Pérez Esquivel,.A. **Desafíos de la videovigilancia automatizada.** *Derecho y Ciencias Sociales*. Noviembre 2020 – Abril 2021. Nº 24 .Pgs 100-122 ISSN 1852-2971. Instituto de Cultura Jurídica y Maestría en Sociología Jurídica. Facultad de Ciencias Jurídicas y Sociales. Universidad Nacional de La Plata. Argentina.

Desafíos de la videovigilancia automatizada

Challenges of automated video surveillance

Andrés Pérez Esquivel•

Resumen

La videovigilancia automatizada y semiautomatizada, con algoritmos de reconocimiento facial y de comportamientos, está generando debates a nivel internacional que son importantes de profundizar sin apresurarnos a conclusiones rápidas, pero tampoco lentas.
A diferencia de otros países de América y de Europa, Argentina, aún en 2020 no cuenta con una ley nacional regulatoria de la videovigilancia clásica y, el distrito más poblado y con más cámaras del país, la Provincia de Buenos Aires, tampoco se ha dado un marco regulatorio integral propio. Los frágiles cimientos institucionales que hacen de puerto de llegada a esta tecnología de punta no deberían ser desatendidos si se quieren evitar efectos negativos, no sólo en la protección de la privacidad, sino también en clave de fortalecimiento del derecho a la seguridad, el motivo que legitima su implementación.

La intención principal de este escrito, enmarcado en el campo de los estudios de vigilancia y las políticas públicas, es aportar elementos desde las Ciencias Sociales para intentar desentrañar algunos nudos conceptuales que, además de generar malentendidos recurrentes, tienen efectos normativos que colaboran en naturalizar ciertas prácticas que deberían requerir mayor detenimiento. Entre ellos podemos mencionar la imprecisa y mecánica asimilación entre vigilancia y seguridad; la efectividad relativa de los sistemas de videovigilancia en función de seguridad y en función judicial; la relación entre los derechos a la privacidad e intimidad con el espacio público; los vínculos entre lo tecno-lógico y lo ideo-lógico; etc. Estos aspectos serán ejemplificados a partir del caso de la implementación de esta tecnología en la Ciudad Autónoma de Buenos Aires, a través del análisis documental de normativas y documentos oficiales.

Palabras clave: seguridad, privacidad, biometría, CCTV, videovigilancia.

Abstract

Automated and semi-automated video surveillance, with facial and behavioral recognition algorithms, is generating international debates which are important to delve into without rushing to quick, but neither slow, conclusions.
Unlike other countries in America and Europe, in 2020 Argentina still does not have a national regulatory law for classic video surveillance, and the most populated district with the most cameras in the country, the Province of Buenos Aires, does not have its own integral regulatory framework either. The fragile institutional foundations that receive this advanced technology should not be overlooked if negative effects are to be avoided, not only in the protection of privacy, but also in terms of strengthening the right to security, which is the reason that legitimizes its implementation.

• Licenciado y Profesor en Sociología, Universidad de Buenos Aires. Magister en Políticas Públicas y Gestión del Desarrollo, Universidad Nacional de San Martín. Master of Arts in Development, Management and Policy, Universidad de Georgetown. Doctorando en Ciencias Sociales, Universidad de Buenos Aires. apesquivel@sociales.uba.ar / ap1281@georgetown.edu.

Recibido: 24/8/2020. Publicable con correcciones: 12/02/2021.

The main intention of this paper, framed in the field of surveillance studies and public policies, is contribute from a Social Sciences perspective to unravel some conceptual knots that, in addition to generating recurrent misunderstandings, have normative effects that collaborate in naturalizing certain practices that require further thought. Among them, we can mention the imprecise and mechanical assimilation of surveillance and security; the relative effectiveness of video surveillance systems in terms of security and judicial functions; the relationship between the rights to privacy and intimacy with public space; the links between the techno-logical and the ideo-logical; etc. These aspects will be exemplified through the case of the implementation of this technology in the City of Buenos Aires, through the documentary analysis of regulations and official documents.

Keywords: security, privacy, biometry, CCTV, video surveillance.

Pérez Esquivel,.A. **Desafíos de la videovigilancia automatizada.** *Derecho y Ciencias Sociales*. Noviembre 2020 – Abril 2021. Nº 24 .Pgs 100-122 ISSN 1852-2971. Instituto de Cultura Jurídica y Maestría en Sociología Jurídica. Facultad de Ciencias Jurídicas y Sociales. Universidad Nacional de La Plata. Argentina.

Desafíos de la videovigilancia automatizada

Andrés Pérez Esquivel

Introducción

A nivel internacional, la videovigilancia automatizada y semiautomatizada está siendo motivo de arduos y complejos debates que resulta pertinente profundizar con cierta celeridad en la Argentina en función de un adecuado diseño, implementación y evaluación de este tipo de políticas públicas.

Desde hace un tiempo, el punto de encuentro entre las dinámicas de videovigilancia de flujos poblacionales en gran escala, y de personas particulares para propósitos de investigación judicial, está fomentando las condiciones de posibilidad para identificar quién está en un lugar determinado, qué está haciendo, y trazar que hizo o hará en diversos lapsos de tiempo, con distintos grados de probabilidad de éxito de acuerdo con el objetivo de vigilancia definido. Los países que usan esta tecnología hace más tiempo, usan el reconocimiento facial de manera aérea con drones, en eventos masivos, y con cámaras policiales portátiles “al ras del piso”, entre otras variantes. Este permanente incremento de la videovigilancia en términos de escala y funcionalidades ha generado que muchos países establecieran normas regulatorias para evitar abusos de poder. Pero una destacable y reciente novedad es que en el año 2019 muchas ciudades de los Estados Unidos, un país vanguardia en esta materia, comenzaron a prohibir los sistemas de reconocimiento facial por considerar que vulneraban los derechos de su población.

Argentina, por su parte, a diferencia de otros países de América y de Europa, aún en 2020 no cuenta con una ley nacional regulatoria de la videovigilancia clásica[1] y la Provincia de Buenos Aires, el distrito más poblado y con más cámaras del país, tampoco se ha dado un marco regulatorio integral propio como sí lo han hecho la mayoría de las provincias. Los frágiles cimientos institucionales que hacen de puerto de llegada a esta tecnología de punta no deberían ser desatendidos si se quieren evitar efectos negativos, no sólo en la protección de la privacidad, sino también en clave de fortalecimiento del derecho a la seguridad, el motivo que legitima su implementación.

Más allá de esto, la intención principal de este trabajo es aportar elementos desde las Ciencias Sociales para intentar desentrañar algunos nudos conceptuales que, además de generar malentendidos recurrentes, tienen efectos normativos que colaboran en naturalizar ciertas

[1] Sólo existe la Disposición Reglamentaria Nº 10/2015 de la Ley de Protección de Datos Personales de la Dirección Nacional de Protección de Datos Personales, que aprobó las *"Condiciones de licitud para las actividades de recolección y posterior tratamiento de imágenes digitales de personas con fines de seguridad"*.

prácticas que deberían requerir mayor detenimiento. Entre ellos podemos mencionar la imprecisa y mecánica asimilación entre vigilancia y seguridad; la diferencia entre seguridad preventiva y anticipatoria; la relación entre los derechos a la privacidad e intimidad con el espacio público; los vínculos entre lo tecnológico y lo ideológico; la efectividad relativa de los sistemas de videovigilancia en función de seguridad y en función judicial; los criterios de autenticidad y confiabilidad de las imágenes y los intérpretes en el proceso penal; el vínculo entre vigilancia algorítmica y el derecho al debido proceso; entre otros.

