VI SIMPÓSIO INTERNACIONAL LAVITS 2019 >>>> SALVADOR

ASSIMETRIAS E (IN)VISIBILIDADES: VIGILÂNCIA, GÊNERO E RAÇA
ASIMETRÍAS Y (IN)VISIBILIDADES: VIGILANCIA, GÉNERO Y RAZA
ASYMMETRIES AND (IN) VISIBILITIES: SURVEILLANCE, GENDER AND RACE

Ojos humanos, cámaras digitales, sueños algorítmicos. El ensamblado local de *vigilantes electrónicos* en la ciudad de Ensenada

MARTIN JAVIER URTASUN[1]

Resumen

La implementación de sistemas de videovigilancia – y su estudio por parte de las ciencias sociales – son fenómenos consolidados a nivel mundial, aunque en América Latina el compromiso de las ciencias sociales con el tema pareciera estar menos desarrollado (ARTEAGA BOTELLO, 2012). En este sentido, una de las limitaciones en la literatura actual es la escasez de estudios situados que aborden en profundidad la complejidad de las tramas locales entre humanos y máquinas que conforman a los *vigilantes electrónicos.* El presente trabajo se propone realizar un aporte a la apertura de estas "cajas negras", desde una etnografía del Centro de Operaciones Municipales (COM) de la ciudad de Ensenada, Argentina. Abordaremos esta tarea desde una pregunta específica por aquellos componentes tecnológicos, "no humanos", del sistema. Para ello se apelará a una sociología pragmática de las innovaciones tecnológicas y su dimensión como formas materiales de estabilizar relaciones de poder, en la reconstrucción de algunas tensiones atravesadas durante la implementación del sistema. Con estas herramientas indagaremos en los elementos de software del sistema, particularmente en la construcción de bases de datos, el uso de algoritmos y el rol de los expertos informáticos que actúan como sus portavoces. Nos interesa particularmente visibilizar cómo se piensa el rol de los algoritmos en la videovigilancia, desde una ciudad pequeña cuyo sistema aún se basa fundamentalmente en una vigilancia "analógica", a cargo de operadores/as de cámara. Para quienes dirigen el COM, la automatización de la vigilancia se abre como un interrogante futuro, a veces como un sueño, otras como una pesadilla. Intentaremos finalmente entablar un diálogo con la bibliografía disponible sobre el tema, buscando que nuestros informantes, sus prácticas y perspectivas, ingresen como interlocutores.

Palabras clave: videovigilancia; etnografía; algoritmos; vigilantes electrónicos.

Videovigilancia, agenciamientos, etnografías

La implementación de sistemas de videovigilancia – y su estudio académico – son fenómenos consolidados a nivel mundial, aunque el compromiso de las ciencias sociales latinoamericanas con el tema parece estar menos desarrollado que los *surveillance studies* del mundo anglosajón y son muchas las aristas que aún quedan por explorar (ARTEAGA BOTELLO, 2012). En trabajos previos en la construcción de estados del arte pudimos identificar una línea de estudios incipiente, aunque

1 Licenciado y Profesor en Sociología (FaHCE, UNLP). Estudiante del Doctorado en Ciencias Sociales (FaHCE, UNLP). Becario doctoral del CONICET. Integrante del Núdeo de Estudios sobre Seguridad en Provincia de Buenos Aires (NESBA, IdIHCS, CONICET-UNLP). Correo electrónico: martinjurtasun@gmail.com

prometedora, centrada en la pregunta por la vigilancia como tarea cotidiana URTASUN, 2014; LÍO y URTASUN, 2015). Sea por la movilización de supuestos teóricos sobre su el carácter técnico o automático de la vigilancia, sea por dificultades metodológicas para llevar adelante estudios empíricos, se suele obviar la existencia de "trabajadores/as de la vigilancia" o simplificar en exceso la labor que realizan (SMITH, 2012). Frente a esta situación, los y las etnógrafos/as de la videovigilancia apuestan a un contacto más directo con el ámbito de estudio y al ingreso de teorías nativas en diálogo con las elaboraciones académicas, visibilizando los límites de un "determinismo tecnológico" que subestima la importancia del "factor humano": aquellas personas cuyo trabajo es observar las imágenes y operar el sistema (NORRIS Y ARMSTRONG, 1999; SMITH, 2004). Reformulando la misma crítica en clave de la "teoría del actor-red", Bruno Cardoso se refiere a la necesidad de superar la "sobredeterminación técnica" para desplegar las redes de agenciamientos sociotécnicos propias de lo que él llama "*vigilantes electrónicos*": ensamblajes heterogéneos de máquinas y seres humanos que hacen posible a la videovigilancia (CARDOSO, 2010 y 2011). En sus distintas formulaciones, los distintos estudios coinciden en el llamado a abrir las "cajas negras" para describir qué y quiénes las componen, cómo se relacionan, qué tensiones existen (o existieron) y cómo se las intenta estabilizar.

