores de servicios, personas periodistas o investigadores académicos que recurren a esta fuente de información. A nivel nacional se ha observado que sólo el 3.6% de la población realiza solicitudes de información (INEGI, 2019b), lo cual refleja un sector muy específico de la población y que probablemente se focalice aún más en el caso de personas peticionarias de información sobre tecnologías de vigilancia.<sup>5</sup>

<sup>4</sup> En la solicitud 0002700035920 se respondió lo siguiente: “después de realizar una búsqueda exhaustiva dentro de sus archivos físicos y electrónicos con los que cuenta, no se localizó registro alguno de que la Secretaría de la Función Pública haya formalizado contratos marco para la contratación de servicios de seguridad y/o en materia de videovigilancia, o seguridad tecnológica, por lo que dicha información es inexistente”.

<sup>5</sup> A nivel nacional, el 4.4% de los peticionarios usó la información recibida para “compartir o difundir” (INEGI, 2019b). Esto podría coincidir con los reportajes y artículos periodísticos sobre tecnología de vigilancia que recurren a las solicitudes de información.

No en todos los casos es posible consultar los documentos directamente desde la plataforma, y al intentarlo aparece la leyenda “Para los archivos no disponibles, consulta al organismo de transparencia correspondiente”. Esto particularmente ocurre con las solicitudes dirigidas al C5 de la CDMX, que es la principal dependencia a nivel nacional hacia la que se dirigieron las solicitudes.

Llama mucho la atención que prácticamente no hay solicitudes de información sobre los operadores de las tecnologías de vigilancia; es decir, sobre el “elemento humano” (Smith, 2004) que cotidianamente observa a la sociedad y que, como se ha demostrado en investigaciones empíricas, pueden incurrir en prácticas no adecuadas, como usar las cámaras para fines informales y no oficiales, e incluso voyeristas (Abu-Laban, 2015) o discriminatorias (Smith, 2004; Arteaga, 2018).

49

La demanda por la transparencia y la rendición de cuentas sobre las tecnologías de vigilancia públicas en México ha incrementado, pero no así la oferta por parte de los sujetos obligados. Por una parte, se han registrado retrocesos con el desfase de la información que se deja de actualizar, e incluso se ha eliminado información que ya era pública, como se documentó para los casos de la Ciudad de México y Morelos. En este contexto, la transparencia y la rendición de cuentas han sido intermitentes.

Esta cuestión no ha sido homogénea. Entre entidades federativas y municipios existen diferencias entre la información que deciden publicitar, así como en la manera en que contestan las solicitudes de información que les realiza la ciudadanía. Lo mismo ocurre entre las dependencias de una misma administración, que responden de manera diferenciada a solicitudes de información similares.

Tampoco ha sido lineal e incremental. En el tiempo, se identifican rupturas en las que la información que se publicaba y actualizaba periódicamente deja de hacerse. En algunos casos, ello obedece a los tiempos administrativos, pues al cambiar un gobierno o un titular de la dependencia se modifican las formas de transparentar y rendir cuentas; sin embargo, también hay cambios que obedecen a otras coyunturas distintas.

## VII. CONCLUSIONES

Es fundamental evaluar el nivel y la calidad de la transparencia y la rendición de cuentas de fenómenos sociales como la implementación y gestión de las tecnologías de vigilancia pública, que se han incrementado notoriamente en

LUCÍA CARMINA JASSO LÓPEZ

las ciudades y que generan efectos sociales en el espacio público y en la sociedad que es observada.

En el caso mexicano, se ha observado que existe una brecha entre las expectativas y necesidades de transparencia de la sociedad y la información que es publicitada por parte de las autoridades que implementan y gestionan estas tecnologías. En el tiempo, esta brecha se ha exacerbado con la información que deja de actualizarse o que se ha retirado cuando ya era pública; así, lo que se encontró en esta investigación fue la presencia de retrocesos o estancamientos en la materia.

50 Sin embargo, las expectativas y necesidades de información por parte de la ciudadanía sobre estos temas han incrementado en el tiempo y es previsible que continúen en aumento, lo que deberá impactar en una mayor rendición de cuentas por parte de las autoridades para responder a esta demanda social, que llevarán a cabo mediante ejercicios de transparencia activa que difundan aspectos que no vulneren la seguridad pública o la nacional, así como otros derechos fundamentales. Entre éstos se consideran relevantes actualizar de manera permanente el número de dispositivos de vigilancia pública que se adquieren y se instalan en el espacio público, conocer los costos y formas de adquisición o contratación, así como transparentar de la manera más clara y sencilla la forma en la que los ciudadanos pueden acceder a estos videos cuando son víctimas de un delito o violencia. Es preciso que la ciudadanía tenga más información para “vigilar al vigilante” y proteger sus derechos fundamentales a la privacidad, a no ser discriminado y a la protección de datos personales.

Para ello, se debe mirar hacia los avances registrados en otras latitudes, como los principios fundacionales de la Carta para el uso democrático de la vigilancia por video, que se elaboró en el Foro Europeo para la Seguridad Urbana y en la cual se suscribe la importancia de la transparencia y la rendición de cuentas de las tecnologías de vigilancia pública.

Asimismo, se deben generar oportunidades y espacios para el debate público, como se documentó en Buenos Aires a través del conversatorio sobre estas tecnologías y su impacto en la sociedad y el ejercicio de los derechos fundamentales.

La agenda de investigación futura es amplia y, en particular, se deberá profundizar en la calidad de las respuestas a las solicitudes atendiendo preguntas clásicas como “¿Con cuánta frecuencia las solicitudes ciudadanas de información reciben la respuesta que están buscando?” (Fox *et al.*, 2011: 6), que se han planteado en otras investigaciones. Igualmente, es necesario comparar las prácticas de transparencia y rendición de cuentas en la materia en otros países.