Sin pretender dar respuestas uniformes ni definitivas a estos interrogantes, se espera aportar al debate interdisciplinario y la toma de decisiones, considerando los riesgos de que haya una expansión acrítica de la videovigilancia automatizada. De esta manera, procederé a ordenar este trabajo alrededor del análisis conceptual de los objetivos políticos que existen detrás de toda política pública de videovigilancia: El mandato primordial de fortalecer la prevención securitaria, y el mandato accesorio de asistir con información y material probatorio a la investigación judicial. Para luego ejemplificar algunos de los elementos desarrollados en el caso de la Ciudad Autónoma de Buenos Aires (en adelante CABA), a partir de avances de investigación para mi tesis del Doctorado en Ciencias Sociales de la Universidad de Buenos Aires, logrados a partir del análisis documental de normativas y documentos oficiales.

El mandato primordial de los CCTV: fortalecer el derecho a la seguridad

La videovigilancia policial en el espacio público es, principalmente, una política pública de seguridad urbana para la prevención situacional del delito, y para reducir el sentimiento de inseguridad en la población. A raíz de esto, las videocámaras de vigilancia son usualmente llamadas "cámaras de seguridad", y las zonas videovigiladas son frecuentemente referidas como "zonas seguras". Sin embargo, detrás de este imaginario se encuentran ciertas confusiones conceptuales que presuponen a la vigilancia como sinónimo de seguridad. Tratemos de identificar sus diferencias.

Supongamos que un gobierno quiere fortalecer los lazos comunitarios entre grupos sociales o territoriales en conflicto, o los lazos de confianza entre la comunidad y las fuerzas policiales. Si para ello implementa un sistema de vigilancia policial intrusiva sobre esos grupos o territorios, probablemente el resultado no sea una desactivación sino una suspensión temporaria del conflicto, o su desplazamiento a espacios no vigilados. Supongamos también que un gobierno "inunda" una ciudad de cámaras pero no cuenta con los efectivos policiales suficientes para asistir a la población *in situ*, o el sistema no está articulado con una estrategia integral de seguridad. Si bien tendrán un inicial efecto disuasorio, a fin de cuentas será un placebo de carácter efímero. En ninguno de los dos casos estas vigilancias aportarían a los objetivos de seguridad definidos: prevención comunitaria y disminución de tasas delictivas. A su vez, sin objetivos securitarios, el mismo gobierno puede

realizar vigilancia sobre la población a través de estadísticas a ciertos grupos poblacionales, como por ejemplo sucede con el cumplimiento obligatorio del calendario escolar y vacunatorio. Por lo cual no toda vigilancia tiene como objetivo o resultado fortalecer el derecho a la seguridad. Definiremos, entonces, en este trabajo a la *vigilancia* como las actividades orientadas a individuos y poblaciones humanas basadas en su observación regular y sistemática (visual, mecánica, electrónica, digital), la producción de conocimiento sobre ellos (patrones, tendencias, causalidades), y la intención de intervenir sobre sus conductas (Bruno, 2013). Y a la *seguridad* desde el enfoque de derechos humanos (CIDH, 2009), como una condición donde las personas viven libres de la violencia practicada por actores estatales y no estatales, y en la que el Estado tiene las capacidades necesarias para garantizar la protección del derecho a la vida, la integridad física, la libertad, el uso pacífico de los bienes, entre otros conexos.

Esta distinción es importante porque en materia de derechos humanos fundamentales, las políticas de videovigilancia en el espacio público son políticas de excepción que empiezan con *saldo negativo*. De manera condicional, esta política vulnera el derecho a la privacidad e intimidad de los habitantes con la promesa de fortalecer paulatinamente su derecho a la seguridad. Concretamente, el Estado ejerce una vigilancia electrónica masiva que aumenta su proyección de poder, sin proyectar vulnerabilidad, avanzando sobre la esfera privada e íntima de los individuos. Por este motivo, bloques regionales como la Unión Europea[2], y distintos países del mundo sancionaron leyes específicas[3] desde los años 90 para regular la actividad. En el caso del continente americano, la *legalidad* de esta política descansa en que cumpla con la única condición aceptada por la Corte Interamericana de Derechos Humanos (en adelante Corte IDH) para restringir el goce o ejercicio de un derecho fundamental de la Convención Americana de Derechos Humanos[4] (en adelante CADH), esto es, que se implemente con fines de seguridad, y a través de una ley sancionada por un órgano legislativo constitucional que regule el balance entre el derecho fundamental jerarquizado y el afectado (CIDH, 2009). Por este motivo, la *legitimidad* de esta política de seguridad descansa en que pueda efectivamente demostrar que es necesaria para reducir las tasas del delito y el sentimiento de inseguridad sin generar vulneraciones desproporcionadas. Ambos aspectos serán analizados a continuación.

[2] Reglamento General de Protección de Datos (EU) 2016/679 (GDPR por sus siglas en inglés).

[3] Francia tiene una ley nacional que regula la videovigilancia desde el año 1995 (Loi Pasqua); España desde el año 1997 (Ley orgánica 4/97); el Reino Unido desde el año 1998 (Data Protection Act 1998); Alemania (Bundesdatenschutzgesetz – BDSG/2003); Italia (Codice in materia di protezione dei dati personali /2003); Portugal (Lei Nº 1/2005), por citar algunos ejemplos. Y en América Latina, Uruguay (Ley Nº 18331/08) y Perú (Ley Nº 30120/13) tienen leyes nacionales, pero la gran mayoría tiene normativas de menor rango.

[4] La expresión "Leyes" en el Artículo 30 de la CADH - Corte IDH - Opinión Consultiva OC-6/86. Serie A No. 6. - 9/05/1986.

Legalidad de los CCTV

Para analizar los aspectos legales, es imprescindible hacer algunas aclaraciones conceptuales sobre la aplicabilidad de los conceptos de privacidad e intimidad en el espacio público, porque es común escuchar funcionarios, abogados, periodistas y personas en general, decir que si uno está en la vía pública no puede pretender reclamar privacidad o intimidad. Si bien es absolutamente cierto que no se puede pretender no ser visto en la vía pública, esto no significa que los espacios de la intimidad se limiten exclusivamente a ciertos ámbitos cerrados como el domicilio, el teléfono o la correspondencia (Garibaldi, 2010). En este sentido se ha manifestado el Tribunal Europeo de Derechos Humanos en el caso *Geoffrey Peck c. Reino Unido*[5] del año 2003, cuando definió que hay interacciones en el espacio público que pueden ser consideradas parte de la vida privada y, por lo tanto, que la intimidad también involucra el espacio público. Lo mismo expresó la Corte IDH en el caso *"Tristán Donoso c. **Panamá"**[6]* **del año 2009, definiendo que el término "vida privada" del texto de la CADH debe tener una interpretación dinámica que no se agote exclusivamente en el domicilio y la correspondencia. Más recientemente, nos encontramos con la sentencia d**el caso *Carpenter c. Estados Unidos*[7] del año 2018, en el que la Corte Suprema de Justicia falló en contra de la trazabilidad de movimientos de personas en el espacio público mediante los registros de las antenas celulares, sin autorización judicial. Y en el ámbito local, con un fallo del Juzgado Penal, Contravencional y de Faltas N°10 de la CABA que, sobre la base de estos antecedentes, declaró la nulidad de una medida dispuesta por un fiscal, quien había solicitado sin orden judicial información sobre la "**intimidad de los registros de transacción de una cuenta"**[8] **que permitían rastrear la ubicación del celular** de una persona.