¿Qué implica adoptar la idea de "abrir la caja negra" para el caso de un sistema de videovigilancia? Se trata, en primer lugar, de detener la aplicación esquemática de grandes "explicaciones sociales" para dar lugar a un esfuerzo minucioso por producir descripciones y análisis situados (LATOUR, 2008). Por más que la atraviesen discursos, racionalidades y mercados de escala mundial, cada sistema de videovigilancia se despliega en un territorio particular, ensamblando elementos heterogéneos y respondiendo a distintos desafíos. El presente trabajo constituye un aporte al conocimiento empírico de las formas concretas en las que se organiza la videovigilancia en América Latina, desarrollando interrogantes construidos desde una investigación etnográfica en curso en el Centro de Operaciones Municipales (COM) de la ciudad de Ensenada, Argentina[2]. En pleno auge y difusión del uso de algoritmos y sistemas de *machine learning* aplicados a la videovigilancia, este interés por los y las trabajadores/as podría parecer un contrasentido. ¿Sigue siendo relevante el factor humano, en la era del reconocimiento facial? Abordaremos esta pregunta desde un estudio de caso sobre las formas en que se reelaboran los componentes "humanos" y "no humanos" del

2 Con algo más de 50.000 habitantes, Ensenada es una ciudad pequeña ubicada en la zona sur del Área Metropolitana de Buenos Aires. Se caracteriza por su actividad portuaria y un fuerte perfil industrial, así como por su historia política ligada a la fuerza de las organizaciones obreras, el movimiento peronista y la presencia represiva de la Armada Argentina.

sistema. Para ello apelaremos al concepto de "programa de acción" propuesto por Bruno Latour en la reconstrucción de las transformaciones ocurridas durante la implementación del novedoso sistema de cámaras, hace casi una década. Luego emprenderemos una serie de exploraciones en los elementos de software del sistema, particularmente en la construcción de bases de datos y el uso de algoritmos. Titulamos "exploraciones" a esta sección, ya que nuestros informantes parecen situar la agencia de los algoritmos en un futuro, como un sueño posible, entre el deseo y la pesadilla.

El COM: la videovigilancia como programa de acción

> "La dominación no es nunca un capital que pueda ser almacenado en un banco. Debe ser desplegado, cajanegrizado, reparado, mantenido" (LATOUR, 1998: 126)

En su clásico artículo "La tecnología es la sociedad hecha para que dure" Latour afirma que para comprender mejor las raíces y fundamentos de la dominación es necesario hacer un lugar para los actantes no humanos que toman parte activa de las relaciones sociales (LATOUR, 1998). El autor rechaza la movilización de conceptos clásicos de la sociología crítica, como "poder" o "dominación", en tanto forma de "explicar" los fenómenos sociales que observamos: más bien, estos son productos posibles de las formas en que distintos actantes se relacionan, alineándose o no en torno a distintos objetivos. El poder y la dominación nunca están asegurados: dependen de la movilización de actantes humanos y no humanos en pos de un cierto "programa de acción", y su realización depende de una constante tarea de asociación: cada elemento nuevo "carga" con su materialidad al programa, volviéndolo más duradero, más previsible, más real. A la vez, su incorporación no es una mera suma, sino una "traducción" que modifica en parte al resto de los elementos y al programa de acción en su conjunto. Para ganar realidad, un programa de acción debe intentar "cajanegrizarse", volver oscuras o autoevidentes aquellas asociaciones en las que se apoya, enfrentando a la vez los posibles "antiprogramas" que intentarán desarticularlo. Nuestra tarea será, por lo tanto, describir las redes en torno a estos programas de acción, desplegando sus tramas de asociaciones sociotécnicas sin esquemas impuestos como las ideas de "trayectoria", "contexto", "escala local-global" o "temporalidad cronológica".

La propuesta teórica y metodológica de Latour, originada en el ámbito de la sociología de las ciencias y las técnicas, es un aporte valioso para reformular los estudios sociales sobre dispositivos sociotécnicos complejos como los sistemas videovigilancia. Muchas veces naturalizadas como "cámaras de *seguridad*", herramientas supuestamente necesarias y efectivas en la lucha contra el

delito, las videovigilancia estatal de espacios públicos puede ser descripta hoy en día como una caja negra. ¿Cómo se volvieron las cámaras un "punto de paso obligado" para dar respuesta al problema de la "inseguridad", tal como fue construido en Argentina durante las últimas dos décadas? (KESSLER, 2009). La explicación más corriente, al menos para los municipios de la provincia de Buenos Aires, dice lo siguiente: los gobiernos locales fueron presionados "desde arriba" por instancias provinciales y nacionales, así como "desde abajo" por los y las vecinos/as (potenciales votantes) a tomar cartas en un asunto tradicionalmente fuera de su responsabilidad, como la seguridad; sin jurisdicción para crear policías propias, se recostaron en políticas de "prevención situacional" buscando dar un mensaje claro de involucramiento y compromiso, a la vez que una imagen de modernidad y eficiencia vinculada a una solución tecnológica (SOZZO, 2009). A esto se le suma la disponibilidad de fondos nacionales en el marco del Plan Integral de Protección Ciudadana, que fomentaba la inversión municipal en tecnologías securitarias como cámaras y dispositivos GPS para los patrulleros, lo que explica por qué buena parte de los municipios bonaerenses crearon sus "secretarías de seguridad", instalaron cámaras y "Centros de Operaciones Municipales" en el año 2010 (GALVANI, RÍOS Y CAÑAVERAL, 2015). Se trata, por otro lado, de un proceso similar al experimentado en el resto de América Latina en el que se avanzó en la "municipalización de la seguridad" de la mano de una asociación supuestamente virtuosa entre el gobierno local y los dispositivos "preventivos" (DAMMERT, 2007).