## VIII. FUENTES DE INFORMACIÓN

- ABU-LABAN, Yasmeen, 2015, "Gendering Surveillance Studies: The Empirical and Normative Promise of Feminist Methodology", *Surveillance & Society*.
- AGENCIA DIGITAL DE INNOVACIÓN PÚBLICA (ADIP), 2022, "Portal de Datos", disponible en: <https://datos.cdmx.gob.mx/>.
- ARTEAGA, Nelson, 2016, "Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad", *Espiral. Estudios sobre Estado y Sociedad*, vol. 23, núm. 66.
- ARTEAGA, Nelson, 2018, *Videovigilancia en México: protesta política, conflicto y orden social*, Flacso-México.
- CEJUDO, Guillermo *et al.* (eds.), 2014, *La política de transparencia en México: instituciones, logros y desafíos*, México, CIDE.
- CHIPULI, Arturo, 2019, "Videovigilancia y corrupción: una relación ambivalente", *VI Simposio Internacional LAVITS 2019*, Brasil.
- DEFENSORÍA DEL PUEBLO, 2018, *Debate sobre tecnologías de vigilancia*, Argentina, Defensoría del Pueblo.
- DÍAZ, Omar, 2021, "Oculta gobierno de Morelos funcionalidad de cámaras de seguridad", *Publimetro*, México, disponible en: <https://www.publimetro.com.mx/noticias/2021/10/14/oculta-gobierno-de-morelos-funcionalidad-de-camaras-de-seguridad/>.
- DÍAZ, Susana y TALENS, Jenaro, 2013, "WikiLeaks, o de la sobreinformación como desinformación", en DÍAZ, Susana y LOZANO, Jorge (eds.), *Vigilados. WikiLeaks o las nuevas fronteras de la información*, Madrid, Nueva Era.
- El Universal*, 2020, "Dan acceso público al C5 del Edomex", 16 de febrero, disponible en: <https://www.eluniversal.com.mx/metropoli/dan-acceso-publico-al-c5-del-edomex>.
- FILIPINI, Jorge Alejandro y SELWOOD, Inés, 2021, "Las obligaciones de transparencia en las políticas públicas: los casos difíciles", *Revista de Estudios en Derecho a la Información*, núm. 12.
- FORO EUROPEO PARA LA SEGURIDAD URBANA (FESU), 2010, "Carta para el uso democrático de la vigilancia por video", París-Barcelona, Foro Europeo para la Seguridad Urbana.
- FOX, Jonathan *et al.*, 2011, "Proporcionar transparencia: ¿hasta qué punto responde el gobierno mexicano a las solicitudes de información pública?", *Gestión y Política Pública*, vol. 20, núm. 1.



LUCÍA CARMINA JASSO LÓPEZ

- GARCÍA, Myrna, 2008, *Derecho de las nuevas tecnologías*, México, UNAM, Instituto de Investigaciones Jurídicas.
- GOBIERNO DEL ESTADO DE GUANAJUATO, 2016, “Acuerdo de Clasificación del Proyecto Escudo”, México, Gobierno del Estado de Guanajuato.
- GOBIERNO DEL ESTADO DE MÉXICO, 2018, “Aviso de Privacidad del Sistema de Videovigilancia Urbana del Estado de México”, disponible en: <https://sseguridad.edomex.gob.mx/sites/sseguridad.edomex.gob.mx/files/files/Aviso%20de%20privacidad%20sistema%20de%20videovigilancia%20urbana.pdf>.
- 52
- INEGI, 2019a, *Censo Nacional de Gobiernos Municipales y Demarcaciones Territoriales de la Ciudad de México 2019. Tabulados básicos*, México, INEGI.
  - 
  -
- INEGI, 2019b, *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales (ENAIID) 2019*, México, INEGI.
- INEGI, 2020, *Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2020*, México, INEGI.
- INEGI, 2021, *Censo Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales 2021*, México, INEGI.
- JASSO, Carmina, 2017, “Seguridad nacional, inteligencia militar y acceso a la información en México”, *URVIO. Revista Latinoamericana de Estudios de Seguridad*, núm. 21.
- JASSO, Carmina, 2021, “(In)Sensibilities to the Vigilance of Others in the City”, en SCRIBANO, A. *et al.* (eds.), *Cities, Capitalism and the Politics of Sensibilities*, Cham, Palgrave Macmillan.
- Ley General de Transparencia y Acceso a la Información Pública, 2015, *Diario Oficial de la Federación*, 4 de mayo, disponible en: [http://www.dof.gob.mx/nota\\_detalle.php?codigo=5391143&fecha=04/05/2015](http://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015).
- MANN, Steve *et al.*, 2003, “Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments”, *Surveillance & Society*, vol. 1, núm. 3.
- SMITH, Gavin J. D., 2004, “Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK”, *Surveillance & Society*.
- TALÉNS, Eduardo, 2018, “Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros”, *Relaciones Laborales y Derecho del Empleo*, vol. 6, núm. 3.
- THOMSEN, Frej Klem, 2019, “The Concepts of Surveillance and Sousveillance: A Critical Analysis”, *Social Science Information*.

- VIZCAÍNO, Álvaro, 2021, “Videovigilancia e inteligencia artificial: entre la utopía y la distopía”, *Revista Mexicana de Ciencias Penales*, vol. 4, núm. 14.
- ZUBOFF, Shoshana, 2020, *La era del capitalismo de la vigilancia. La lucha por un futuro humano frente a las nuevas fronteras del poder*, trad. de Albino Santos, Barcelona, Paidós-Planeta.