Esta interpretación dinámica y amplia de la vida privada nos permite vislumbrar su relación con el concepto de información personal, y el manejo y control de los datos personales. El derecho de *autodeterminación informativa*, derivado de la garantía de intimidad, trata del derecho a decidir y disponer libremente sobre los datos personales, y quiénes pueden acceder a ellos. A través de las leyes de protección de datos personales el Estado garantiza que los individuos puedan ejercer este derecho, restringiendo las capacidades de organizaciones públicas y privadas para obtener, disponer y publicar datos personales, evitando discrecionalidades y recortes de libertad. Por ejemplo, a través

[5] "There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'" ["Existe, por tanto, una zona de interacción de una persona con otras, incluso en un contexto público, que puede caer dentro del ámbito de la 'vida privada'" - Traducción propia]. Tribunal Europeo de Derechos Humanos. Peck vs. Reino Unido (2003). Petición 44647/98, apart.57, TEDH 2003-I.

[6] Tristán Donoso c. Panamá - Corte IDH - Serie C No. 193, párr. 29 - 27/01/2009.

[7] "A person does not surrender all Fourth Amendment protection by venturing into the public sphere" ["Una persona no renuncia a toda la protección de la Cuarta Enmienda al aventurarse en la esfera pública" – Traducción propia]. Corte Suprema de Estados Unidos de América. Carpenter v. United States (2018). 138 S.Ct. 2206, 2217.

[8] Res. Nulidad - Juzgado PCyF N° 10 CABA - Reg. N° 1429. Tomo 11. Expte. N° 24452/18 - 3/09/2018.

del *Habeas Data*. De manera que colaboran con garantizar razonables expectativas de anonimato, autodeterminación informativa y, consecuentemente, mayor intimidad y privacidad.

Por lo tanto, cuando se habla de que los CCTV deben ser regulados porque vulneran la privacidad, la intimidad y la confidencialidad de las personas, no se refiere solamente a que una cámara podría llegar a captar imágenes del interior de propiedades, sino que podría vulnerar la intimidad de personas en el espacio público, inhibiendo conductas privadas que se asientan en la expectativa de anonimato, de no ser visto, ni registrado cuando, por ejemplo, se está con una pareja en un espacio público, se participa en una manifestación pública, o se ingresa a lugares que delatan datos personales sensibles de la persona como son centros religiosos, bares exclusivos para cierta orientación sexual, hoteles alojamiento, locales partidarios, etc.

En pocas palabras, podríamos sintetizar diciendo que caminar en la calle o ir a una plaza nos hace visibles en el espacio público pero no *sujetos públicos*, ni menos aún *sujetos publicitables*, porque existen manifestaciones públicas de la vida privada basadas en expectativas razonables de anonimato que hacen a la dignidad humana. Por lo cual, para que un sistema de videovigilancia sea considerado legal debería ser regulado por una ley que, además de colaborar con la prevención securitaria, establezca garantías de protección de la privacidad, la intimidad y la confidencialidad de los datos personales.

Legitimidad de los CCTV

La legitimidad de este sistema se construye a partir de obtener resultados positivos en materia de reducción de índices delictivos y el sentimiento de inseguridad. De no lograr esto, la política no cumple con el principio de necesidad que motivó su implementación, y deja de justificarse la continuidad de la vulneración del derecho a la privacidad e intimidad. Por otro lado, debe ser implementada de manera proporcional, o sea, debe demostrarse que la técnica usada es la menos invasiva en la práctica, entre otras instancias posibles.

A la hora de evaluar su efectividad para reducir las tasas delictivas, los estudios académicos concuerdan en que los CCTV son más efectivos para reducir crímenes en espacios poco complejos como pueden ser playas de estacionamiento de automóviles, estadios deportivos, aeropuertos, entre otros. Sin embargo, cuanto más amplia y compleja es la situación o el espacio, más difícil es evaluarlos porque es mayor el número de variables a considerar.

A nivel internacional, en los países donde han sido evaluados en el espacio público, estos sistemas han demostrado nula o muy poca eficacia para disminuir las tasas delictivas (Melgaço, Verfaillie y Hildebrandt, 2013; Carli, 2008; Gill y Spriggs, 2005; Webster, 2004; Welsh y Farrington, 2003; Armitage, 2002; Ditton, 2000), aunque se han mostrado más útiles en función de la investigación judicial, algo que veremos más adelante. Lo más frecuente es que estos sistemas logren captar una

cantidad importante de delitos pero que los mismos no representen una proporción significativa del universo total de delitos denunciados como para justificar sus costos en materia de protección de derechos y de presupuesto. La situación más frecuente, en especial en América Latina, es que ni siquiera se hagan evaluaciones de efectividad (Dammert y Silva, 2018), de manera que no se puede saber si los sistemas colaboran en disminuir nula, significativa o insignificativamente en las tasas del delito en el espacio público. A modo de reemplazo, las policías hacen registros de eventos detectados y/o intervenidos, pero en muchos casos esos "eventos" involucran una serie de fenómenos muy diversos que no necesariamente están vinculados con delitos, sino faltas, contravenciones y hasta manifestaciones políticas. También con frecuencia se publican las mismas imágenes de los CCTV con casos de conjuraciones de delitos en flagrancia, como una manera de mostrar su efectividad. Su reiteración permanente suele generar la impresión de que estos casos exitosos impactan significativamente en los índices del fenómeno delictivo, pero no es algo verificado. Por el contrario, un escenario posible es que el CCTV aumente el poder policial, vulnere derechos fundamentales de los habitantes, y que al mismo tiempo las tasas de victimización continúen aumentando. En otras palabras, sin evaluaciones de efectividad no podemos saber si estamos hablando de cámaras de vigilancia, o de cámaras de seguridad.

En términos generales, podemos decir que los detractores de esta política de prevención situacional suelen reconocerle cierta efectividad bajo ciertas condiciones de implementación y para reducir determinados delitos (Melgaço, Verfaillie y Hildebrandt, 2013; Cusson, 2005). Mientras que los promotores entusiastas, consideran que estas tecnologías son inherentemente efectivas, de manera que si los resultados de la evaluación de efectividad no resultan positivos, alegan que se debe a una implementación incorrecta del CCTV, ya sea por problemas humanos, porque falta expandirlo en escala, o porque necesita ser actualizado con tecnología complementaria, como puede ser la videovigilancia aérea, automatizada o sonora, entre otras posibilidades.

Esta última postura, responde a una ideología bastante difundida socialmente que suele mostrar a las tecnologías como "neutrales", "racionales" y "eficientes", o sea, como parte de un progreso científico universal donde los factores culturales y políticos pueden influir de manera contingente, pero no modificar su lógica autónoma, inmanente e indetenible. Ideología que aquí llamaremos "eficientista" (Feenberg, 2012 [2000]). La ideología eficientista, que no se presenta como tal, apela al imaginario de verdad científica como instrumento de legitimación, y deslegitimación de otros principios sociopolíticos que puedan ponerla en discusión. Si hay un problema, no se debe a lo tecnológico, sino a alguna interferencia humana, sea ideológica u operativa, como el factor aburrimiento de los operadores (Smith, 2004), que perjudica el "correcto" funcionamiento o ampliación de la solución tecnológica. Para esta postura cualquier falla o cuestionamiento en el sistema es un motivo para ampliarlo y tecnificarlo aún más. Y aquí es donde entran en escena los

nuevos sistemas de videovigilancia "inteligentes" o automatizados, que vendrían a resolver algunos de los cuestionamientos anteriores. En efecto, los sistemas de análisis automatizado de imágenes alegan resolver el gran punto débil de la ecuación costo-beneficio de los CCTV, que limita su expansión. En el CCTV tradicional, cuantas más cámaras hay, más personal se necesita para monitorearlas en vivo. Con lo cual se quitan recursos económicos que podrían estar destinados, por ejemplo, a tener más policías en las calles que puedan auxiliar a las personas. Los Sistemas de Reconocimiento Facial (SRF), de Comportamientos (SRC), de Sonidos (SRS)[9], supuestamente, resolverían estas falencias humanas facilitando a cada operador poder monitorear una mayor cantidad de cámaras en tiempo real, y hacer análisis retrospectivo de gran escala.