A primera vista, el caso de Ensenada entra dentro del relato: la Secretaría de Seguridad y Justicia se crea en el año 2009 y el COM se inaugura un año después, con algo más de 50 cámaras compradas con fondos nacionales. Sin embargo, un acercamiento etnográfico permite detectar muchos actantes que no aparecen en el relato anterior, o lo hacen de un modo demasiado esquemático que no da cuenta del proceso para nada lineal de intentos de traducción y resistencias. Partiendo desde el punto de vista del Municipio, las cámaras adquirieron una serie de significados muy variados: fueron una compra que había que licitar, una inversión que había que hacer rendir políticamente, una herramienta para la prevención y el control del delito en la ciudad, algo que respondía (o creaba) demandas por parte de los y las vecinas, etc. En cada una de estas direcciones podemos encontrar "programas de acción" en los que las cámaras cumplen el papel de "cargar" de materialidad cierta pretensión por parte del municipio de establecer alianzas y gobernar las conductas. Programas que pueden ser resistidos o contestados de múltiples formas: los "malvivientes" pueden evadir las cámaras desplazándose hacia zonas no vigiladas, romperlas a piedrazos, o simplemente ignorarlas y seguir realizando sus actividades como si nada; los y las vecinos/as pueden no impresionarse

favorablemente por la novedad, sentirse vigilados/as o creer que no funcionan, o bien quejarse porque su esquina aún no tiene una cámara asignada; la policía puede considerar la videovigilancia como un intento ilegítimo de control sobre su accionar, o desestimar el valor de una alerta producida por un/a civil que no está en el lugar del hecho y no responder a los pedidos del COM; abogados/as, peritos/as y jueces/as pueden considerar las imágenes como insuficientes o ilegítimas como material de prueba en una instancia judicial. Hasta las propias cámaras pueden dejar de funcionar, negarse a responder a los comandos o a producir la calidad de imagen necesaria, fallar en la transmisión de los datos. La implementación de la videovigilancia tuvo que sortear de alguna manera todos estos "antiprogramas", impulsando mayores inversiones municipales en la materialidad del sistema: postes más altos, cámaras más robustas y de mejor definición, nuevos softwares, más fibra óptica.

Lo que este breve recuento muestra es la espesa trama de relaciones tejidas entre humanos y no humanos alrededor de la videovigilancia. Podemos ver que en esta red sólo un reducido conjunto de actantes pueden ser identificados como "el municipio", y que tanto dentro de esta categoría como fuera reinan la heterogeneidad, las traducciones y los desplazamientos. Como señalan Peter Miller y Nikolas Rose, las tecnologías de gobierno no se limitan al ámbito estatal, van más allá y más acá de lo definido como "político", convocando a distintas formas de poderes y saberes expertos en torno a racionalidades políticas (ROSE Y MILLER, 2012). En tanto sistema de inscripción y "centro de cálculo", el COM crea registros visuales del espacio público ensenadense que van más allá de la voluntad de poder municipal: modifican el comercio, el tendido de fibra óptica, los recorridos urbanos, la forma en que se gestionan incendios, emergencias médicas y accidentes de tránsito, las pruebas disponibles por parte de las aseguradoras, la forma periodística de narrar la ciudad. Como efecto de la ampliación de la cadena de traducciones que construye, el propio municipio como actor cambia: su materialidad ahora depende también de las empresas que venden software y hardware, técnicos que hacen el mantenimiento, "operadores/as de cámara" que trabajan vigilando al sistema, etc.

El grado de "cajanegrización" del COM responde, entonces, a la extensión de la cadena de asociaciones que unen a distintos actantes, operando a su vez en distintas escalas que van desde la opinión de los vecinos de tal o cual barrio al trabajo de programadores y desarrolladores que se materializa en los paquetes tecnológicos comprados en el mercado, y luego ensamblados por el personal de la secretaría. La videovigilancia en Ensenada ya no aparece explicada como efecto de cambios epocales, enmarcados en la "sociedad de riesgo", "de la información", "del control", la "postmodernidad", el neoliberalismo o alguna otra denominación genérica. No hace falta: hay una

trama de asociaciones que desplegar, procesos que describir y voces que recuperar para volver inteligible las formas situadas en que construye su realidad.

Exploraciones algorítmicas

Como en su momento las huellas dactilares, el telégrafo, el teléfono o el automóvil (REQUENA HIDALGO, 2004), la videovigilancia urbana es una innovación que transforma profundamente el campo del control del delito. El salto de las cintas analógicas a la digitalización permitió pasar de humildes circuitos cerrados en shoppings, bancos e instituciones securitarias, a la extensión de sistemas a escala urbana, reuniendo cientos de imágenes que pueden ser visualizadas en vivo, almacenadas y reproducidas a muy bajo costo. La digitalización implica entonces la articulación de toda una nueva serie de actantes, abre posibilidades, crea nuevos problemas, desplaza los puntos de paso obligados y convoca nuevos expertos al campo de la seguridad. Nos interesan dos actantes en particular: los y las expertos/as en informática y la programación de algoritmos de análisis de video (*video analytics)*.