Videovigilancia automatizada

Cuando hablamos de videovigilancia automatizada nos referimos a *softwares* que permiten, mediante un conjunto de algoritmos, analizar las imágenes captadas y generar automáticamente información con sentido para la toma de decisiones humanas, o para ejecutar una orden de movimiento al dispositivo físico (la cámara). Tiene la capacidad de detectar objetos, personas, sus características biométricas, eventos y movimientos particulares, reforzando el monitoreo en vivo y la búsqueda retrospectiva con fines de selección, identificación y trazabilidad de personas y cosas. En lo que respecta a los SRF, se refieren a una serie de algoritmos de identificación biométrica de individuos que sirven para autenticar (confirmar que esa persona es quien dice que es) e identificar (saber quién es una persona en un grupo determinado de personas). Su uso en videovigilancia suele estar dirigido a identificar personas prófugas de la justicia, entre los individuos que caminan en la vía pública, o sea, dentro de una galería abierta de rostros. En lo que respecta a los SRC, se refiere a algoritmos antropométricos que pueden reconocer en tiempo real movimientos individuales y grupales predefinidos como "anormales", aunque los mismos no constituyan una falta, una contravención, un delito, ni se conviertan nunca en tales. Concretamente, envían una alerta automática al centro de monitoreo policial cuando identifican una persona corriendo en la vía pública, cuando un grupo de personas se queda inmóvil en una esquina o frente a una vidriera, cuando hay demasiada gente en un lugar u horario donde no es frecuente que lo haya, entre una serie de comportamientos que el sistema puede definir como sospechosos. En pocas palabras, alerta automáticamente sobre conductas ajenas a lo que "deberían ser" siguiendo la configuración de prejuicios dada por las agencias de seguridad y justicia del Estado, o incluso importando los que existen en los manuales de procedimientos de las empresas proveedoras.

[9] Por cuestiones de espacio no se analizarán los SRS en este artículo.

Prevención y anticipación securitaria

La incorporación de la automatización hace más fácil brindar una definición completa de la videovigilancia como una política híbrida. Si bien, por un lado, se enmarca en el campo de las políticas de prevención (en inglés *prevention*) (por su carácter disuasorio cuando están debidamente señalizadas y distribuidas) y conjuración del delito cuando están debidamente monitoreadas. Por otro lado, tiene una faceta de anticipación (en inglés *preemption*) porque crean un registro sobre la población vigilada, considerando a todos quienes entran en su rango óptico como potenciales ofensores (y potenciales víctimas) de manera indiscriminada. Esta faceta anticipatoria se ve radicalizada con la incorporación de SRC porque anticipa y señala (bien o mal) en tiempo real a supuestos ofensores que pueden no serlo. Si bien el objetivo de la prevención y la anticipación es neutralizar amenazas, ambas difieren epistemológica y ontológicamente (IRISS, 2012). La *prevención* asume la habilidad de evaluar amenazas empíricamente e identificar sus causas. Una vez que las causas están identificadas se toman medidas apropiadas para evitar su realización. La prevención funciona en un mundo conocible donde la incertidumbre está en función de la falta de información, y donde los eventos tienen causas y efectos. La *anticipación*, por el contrario, actúa sobre riesgos que permanecen perpetuamente indeterminados. Criminalísticamente lleva al extremo la prevención situacional/ambiental asumiendo que las políticas no se deben enfocar en el control de las causas que generan el delito, porque ese objetivo es una utopía. El delito se vuelve un fenómeno natural que debe ser calculado, dejando de ser una actividad que necesite ser comprendida para lograr su disminución. De esta manera busca neutralizar amenazas que están en permanente estado potencial, interviniendo sobre los hábitos de la interacción, el diseño espacial urbano y los incentivos existentes para cometer actos delictivos. A diferencia de la inteligencia criminal, en el paradigma anticipatorio predelictivo cualquiera puede ser considerado un potencial ofensor, por lo cual es necesario recolectar la mayor cantidad de datos e información posible sobre la mayor cantidad de personas posible, ya que nunca está claro qué dato o información podría llegar a ser útil. En su cara más extrema, el paradigma anticipatorio predictivo es una universalización de la sospecha sobre todo el cuerpo social a través de la vigilancia digital semiautomatizada de datos personales (en inglés *datavaillance*) y su trazabilidad en tiempo y espacio. Y no sólo vigila individuos, sino *dividuos*, porque la biometrización implica medir y dividir la biología única de cada persona. Aquí es importante aclarar que los conceptos de prevención y anticipación no se dan en estado puro sino que son tipos ideales orientativos. No hay un país o policía que pueda llamarse preventiva o anticipatoria, en general se dan diferentes combinaciones en función de los marcos normativos (o la ausencia de estos), los recursos y capacidades disponibles, y las posibles dificultades políticas para su desarrollo. En los últimos años, de la mano de las nuevas TICs y la datificación urbana producida

por los modelos de ciudades inteligentes (Rennó et al., 2017), se han generado las condiciones de posibilidad para el auge y sofisticación de los modelos de policiamiento guiado por inteligencia (Ugarte, 2012) o predictiva (Perry et al., 2013) en distintas partes del mundo, cada una con distintos balances entre prevención y anticipación.

Por otro lado, la posibilidad que brindan los SRF de hacer averiguaciones de identidad en la vía pública de manera remota, automatizada y en tiempo real, hacen que los CCTV potencien una faceta de uso persecutorio que antes sólo tenían a demanda de un juez. Si bien la persecución penal está en el marco de la investigación judicial, estos sistemas también pueden reforzar el carácter anticipatorio de la videovigilancia dependiendo de si es usado para contrastar con una base de rostros de personas con requerimiento de un tribunal, o con una base de datos más amplia que expanda la escala de la sospecha más allá de la investigación judicial de delitos. En este último caso, los objetivos irían mucho más lejos. Si los SRF se utilizan bajo un paradigma anticipatorio para ampliar masivamente la vigilancia, la sospecha y el rastreo de personas que no están acusadas ante una corte de ningún delito, las ubicará en un limbo donde se les estará vulnerando el derecho de presunción de inocencia. Una especie de rueda de reconocimiento perpetua[10]. En efecto, no podrán exigir el derecho al debido proceso porque no habrá ninguna acusación formalizada en el marco de un procedimiento penal (IRISS, 2012). Lo mismo sucede con el derecho a no autoincriminarse, los habitantes (sus datos personales biométricos) son registrados y convertidos en objetos de prueba ante potenciales futuras imputaciones. Estas prácticas de vigilancia se ponen al mismo tiempo dentro y fuera del derecho penal, lo que puede facilitar a las agencias policiales eludir el debido proceso en nombre de la aplicación de la ley.