El director del COM es un claro ejemplo de cómo la videovigilancia atrae a nuevas figuras al campo del control del delito. Aunque ahora está recibido como analista de sistemas, comenzó a trabajar para la Secretaría como estudiante, haciendo pequeños trabajos de mantenimiento de las computadoras. Cuando surgió la necesidad de hacer una licitación para adquirir las cámaras y todos los equipos necesarios para lanzar el sistema, la Secretaria le pidió ayuda. Desde entonces ha cumplido un rol fundamental en el desarrollo del sistema, traduciendo los problemas políticos y policiales en términos de fibra óptica, cámaras domo o fijas, servidores, software especializado y mapas del delito. Es él quien organiza el trabajo de los y las operadores/as de cámara, media entre el municipio y las empresas que venden tecnología y realizan el mantenimiento de las cámaras, programa distintas aplicaciones y vela por el funcionamiento general. Su incorporación trae una mirada distinta a la trama estatal en torno a la seguridad: un civil (no policía), que no viene de la gestión política y ni del derecho, sino de un saber técnico crucial para mantener los distintos elementos que conforman a la videovigilancia unidos entre sí y funcionando correctamente.

El segundo elemento, los algoritmos, puede ser menos fácil de apreciar en un primer acercamiento. Si algo caracteriza al actual despliegue de algoritmos en casi todas las esferas de la vida cotidiana es su capacidad para ocultarse de las miradas curiosas, revestirse de ficciones de objetividad y pasar desapercibidos. Como señala Cathy O'Neil, más allá de cómo los presenten las

empresas y autoridades que los utilizan, estas "armas de destrucción matemática" se basan siempre en modelos más o menos sesgados de interpretación de la información y pequeños errores pueden desatar grandes daños al sumarse la opacidad del funcionamiento y la operación en gran escala (O'NEIL, 2016). Lo cierto es que, como afirmaba en una entrevista el director del COM, "en el Centro de Monitoreo, hoy en día, todo depende de algoritmos: ya sea para guardar el video, donde analizan las imágenes, hoy en día todo tiene algoritmo". Pero no necesariamente se trata siempre de sistemas complejos capaces de desplegar grandes decisiones: la mayoría tienen aplicaciones sencillas que serían casi imperceptibles si no fuera porque él posee los conocimientos y habilidades necesarios como para identificarlos, transformarlos y en cierta medida, hablar por ellos.

¿Qué papel cumplen los algoritmos en la videovigilancia de Ensenada? Según nuestro informante, en el COM "no se toman decisiones mediante algoritmos". Con esto demarca las "decisiones" de otras formas de agencia presentes en algunas funciones básicas del software, como analizar la imagen producida para compensar el contraste y el brillo, o pasar del color al blanco y negro durante la noche. Estas funciones forman parte del software general, pero también son incorporadas en las propias cámaras, que cuentan con pequeños procesadores. Existen otras funciones más complejas y el director del COM admite que son útiles para tomar decisiones relevantes al sistema. Se trata de programas que él ha diseñado y que permiten crear bases de datos, visualizarlos y hacer análisis estadísticos, tanto de las llamadas de emergencia médica recibidas como de las denuncias policiales. Cruzando datos georeferenciados con categorías como tipo de hecho registrado, horario, tiempo de llegada del personal policial o médico, etc, estas bases le permiten explotar las posibilidades de la videovigilancia como aparato de inscripción, condensando y a la vez creando nuevas formas de conocer la situación de la ciudad.

Como señala Richard Wright en una breve reseña titulada "visualización de datos", el tamaño de ciertas bases de datos ha llevado al desarrollo de distintas técnicas de representación que permiten encontrar relaciones donde antes solo se percibía un mar de datos (WRIGHT, 2008). Los algoritmos que programan en el COM son un buen ejemplo de la capacidad de convencimiento que ejerce la visualización: sus "mapas del delito" brindan al municipio una herramienta para decidir dónde deberá ubicar nuevas cámaras o tender fibra óptica, por fuera de los métodos tradicionales como la consulta a las fuerzas policiales o el atendimiento de reclamos vecinales. En un proceso municipalización de la seguridad, en el que el gobierno local se suma a un campo dominado por las policías provinciales y nacionales, contar con un sistema de videovigilancia le ha permitido acceder a

las estadísticas policiales (cada denuncia está obligada a elaborar un "oficio" pidiendo al municipio las posibles imágenes captadas por las cámaras) y lograr así cierta autonomía que habilite el despliegue de iniciativas propias.