Confiabilidad y efectividad

Definir la confiabilidad de los SRF y los SRC no es una tarea sencilla porque la vigilancia algorítmica no es un proceso transparente. Esto se debe a dos motivos principales (Introna y Wood, 2004): El primero es que la mayoría de los *softwares* son propietarios, o sea, de código cerrado. Esto significa que el Estado puede comprarlos llave en mano pero no puede inspeccionarlos, auditarlos, ni modificarlos. Y en el caso de que eso fuera posible, analizando el código línea por línea, es imposible saber si el código inspeccionado es el mismo en acción porque se ejecuta a través de múltiples capas de traducción. Son operacionalmente oscuros. En segundo lugar, la mayoría de los algoritmos están basados en métodos estadísticos sofisticados que sólo unos pocos expertos pueden interpretar y entender, para el resto se trata de "cajas negras", por lo cual también son políticamente

[10] Garvie, C. (2019). You're in a Police Lineup, Right Now (Estás en una rueda de reconocimiento policial ahora mismo – Traducción propia). New York Times. Recuperado el 10 de febrero de 2020: https://www.nytimes.com/2019/10/15/opinion/facial-recognition-police.html?smtyp=cur&smid=tw-nytopinion.

oscuros. Esta falta de transparencia y explicabilidad, combinada con una ideología eficientista tecnológica, pueden generar un aura de legitimidad que vaya más allá de lo que merecen, y que los algoritmos puedan ser considerados con mayor autoridad que los humanos a la hora de decidir sobre ciertos aspectos. En efecto, la fuerza de los hábitos puede hacer que los operadores se acostumbren a reaccionar a las alertas excluyendo otras informaciones igualmente o más válidas.

Con respecto a su eficiencia, no basta con saber cuánto aciertan sino también cuanto se equivocan. Si estos sistemas automatizados se muestran eficientes hay que preguntarse para qué objetivo y por qué. Por ejemplo, pueden ser muy efectivos para identificar prófugos (una buena noticia), pero al mismo tiempo pueden ser muy efectivos para aumentar las detenciones arbitrarias de personas inocentes, que refuercen los actuales procesos de exclusión y selectividad del sistema penal basados en "ajustes fenéticos" (en inglés *phenetic fix*) vinculados al fenotipo (Lyon, 2002) en especial en áreas urbanas de elevado interés turístico (Kanashiro, 2008). En este sentido, es necesario definir los índices de aceptación falsos, o sea, la probabilidad de que el sistema haga coincidir de manera incorrecta las imágenes a contrastar creando un falso positivo. Por otro lado, es necesario definir los índices de rechazo falsos, o sea, la probabilidad de que el sistema falle en detectar una coincidencia creando un falso negativo. Por lo tanto, lidiar con un SRF es, al mismo tiempo, determinar cómo lidiar políticamente con estos falsos positivos y negativos, ya que muchas falsas alarmas requieren recursos extra para hacer un seguimiento constante, y tienen implicancias sociales y legales significativas (Introna y Wood, 2004).

Y los problemas de eficiencia y efectividad han aparecido. No es un dato menor que en la ciudad más videovigilada del mundo, Londres, de ocho pruebas realizadas entre 2016 y 2018 el 96% de los casos haya resultado en falsos positivos[11]. Ni que en las pruebas realizadas por el gobierno de los Estados Unidos, los sistemas hayan tenido un sesgo de identificación errónea de personas de piel oscura, con tasas de cinco a 10 veces más altas que a las de piel blanca[12]. A esto debemos sumarle posibles problemas vinculados a la gestión del sistema. Hay estudios que demostraron cómo algunos policías pueden considerarse no atados a las normativas regulatorias y, por lo tanto, sentirse habilitados a manipular los registros de imágenes si los mismos pueden convertirse en evidencia que los incrimine (Goold, 2003; en Carroll-Mayer et al., 2008). De manera que también es importante saber si los sistemas automatizados realizan exclusiones o "listas blancas" de algún tipo,

[11] "Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal" ("El reconocimiento facial identifica erróneamente al público como posibles delincuentes el 96% de las veces, según revelan las cifras" – Traducción propia). (7 de mayo de 2019). *Independent*. Recuperado el 10 de febrero de 2020 de: https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html.

[12] "The Best Algorithms Struggle to Recognize Black Faces Equally". ("Los mejores algoritmos luchan por reconocer las caras negras en igualdad" – Traducción propia) (22 de julio de 2019). *Wired*. Recuperado el 10 de febrero de 2020 de: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

por ejemplo, si identifica los uniformes de los efectivos policiales y los excluye de las alertas, asumiendo que ninguno puede cometer delitos.

En general, en los casos en que los SRF se han demostrado más eficientes es en aplicaciones de verificación cerradas (en inglés *close set*) que de identificación abierta (en inglés *open set*), y en casos de pequeñas poblaciones y ambientes controlados (Introna y Nissenbaum, 2009). Pero sus aspectos técnicos y operacionales nunca pueden dejar de ser evaluados porque los algoritmos realizan aprendizajes autónomos mediante inteligencia artificial (en inglés *machine learning*) que podrían no coincidir con el mismo sentido en que las normas sociales y objetivos políticos van cambiando.

El mandato accesorio de los CCTV: fortalecer el derecho a la justicia

Hasta aquí desarrollamos los CCTV puestos en función de seguridad, única capaz de justificar la implementación y mantenimiento de estos sistemas. En esta sección trataremos su uso concomitante en función de la investigación judicial. La función de justicia es un eje con mayor capacidad de medición de los CCTV porque, si bien las videocámaras pueden no aportar a la prevención o conjuración del delito, es más probable que puedan aportar información o material probatorio sobre hechos ocurridos en el marco de investigaciones judiciales. No sólo son importantes para identificar ofensores sino también para establecer la naturaleza, lugar y tiempo de algunos crímenes. Sin embargo, tampoco es una tarea sencilla lograr esto, porque es frecuente que las cámaras no capten lo ocurrido, o que lo hagan pero las imágenes no sean buenas. Aquí, su utilidad depende mucho de cómo se gestione el carácter de confiabilidad de la lectura de la imagen desde el Poder Judicial. Un aspecto menos estudiado de estos sistemas[13], por lo que vale la pena poner atención a reconceptualizar las relaciones constitutivas de coproducción entre tecnologías, operadores judiciales (incluyendo expertos forenses), procedimientos legales y destinatarios finales.

De acuerdo con Edmond y San Roque (2013), la manera en que el Poder Judicial ha incorporado imágenes de vigilancia y creado evidencia forense a partir de comparación de imágenes, tiende a mostrar una confianza exagerada. En un contexto de crecimiento exponencial de material visual de vigilancia como potencial evidencia, y el correspondiente aumento en la brecha para poder trabajarlo, resulta un desafío definir reglas claras de admisión y tratamiento de imágenes en el fuero penal, en especial cuando hay que lidiar con imágenes poco claras o confiables.

Según estos autores, la elevada inversión en tecnologías, y las expectativas políticas y sociales en torno a los imaginarios que las rodean, pueden fomentar la comodidad judicial acrítica, o que a los

[13] Entre los autores que sí lo han hecho vale la pena mencionar a Edmond y San Roque (2013); Matthew Ashby (2017); Tim Valentine (2015); entre otros.

jueces les resulte más difícil excluir cierto material como evidencia. Así los investigadores, fiscales y jueces pueden asimilar imágenes y nuevas tecnologías de identificación como si permitieran reproducciones mecánicas de la realidad. Y desatender la cadena de preservación de las imágenes; distorsiones; la significación de similitudes aparentes; efectos contextuales; tendencias; la validación y márgenes de error; entre otros elementos que repercuten en la ampliación o disminución de material de vigilancia a incorporar como evidencia probatoria.