> Los algoritmos ya existen, pero no tenemos el resto de la información para poder aplicarlos (…) Nos falta desarrollarnos como país en el sentido de que esa información sea pública a todos los entes del estado. Si esa información se bajara al resto de los entes estatales, se podría hacer algo como lo que estamos planteando. Yo veo a alguien que tiene pedido de captura, por reconocimiento facial hoy en día una cámara lo puede hacer. No estamos lejos, no es algo súper complicado, ya existe el algoritmo que detecta una cara y la puede reconocer. (…) ¿Cuánto nos falta? Yo te digo, 15 o 20 años, no por lo técnico, sino de laburo como país" (Director del COM, entrevista personal, 26-12-2018).

Hay sin embargo un sentido en el que los algoritmos si podrían "tomar decisiones", o al menos realizar una parte más relevante del trabajo de vigilancia: las distintas formas de reconocimiento de imagen y análisis de video. Aunque no se utilicen todavía en el COM, el entrevistado deja en claro que los algoritmos están disponibles, incluso algunos de acceso abierto, y que los medios técnicos ya están a disposición. El reconocimiento de patentes, por ejemplo, está entre los objetivos más cercanos: requiere de unas cámaras especiales, capaces de enfocar muy rápido y captar muchas imágenes por segundo, pero no sería muy costoso incorporarlas. El principal problema, señala Juan, es la falta de acceso a bases de datos externas contra las cuales poder cotejar la información captada. ¿De qué sirve un reconocimiento facial, si no accedo a una base de datos personales en la que salte, por ejemplo, si la persona tiene un pedido de captura? Según nuestro informante los algoritmos solos no sirven sin los datos necesarios, algo en lo que "nos falta desarrollarnos como país, no como centro de monitoreo, o como municipio".

Vigilantes electrónicos **en busca del reconocimiento**

> "De acuerdo con el funcionario, la idea es 'que la tecnología ayude' a combatir el delito. Sin embargo, la presidenta de la Fundación Vía Libre y especialista en temas de derechos humanos en entornos tecnológicos, Beatriz Busaniche, afirmó que 'esto implica un avance sobre las garantías de protección de la intimidad que tienen los ciudadanos. La vida privada de las personas no solo incluyen su esfera domiciliaria sino también el espacio público', y advirtió, además, que este tipo de tecnología 'funciona mal y produce muchos falsos positivos'" (Nicolás Romero, "Otro juguete para papelones en seguridad", Página 12, 4-4-2019)3

> "El problema radica en que, en el afán de identificar a uno, nos identificarán a todos. No hay forma de que así no sea desde el momento que nuestra foto se encuentra en un pasaporte o documento nacional

3 Disponible online en: https://www.pagina12.com.ar/185084-otro-juguete-para-papelones-en-seguridad

> de identidad" (Nicolás Lucca, "Adiós a la privacidad otra vez: se viene el sistema de reconocimiento facial en las calles", *Infobae*, 4-4-2019)[4]
>
> "Surge, también, el tema de la protección de datos. '¿Quién va a cuidar la información? ¿Cómo vamos a asegurarnos que estos datos no van a ser filtrados?', se pregunta [Leandro Ucciferri]. Busaniche, en la misma sintonía, plantea: 'A cambio de costos en derechos fundamentales, se está creando una base de datos que es muy valiosa en el mercado'" (Sebastián Davidovsky, "El debate detrás del uso de las cámaras de seguridad para identificar personas", *La Nación,* 3-5-2019)[5]

Cuando realizamos la entrevista los algoritmos de reconocimiento facial tenían en Ensenada un grado de realidad muy bajo: apenas existían como un sueño futuro para el director del COM y nadie más hablaba de ellos. Unos meses después, contra toda predicción, el jefe de gobierno de la Ciudad Autónoma de Buenos Aires anunció la implementación, por primera vez en la capital argentina, de un programa de reconocimiento facial para detectar y detener prófugos con pedido judicial de captura mediante el sistema de videovigilancia ya instalado en espacios públicos y medios de transporte. Sin un tratamiento legislativo ni un debate público previo, la medida despertó una serie de cuestionamientos por parte de ciertos actores de la sociedad civil que lograron hacer escuchar su voz en los medios de comunicación. Como muestran los extractos escogidos de distintos diarios, incluyendo algunos francamente oficialistas, las críticas se formulan en términos de eficacia (falsos positivos), violación de derechos (privacidad), falta de proporcionalidad (vigilancia generalizada) y seguridad de los datos recabados. En tanto innovación, el uso de algoritmos de reconocimiento estaría enfrentando cierta resistencia por parte de "expertos" en tecnología, seguridad y derechos humanos, aunque sin llegar la controversia a frenar su implementación.