Además de la regulación de la utilización de imágenes, también plantean la necesidad de establecer criterios claros de selección de opiniones de "expertos" en lecturas de imágenes y de voces en *off*, que puedan colaborar en la determinación de culpabilidad, haciendo interpretaciones de situaciones y comparaciones identificatorias de sospechosos. Si bien la utilización de expertos puede ser leída como un reconocimiento de la insuficiencia de las tecnologías para operar efectivamente en la identificación de criminales y situaciones. En otro nivel, puede haber una tendencia a aceptar de manera acrítica proposiciones presentadas por expertos como lecturas que otros operadores no son capaces de realizar sobre productos tecnológicos. De manera que sobre una misma identificación de un rostro en una imagen se corre el doble riesgo de aplicar un algoritmo "llave en mano" no evaluado, y también sumarle luego el conocimiento de "expertos" que pueden no haber sido puestos a prueba con procedimientos claramente reglados para conocer sus capacidades reales. En ambos casos puede haber determinismo tecnológico si se considera que la tecnología, y los expertos en interpretarla, tienen la capacidad de resolver por sí solos una serie de problemáticas (Lyon, 2010).

Partiendo de la base de que no hay método forense, con excepción del uso de ADN, que haya logrado una rigurosa capacidad de demostrar una conexión entre evidencia y un individuo o fuente específica. Y la ausencia de estudios de validez y confiabilidad. Se puede decir que la admisión y las condenas no necesariamente prueban el valor de las tecnologías de vigilancia, ni sus interpretaciones algorítmicas o "expertas" para fines penales.

En este sentido, las agencias del sistema penal especializadas deberían tener protocolos fuertes en relación con la recolección, guarda y modificación de imágenes, en especial en formato digital. Para que la lectura de imágenes gane eficiencia sería necesario tener en cuenta ciertos factores distorsivos vinculados al ambiente de captura, características técnicas de captura, transferencia y reproducción, antigüedad y mejora de imágenes. Por otro lado, con respecto a determinar empíricamente la precisión y error de las interpretaciones de los expertos se debería evaluar su capacidad haciéndolos analizar una variedad de situaciones donde ya se conocen las respuestas correctas, y así determinar la validez y confiabilidad de sus opiniones.

El imperativo tecnológico porteño

Así como el fenómeno criminal o "criminalidad" no es una realidad natural, sino que es un entrecruzamiento de fenómenos culturales de conflictividad social y procesos de criminalización estatal. También es importante resaltar que la confiabilidad y la efectividad de las tecnologías son construcciones sociales disputadas por diversos intereses políticos y, por lo tanto, son coproducidas por distintos actores, instituciones, ideologías, prácticas y objetos. Mucho se puede hacer para mejorar la implementación de políticas, y mucho pueden refinarse las habilidades técnicas de los sistemas, pero no se puede evitar que sean objeto de una tensión política e interdisciplinaria. Por eso es fundamental que existan evaluaciones de efectividad de las tecnologías que apunten a evitar los "diálogos de sordos", y la coproducción de la fe en la eficiencia tecnológica. Y aquí es donde resulta importante mencionar lo que denomino el *imperativo tecnológico porteño*.

En el año 2016 la Legislatura porteña sancionó una nueva ley marco denominada "Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires" (Ley Nº 5688). Entre las novedades se destaca que crea como uno de los principios rectores del sistema de videovigilancia, la obligación de que el Estado promueva "el uso intensivo de nuevas tecnologías para el abordaje de sus funciones y la mejora de la gestión institucional" (Ley CABA Nº 5688, 2016, art. 477, inc. 2). Sin embargo, no establece la obligación de hacer estudios de impacto sobre la privacidad *ex ante*, de consultar a la población, ni tampoco de hacer evaluaciones de efectividad *ex post* sobre la utilidad de las tecnologías incorporadas. Como continuidad del modelo de "Ciudad Inteligente" que el Poder Ejecutivo porteño ha estado construyendo en la última década, la nueva ley establece que las soluciones tecnológicas en materia de vigilancia y seguridad son una prioridad, generando un patrón de dependencia que las jerarquiza sobre otras alternativas y valores, a la hora de gestionar la conflictividad social y direccionar el presupuesto. En pocas palabras, la ideología del eficientismo tecnológico aplicado a la seguridad se ha institucionalizado en un mandato positivo, facilitando que la amplificación de escala y funciones de las tecnologías de vigilancia masiva corran el riesgo de volverse una estrategia de gobierno en sí misma.

Citando este imperativo tecnológico en sus fundamentos, el Poder Ejecutivo aprobó la Resolución Nº 398/MJyS/2019, creando el Sistema de Reconocimiento Facial de Prófugos (en adelante SRFP) en abril de 2019, para identificar en la vía pública a personas con requerimiento judicial que forman parte de la base de datos del Sistema de Consulta Nacional de Rebeldías y Capturas (en adelante CoNaRC), creado por Decreto PEN N° 346/09. Los cimientos institucionales sobre los que se implementó esta política no fueron sólidos. Así lo expresó el Relator de Privacidad de las Naciones Unidas, Joseph Cannataci, luego de diagnosticar esta política durante su visita a la Argentina en el mes de mayo de 2019. Concretamente, en su informe le señaló al Poder Ejecutivo que no realizó estudios de impacto previos, ni supo demostrar la necesidad y proporcionalidad del sistema. Le

señaló al Poder Judicial que no actualiza el listado CoNaRC, que incluye menores de edad y casos de delitos menores. Y también le señaló al Congreso Nacional y la Legislatura porteña que debían sancionar una ley específica, dado que "las evaluaciones de impacto en la privacidad deberían ser obligatorias por ley como requisito previo para el despliegue de todas las tecnologías de vigilancia"[14]. De manera que los problemas de legalidad y legitimidad del SRFP aparecen como coproducidos por los tres poderes del Estado porteño.

Estas debilidades no tardaron en generar problemas concretos de vulneración de derechos. Entre las primeras detenciones muchos casos correspondían a requerimientos judiciales que habían perdido vigencia pero aún estaban vigentes en la base de CoNaRC. Este problema fue denunciado por la Defensoría del Pueblo de la CABA cuando, en agosto de 2019, remitió a la Corte Suprema de Justicia de la Nación un oficio con los resultados preliminares de su auditoría[15]. En el mismo señaló que el SRFP "derivó en vulneraciones de derechos fundamentales de las personas, como la libertad", porque verificaron que hubo "interceptación de ciudadanos que finalmente no resultaron ser las personas requeridas judicialmente" (subrayado original), ya sea porque "los números de documentos (DNI) eran erróneos" (subrayado original) u otras "inconsistencias entre los datos que el sistema contiene y las personas con requerimientos judiciales en cuestión"[16]. Entre ellos se destaca el caso de "Guillermo Federico Ibarrola", quien llegó a estar detenido de manera arbitraria durante seis días[17]. Por lo cual le recomendó a la máxima autoridad judicial del país que todos los juzgados bajo su jurisdicción tomen las medidas necesarias para subsanar y corregir estos errores.

De la información que surge de un pedido de acceso a información pública realizado por el autor en el marco de esta investigación[18], se puede concluir que al día 25 de octubre de 2019 la efectividad del SRFP en función seguridad, o sea, para detener prófugos peligrosos en base a las alertas automáticas recibidas fue del 9% (336 personas). Lo que representó sólo un 1% del total del CoNaRC. Mientras que la efectividad del SRFP para vulnerar derechos, o sea, para retener arbitrariamente personas que no estaban o no debían estar en el CoNaRC fue del 4% (145 personas), un 2% (81) por error del Poder Ejecutivo y otro 2% (64) por error del Poder Judicial.