El uso de las llamadas "analíticas de video" y de algoritmos para el análisis de las imágenes de la videovigilancia, sea para identificar patentes, reconocimiento facial, detección de movimiento o de patrones inusuales, no es ninguna novedad. Su aplicación se remonta a fines de la década de 1990 en Estados Unidos y el Reino Unido, volviéndose especialmente visibles con la nueva oleada de endurecimiento de la "seguridad" y medidas de vigilancia post septiembre del 2001. Como señalara Mitchell Gray, en esta primer etapa la fuerte inversión y las posibles pérdidas de derechos se justificaron como un precio a pagar en la lucha contra el terrorismo (GRAY, 2003). Ya los primeros

4 Disponible online en: https://www.infobae.com/opinion/2019/04/04/adios-a-la-privacidad-otra-vez-se-viene-el-sistema-de-reconocimiento-facial-en-las-calles/

5 Disponible online en: https://www.lanacion.com.ar/tecnologia/el-debate-detras-del-uso-camaras-seguridad-nid2243734

estudios alertaron sin embargo sobre el desplazamiento hacia fines mucho más banales relacionados a la administración del espacio público y la represión de pequeñas incivilidades y delitos menores, en un típico caso de "surveillance creep", así como el preocupante hallazgo de una conjunción de baja eficacia, sesgos contra poblaciones específicas y alta capacidad de invisibilización (INTRONA Y WOOD, 2004). A pesar de las críticas, el uso de este tipo de analíticas de video no ha parado desde entonces, todo lo contrario: las nuevas capacidades de almacenamiento y procesamiento de datos han permitido elaborar algoritmos mucho más ambiciosos y sofisticados. Además del crecimiento en la cantidad y calidad de las cámaras en espacios públicos, se suman otros dispositivos (principalmente, smartphones equipados con cámaras digitales) y otros actores (usuarios/as de redes sociales y plataformas en las que se comparten imágenes), ampliando enormemente el volumen de las bases de datos disponibles (CRAMPTON, 2019). La biometría, y en particular el reconocimiento facial, se están volviendo cada vez más un dispositivo de uso cotidiano y masivo: desde el control de acceso y la venta de comida en las escuelas (TAYLOR, 2012) o el uso en animales (DONALDSON, 2012) hasta el caso de China, que con la articulación entre sus 400 millones de cámaras y sus detalladas bases de datos personales cuenta hoy en día con una de las herramientas más poderosas de control y gobierno de poblaciones (SIQUEIRA CASSIANO, 2019).

¿Cómo procesan estas tendencias globales los ensambles locales que conforman *vigilantes electrónicos* en el COM? Si dejamos por un momento de lado los discursos políticos y mediáticos de gran difusión e indagamos en el caso de Ensenada, podemos captar otras formas que adopta esta misma controversia. Durante nuestras últimas visitas a la sala de monitoreo propusimos, intencionalmente, una discusión sobre la novedad que llegaba a las ciudades vecinas. El resultado fue una serie de acaloradas discusiones que dejaron en claro la mezda de fascinación, miedo y escepticismo que produce la perspectiva de una vigilancia automatizada. Según afirmaba una policía de turno en el COM "en China con las cámaras hacen todo, está buenísimo, tienen toda la información; la tecnología nos va a superar, las cámaras se van a mover solas, van a encontrar delitos solas y listo". Junto a esta valoración positiva se repetía una constante sospecha respecto a las posibilidades de aplicación a nivel nacional. La idea de que probablemente no funcione tan bien como dicen quienes lo promocionan y que "no estamos preparados como país" se muestra como un consenso entre trabajadores/as de la videovigilancia. La impugnación se basa en las denuncias recientes sobre el alto número de falsos positivos producidos por el sistema en Buenos Aires, pero se ramifica en una crítica más profunda. Los y las policías resaltan que para el gasto que implica, el uso de este tipo de sistema no tiene sentido porque "el tema es que el hecho es dinámico, en general

nunca se quedan un rato mirando la cámara como para que puedan identificar. Igual, si te sale un pedido de captura o algo, hasta que llega el móvil, tarda unos 7 minutos mínimo, no sirve de nada". Por otro lado, todos/as en el COM coinciden en que Ensenada es un lugar chico en el que "no hay dónde esconderse". En este marco señalan que el problema del reconocimiento, de saber quién es quién, no precisa de este tipo de costosas tecnologías: para eso están ellos/as, que en tanto ensenadenses nacidos/as y criados/as pueden fácilmente reconocer a quien aparezca bajo cámara, aportando información de quién es, dónde vive, de qué trabaja, con quién se relaciona. Aunque se trate de información muy distinta a la brindada por las bases de datos estatales o privadas que podrían alimentar un sistema de reconocimiento facial, este tipo de conocimiento interpersonal es claramente una herramienta poderosa que los y las operadores/as del COM aprovechan muy bien. Según dicen, el problema no es reconocer sino la imposibilidad o la falta de voluntad para enfrentar a los delincuentes conocidos, atribuída a la policía y al poder judicial.

> (Operador): Es una boludés, no va a cambiar nada. Por ahí si se pierde un pibito, para encontrarlo más rápido. Pero hay tipos que se sabe que roban y la policía les pasa por adelante y no los pueden detener. [6]
>
> (Supervisor): Si total lo aprehendés, se lo llevás a un fiscal y lo larga. Tendrían que gastar en educación, no está preparado el país para eso. Si sabés que tenés pedido de captura, no vas a esa zona y listo. Ponele, si hay cámaras en el centro de Buenos Aires, no vas y ya está. (Nota de campo, 2-5-2019)