---

[14] ACNUDH (2019). *Declaración a los medios de comunicación del Relator Especial sobre el Derecho a la Privacidad, al concluir su visita oficial a la Argentina del 6 al 17 de mayo de 2019*. Recuperado el 10 de febrero de 2020 de: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=24639&LangID=S.

[15] Irregularidades en el Sistema de Reconocimiento Facial. Sitio web de la Defensoría del Pueblo de la CABA. 21 de agosto de 2019. Recuperado el 10 de febrero de: http://www.defensoria.org.ar/noticias/irregularidades-en-el-sistema-de-reconocimiento-facial-la-defensoria-presento-un-informe/

[16] Entre otras, mencionan las denuncias registradas en los trámites N° 14122/19, 16759/19, 18437/19, 19276/19, 19426/19, 21470/19.

[17] Pasó casi una semana preso por un error policial. Clarín. 2 de agosto de 2019. Recuperado el 10 de febrero de 2020 de: https://www.clarin.com/policiales/paso-semana-preso-error-policial-sistema-reconocimiento-facial_0_6KiuCu0fy.html

[18] Nota NO-2019-34687512-GCABA-DGEYTI del Gobierno de la Ciudad de Buenos Aires del día 7 de noviembre de 2019, Expte. N° 2019-31085437-GCABA-DGSOCAI, Ley N° 104.

En parte esto se explica en que *"el índice de precisión aceptable definido por el MJyS* [Ministerio de Justicia y Seguridad] *es de 95% en relación con la operatividad del Sistema de referencia"*[19]. Esto significa que, sin una normativa del Poder Legislativo ni del Ejecutivo, el Gobierno porteño define deliberada y extralegalmente como aceptable un 5% de margen de error, que implica la retención/detención arbitraria de cientos de personas por año.

Como puede observarse, la efectividad del SRFP en función seguridad fue baja (9%) y muy cercana a la efectividad del SRFP para realizar retenciones/detenciones arbitrarias (4%). Al mismo tiempo, el SRFP en función judicial mostró una eficacia que alcanzó sólo el 45% (1695) en las 3811 alertas recibidas, esto significa que de cada dos alertas enviadas por el *software*, la Policía de la Ciudad tuvo capacidad operacional para interceptar a sólo una de las personas identificadas.

En lo que respecta a los aspectos anticipatorios del sistema, también es importante señalar que la resolución ministerial citada tiene dos omisiones importantes que abren la puerta a un uso desregulado de esta tecnología de vigilancia:

En primer lugar, en el expediente de contratación de la empresa proveedora queda claro que el GCBA adquirió un SRC que envía alertas automáticas en caso de comportamientos predefinidos como de riesgo potencial. Concretamente, envía alertas si una persona está "comportándose de una manera sospechosa"[20], o con actitud de "merodeo"[21], si una persona ingresa en "una zona estéril definida previamente"[22], entre muchas otras cosas. Sin embargo, en la resolución regulatoria no hay ninguna mención de esto. Esto significa que el CCTV está expandiendo sus funciones anticipatorias sin marco legal regulatorio específico.

En segundo lugar, la resolución menciona que los rostros de las personas buscadas son extraídos a través del "Sistema Federal de Identificación Biométrica para la Seguridad" (SIBIOS), creado por el Poder Ejecutivo Nacional mediante el Decreto N° 1766/11, "en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad". El SIBIOS es un sistema que permite a todas las agencias de seguridad del país acceso de consulta parcial en tiempo real[23] a la base nacional centralizada de datos biométricos de toda la población argentina, en manos del Registro Nacional de las Personas (ReNaPer). A nivel internacional, estas bases

[19] Ib Ídem.

[20] "Pliego de bases y condiciones particulares de contratación directa de un servicio de análisis integral de video" - PLIEG-2019-10400885-GCABA-SSGA – Expte. N° 2019-09774230-DGAYCSE - pág. 41.

[21] Ib Ídem.

[22] Ib Ídem, pág. 40.

[23] Si bien las policías no pueden acceder a toda la base, sino realizar consultas particulares, la escasa regulación del sistema no impide la creación de convenios específicos para un uso más extendido de la misma en función de que el SRF pueda realizar el aprendizaje necesario para adaptarse a las características fenotípicas de la población del país.

biométricas nacionales y centralizadas han despertado debates acerca de su constitucionalidad. Son pocos los países que cuentan con ellas, algunos las crearon y las eliminaron por ley (Inglaterra[24] y Francia[25]) y, dentro de los países que las crearon, no todos permiten su uso para fines policiales. Si bien en el anexo de la resolución Nº 398/MJyS/2019 el GCBA aclara que "salvo orden judicial, se encuentra prohibido incorporar imágenes y registros de otras personas que no se encuentren registradas en el CoNaRC", del pliego del expediente de contratación queda claro que el gobierno adquirió tecnología con la intención de "trabajar con base de datos indexadas manejando más de diez millones (10.000.000) de rostros a modo de contar con una búsqueda veloz"[26]. Si bien hasta el momento no se ha encontrado evidencia de que el gobierno nacional haya facilitado durante el año 2019 el uso de la base nacional de datos biométricos para el aprendizaje del SRF del gobierno porteño, se observa un claro desfajase entre la finalidad del sistema expresada en la normativa, y las capacidades técnicas solicitadas y obtenidas por el Estado porteño.

Teniendo en cuenta el bajo rango de las normativas con las cuales se han estado implementando políticas como el SIBIOS y el SRFP; la ideología eficientista plasmada en el mandato legal de seguir sumando y actualizando tecnología digital sin condiciones normadas; que el Poder Ejecutivo porteño se ha propuesto duplicar el actual parque de videocámaras fijas, móviles y aéreas; y que la ley de seguridad permite la incorporación de videocámaras privadas a la red pública policial; se puede pensar que son elevadas las probabilidades de que ocurra un incremento de escalas, funcionalidades y finalidades sin debate en la Legislatura porteña, ni en el Congreso Nacional. Y si este escenario es posible en la CABA, que cuenta con un marco regulatorio integral de videovigilancia desde el año 2007, podríamos presuponer que los riesgos son aún mayores en las provincias que aún no cuentan con uno, donde la mayoría de los CCTV continúan anómicos, o con escasos controles municipales.

[24] Por motivos vinculados a la privacidad y la seguridad nacional, en el año 2010 el Parlamento Británico sancionó el "Identity Documents Act 2010" para abrogar la "Identity Cards Act 2006" (Ley de tarjetas de identidad 2006 – traducción propia), ordenando la destrucción del Registro Nacional de Identidad (en Inglés *National Identity Register*) y la deshabilitación de todas las tarjetas de identidad digitales entregadas hasta ese momento.

[25] En 2012 el Consejo Constitucional de Francia declaró, mediante la Sentencia n° 2012-652 DC, la inconstitucionalidad parcial de la "Loi relative à la protection de l'identité" (Ley de protección de identidad – Traducción propia) en lo respectivo a la creación de una base nacional de datos biométricos, por considerar que "atentan contra el derecho al respeto de la vida privada" y que "no puede ser considerado como proporcionado al fin perseguido". En el año 2016 el Estado francés hizo otra contramarcha. El Poder Ejecutivo aprobó el decreto del N° 2016-1460, y desde el año 2018 se encuentra en funcionamiento una base biométrica nacional que continúa recopilando la biometría de la población.