Por otro lado, la innovación desata una antigua discusión en términos de privacidad. ¿Es la vigilancia algorítmica más invasiva, o más peligrosa? El debate sigue las líneas de opinión sobre la vigilancia "analógica" que ellos/as realizan como tarea cotidiana: por un lado, un rechazo a toda expectativa de privacidad en el espacio público, por el otro, la percepción de que con los algoritmos se da un riesgoso salto de escala. Significativamente, la preocupación se expresa en clave política: ahora "te van a hacer registro de lo que hacés, de las movilizaciones a las que vas", y nadie queda libre porque para reconocer los supuestos objetivos el algoritmo debe aplicarse a todos/as. En este sentido, defienden la idea de que su forma artesanal de "monitoreo" es de alguna forma menos invasiva, más controlable, menos amenazante. A diferencia del monitoreo realizado por humanos, el algoritmo no discrimina sujetos y situaciones para establecer un uso proporcional de la invasión a la privacidad, sentando así las bases para un potencial uso autoritario.

> "Lo que pasa es que lo van a usar para todo, para gente con pedido de captura y para el resto. Como el registro ese que hicieron de personas que van a movilizaciones. Lo van a usar para las movilizaciones, las hinchadas. Por ejemplo si vas a una marcha a favor del aborto, van a saber que estás a favor aunque

6 "Boludés" refiere a una forma coloquial de decir "tontería". Un "pibito" es un diminutivo de pibe, es decir niño o joven.

> nunca hayas dicho nada, aunque no lo pongas en facebook (...) El tema es que es automático, no es que la cámara te muestra la foto y hay alguien buscando en una lista de fotos a ver quién es. La cámara domo va girando y va identificando. Andá a saber cuántas caras reconoce por segundo" (Supervisor, Nota de campo, 2-5-2019)

Por supuesto, esta alerta puede leerse en el marco de una amenaza tangible al control de los y las trabajadores/as del COM sobre el propio proceso de trabajo. Si el sistema se vuelve automático y ya "no hay nadie detrás", ¿sigue teniendo sentido emplear a alguien para realizar el "monitoreo"? A decir verdad, por el momento en el COM no se muestran muy preocupados, y seguramente tengan buenas razones para ello. A diferencia de las autoridades políticas que promocionan las innovaciones y los y las analistas que ponen el grito en el cielo alertando de sus riesgos, quienes lidian cotidianamente con la operación de la videovigilancia en Ensenada parecen depositar su confianza en que el factor humano seguirá siendo clave.

A modo de cierre: vigilancia, innovación y resistencia

Latour nos indicaba la importancia de ubicar al poder y la dominación como producto de redes de asociaciones entre humanos y no humanos, cuya estabilidad depende del número de uniones y la capacidad de "cajanegrizar" tramos de la cadena. Al plantearle esta perspectiva al director del COM puso rápidamente una cara de disgusto, mientras indicaba a su celular "acá tienen mi información personal, mis mails, mis contactos, mi información bancaria, mis huellas digitales, tienen todo. Eso es mucho más dominación que las cámaras". Debemos concordar que, comparados con el tamaño de las bases de datos y la capacidad de cómputo de las grandes corporaciones de internet, un sistema de videovigilancia municipal parece inofensivo. Sin embargo, el COM a demostrado su capacidad de articular elementos en torno una red, enfrentar distintos antiprogramas y ganar un lugar de influencia en el campo del control del delito de Ensenada. Aunque siempre situada, la trama que construye no está necesariamente limitada a una escala local: la cadena de asociaciones no está fija y es de hecho susceptible a nuevas incorporaciones.

Frente a la innovación en ciernes, ¿dónde ubicar la agencia humana, particularmente la de los y las trabajadores/as de la vigilancia? El caso de Ensenada nos brinda una muestra del valor de un análisis situado de la dinámica de estos ensamblajes sociotécnicos: allí donde el conocimiento personal de quienes realizan el monitoreo es una pieza clave para el éxito de todo el sistema, el "factor humano" gana cierto margen de control sobre el resto de los elementos. Sin embargo, como decíamos, la estabilidad de un actor red nunca puede darse por sentado, es un trabajo constante de reconstrucción e imposición de lazos. Los algoritmos de reconocimiento facial pueden no haber

llegado al COM, pero su aplicación en ciudades vecinas ya está generando repercusiones locales: fascinación, escepticismo y rechazo por partes iguales. ¿Seguirán ejerciendo una influencia "desde afuera" o lograrán introducirse en el ensamblado local de *vigilantes electrónicos*? ¿En qué medida puede convertirse el conocimiento personal en un antiprograma que resista la innovación? Se trata de interrogantes cruciales, si queremos aprovechar este momento de expansión – y controversia – para pensar el cruce entre videovigilancia, algoritmos y ciudades pequeñas o medianas. Algo al menos queda claro: detrás de la expansión de la videovigilancia algorítmica a nivel mundial, se esconden realidades heterogéneas y fragmentadas en la que elementos que operan a distintas escalas (un motor de búsqueda ruso, cámaras chinas, vigilantes ensenadenses) se combinan para dar fisonomías particulares a los *vigilantes electrónicos.*

Bibliografía

ARTEAGA BOTELLO, Nelson. Surveillance Studies: An Agenda for Latin America. **Surveillance & Society**, v. 10, n. 1, p. 5-17, jul 2012.

CARDOSO, Bruno. **Todos os Olhos. Videovigilâncias, videovoyeurismos e (re)produção imagética na tecnologia digital**. Tesis para la obtención del Doctorado en Ciencias Humanas (Antropología Cultural), Universidad Federal de Río de Janeiro, 2010.

CARDOSO, Bruno. Vigilantes eletrônicos no Rio de Janeiro: agenciamentos sociotécnicos e pesquisa em tecnologia. **Configurações: Revista de Sociologia**, n. 8, p. 97-108, 2011.

CRAMPTON, Jeremy W. Platform Biometrics. **Surveillance & Society**, v. 17, n. 1/2, p. 54-62, mar 2019.

DAMMERT, Lucía. Seguridad pública en América Latina: ¿qué pueden hacer los gobiernos locales? **Nueva Sociedad**, n. 212, p. 67-81, nov-dic 2007.

DONALDSON, Andrew. Surveillance and Non-Humans. En (Eds.) BELL, Kirstie, HAGGERTY, Kevin D. y LYON, David. **Routledge Handbook of Surveillance Studies**. New York: Routledge - Taylor and Francis Group: New York, 2012, p. 217-226.

GALVANI, Mariana; RÍOS, Alina L. y CAÑAVERAL, Lucía. **Seguridad, policía y gobiernos locales: eL Programa Integral de Protección Ciudadana**. Buenos Aires: Clacso, 2015.

GRAY, Mitchell. Urban Surveillance and Panopticism: will we recognize the facial recognition? **Surveillance & Society**, v. 1, n. 3, p. 314-330, sep 2003.

HIDALGO REQUENA, Jesús. De la 'sociedad disciplinaria' a la 'sociedad de control': la incorporación de nuevas tecnologías a la policía. **Scripta Nova**, Revista electrónica de geografía y ciencias sociales, v. 8, n. 170, ago 2004.

INTRONA, Lucas y WOOD, David. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. **Surveillance and Society**, v. 2, n. 2/3, sep 2002.

KESSLER, Gabriel. **El sentimiento de inseguridad. Sociología del temor al delito**. Buenos Aires: Siglo XXI Editores, 2009.

LATOUR, Bruno. La tecnología es la sociedad hecha para que dure. En DOMENECH, Miquel y TIRADO, Francisco J. (Comps.) **Sociología simétrica. Ensayos sobre ciencia, tecnología y sociedad**. Barcelona: Gedisa, 1998, p. 109-142.

LATOUR, Bruno. **Reensamblar lo social. Una introducción a la teoría del actor-red**. Buenos Aires: Manantial, 2008.

LIO, Vanesa y URTASUN, Martín J. . Devolviendo la mirada: Interrogantes y claves de lectura para la investigación de la videovigilancia. **Delito y sociedad**, v. 25, n. 41, p. 37-58, 2016.

NORRIS, Clive y ARMSTRONG, Gary. CCTV and the social structuring of surveillance. **Crime Prevention Studies**, v. 10, p. 157–178, 1999.

O'NEILL, Cathy. **Weapons of Math Destruction: how big Data increases inequality and threaten democracy**. New York: Crown, 2016.

ROSE, Nikolas y MILLER, Peter. **Governando o presente: gerenciamento da vida econômica, social e pessoal**. São Paulo: Paulus, 2012.

SIQUEIRA CASSIANO, Marcella. China's Hukou Platform: Windows into the Family. **Surveillance & Society**, v. 17, n. 1/2, p. 232-239, mar 2019.

SMITH, Gavin. Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK. **Surveillance and Society**, v. 2, n. 2/3, p. 376-395, sep 2004.

SMITH, Gavin. Surveillance work(ers). En (Eds.) BELL, Kirstie, HAGGERTY, Kevin D. y LYON, David. **Routledge Handbook of Surveillance Studies**. New York: Routledge - Taylor and Francis Group: New York, 2012, p. 107-115.

SOZZO, Máximo. Gobierno local y prevención del delito en la Argentina. **Urvio**, Revista Latinoamericana de Seguridad Ciudadana, n. 6, p. 58-73, ene 2009.

TAYLOR, Emmeline. The rise of the surveillance school. En (Eds.) BELL, Kirstie, HAGGERTY, Kevin D. y LYON, David. **Routledge Handbook of Surveillance Studies**. New York: Routledge - Taylor and Francis Group: New York, 2012, p. 225-231.

URTASUN, Martín J. Superar el punto ciego. La vigilancia en Latinoamérica y sus estudios. **Cuestiones de Sociología**, n. 10, jun 2014.

URTASUN, Martín J. **Vigilancia detrás de cámara: Acercamiento etnográfico a un sistema de videovigilancia**. Tesis de grado para la Licenciatura en Sociología, FaHCE, UNLP, 2016. Disponible online: http://www.memoria.fahce.unlp.edu.ar/tesis/te.1245/te.1245.pdf

WRIGHT, R. Data Visualization. En FULLER, Mathew (Org.) **Software Studies: a lexicon**. London: The MIT Press, 2008, p. 78-87.

AS mit MIT Press, 2008, p. 78-87.