[26] "Pliego de bases y condiciones particulares de contratación directa de un servicio de análisis integral de video" - PLIEG-2019-10400885-GCABA-SSGA – Expte. N° 2019-09774230-DGAYCSE - pág. 40.

Conclusiones

Nuestras sociedades se organizan cada vez más entorno a la tecnología. Esto significa que no es sólo un medio, sino un entorno de nuestro modo de vida. Más allá de las intenciones de quienes las usan, la tecnología va estructurando el mundo cada vez que se decide usar cierta tecnología sobre otra, lo que nos va definiendo, dando forma a nuestros valores y condicionando elecciones futuras, que también estarán impregnadas tecnológicamente. Si tenemos en cuenta que en nuestras sociedades son pocas las grandes decisiones que pueden tomarse por fuera del marco de los límites técnicos y económicos, el poder tecnológico se ha vuelto "la forma principal de poder en la sociedad" (Feenberg, 2012 [2000]:40).

En este contexto es absolutamente comprensible que las políticas de seguridad estatales, el poder de coacción del Estado, sean cada vez más dependientes de desarrollos tecnológicos. No resulta problemático o negativo producir soluciones técnicas a problemas de seguridad, más bien lo contrario, algunas tecnologías han resultado muy importantes para aumentar la planificación estratégica, el sistema de emergencias, y el control de las agencias policiales. Lo que sí resulta problemático es que la ideología eficientista se vuelva un imperativo excluyente, bajo el supuesto de que la mediación técnica es la única e inmejorable solución posible, porque facilitaría mayores beneficios con menor esfuerzo. O que incluso se vuelva un imperativo moral, bajo la idea de que la eficiencia es "hacer lo correcto del modo correcto" (Ibarra: 2014:16)[27]. Si bien es legítimo y positivo pretender lograr mayor eficiencia y eficacia en el cumplimiento de objetivos, aplicar el principio de que "cuanto más se puede ver, más queremos ver" (Lyon, 2010:135, traducción propia), podría también fomentar muy eficazmente la vulneración de derechos humanos de una manera difícil de revertir.

Con las nuevas tecnologías de vigilancia digital automatizada de datos a gran escala, se abre la posibilidad de intervenciones policiales anticipatorias en función de seguridad y de investigación penal. La anticipación securitaria es un proceso de radicalización de la prevención situacional/ambiental del delito, cuyo fin último es convertir en sospechosos vitalicios a todos los *individuos* de una sociedad, y a sus datos personales biométricos (los *dividuos*) en objeto de prueba para delitos que aún no se cometieron. Incorporar (y dejar incorporar) tecnologías de vigilancia y rastreo masivo de manera acrítica nos lleva a un curioso tipo de democracia basada en la desconfianza de los gobiernos sobre sus gobernados, en la creciente opacidad de los primeros y la creciente transparencia de la vida de los segundos; y en la creciente confianza en reglas algorítmicas que pueden funcionar, pero no sabemos bien por qué, cómo, o para qué. La videovigilancia

[27] Así definió el concepto de eficiencia quien fuera Ministro de Modernización del GCBA y de la Nación, principal responsable de los proyectos de Ciudad Inteligente.

automatizada es heredada de usos bélicos, más enfocada en identificar potenciales objetivos humanos, que ciudadanos a los que se debe proteger. Los algoritmos no pueden decidir qué datos son relevantes para construir acciones morales informadas, y clasifica nuestros movimientos de manera binaria en "permitidos" o "sospechosos". Esto podría abrir la puerta a "detenciones inteligentes" (Pérez Esquivel, 2017), que se conviertan (intencionalmente o no) en una nueva variante de detenciones arbitrarias en las que el Estado disimula su accionar arbitrario a través de la "delegación" de responsabilidades en los objetos técnicos. Todos estos elementos deberían abrir debates profundos en materia de constitucionalidad y construcción democrática de la ciudadanía.

En los países en donde el desarrollo de la videovigilancia automatizada está más expandido, no sólo hay regulaciones específicas para limitar abusos de poder[28], sino que hoy nos encontramos con reacciones que apuntan a suspenderla o prohibirla. En este sentido, no sólo es importante el GDPR europeo, sino también lo que está ocurriendo en los Estados Unidos de América, uno de los países con bases de datos biométricos más grandes del mundo. En el año 2019 muchos estados y ciudades comenzaron a sancionar leyes que establecen moratorias (California) e incluso prohibiciones (San Francisco, Oakland, Somerville, Berkeley, Cambridge, Alameda, Northampton, Brookline) en materia de SRF policial. Mientras que muchos otros se encuentran discutiendo proyectos de ley para limitarlos o prohibirlos para su uso público y/o privado (Maryland, Massachusetts, Nebraska, New Hampshire, New York, Vermont y Washington)[29]. Interesantes ejemplos de que la instrumentalización tecnológica no es tan neutral como parece, ni fruto de un supuesto patrón evolutivo de progreso técnico lineal, inmutable y común a todas las sociedades, en el cual los factores políticos e ideológicos no podrían influir. O, en otras palabras, ejemplos de que las mediaciones tecnológicas de las relaciones de poder social pueden ser sacadas a la luz y cuestionadas, de ser necesario.

En este recorrido, el derecho a la privacidad e intimidad han perdido terreno frente a propuestas de vigilancia de la sociedad que se presentan como protectoras de la comunidad. Esto se debe a que han sido tratados principalmente como un derecho individual negativo que delimita el dominio público del privado. O sea, como la expresión de individuos atomizados que no quieren que el Estado se meta en sus cosas. Sin embargo, paulatinamente, la privacidad, la intimidad y la autonomía informativa están adquiriendo un sentido cada vez más colectivo y positivo para el bien común democrático, lo que puede favorecer un cambio en la definición de políticas públicas, normativas y

[28] Vale destacar la utilidad del modelo de regulación de SRF creado por el Centro de Privacidad y Tecnología de la Universidad de Georgetown. "The perpetual Line-Up. Unregulated Police Face Recognition in America" ("La rueda de reconocimiento perpetua. Reconocimiento facial policial no regulado en Estados Unidos" – Traducción propia). Recuperado el 10 de febrero de 2020 de: https://www.perpetuallineup.org/.

[29] Para más información consultar el Centro de Privacidad y Tecnología de la Universidad de Georgetown: https://www.law.georgetown.edu/privacy-technology-center/.

sus interpretaciones (Regan, 2018; Van Der Sloot, 2018; Nissembaun, 2011). Incluso más, por la interdependencia que tienen entre sí los derechos humanos, hay casos que demostraron que debilitar la privacidad puede ser sinónimo de debilitar la seguridad (Pérez Esquivel, 2019). Más aún si tenemos en cuenta que ninguna tecnología está exenta de errores o vulnerabilidades, al igual que ninguna política pública está exenta de errores humanos. De manera que, además, el fortalecimiento de la privacidad y la intimidad también puede ser una forma de construir seguridad.

Bibliografía

Armitage, R. (2002). *To CCTV or not to CCTV?: A review of current research into the effectiveness of CCTV systems in reducing crime*. Reino Unido: Nacro. Recuperado el 10 de febrero de 2020: http://epic.org/privacy/surveillance/spotlight/0505/nacro02.pdf.

Ashby, M.P.J (2017). The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis. *Eur J Crim Policy Res* 23, 441–459. https://doi.org/10.1007/s10610-017-9341-6.

Bruno, F. (2013). *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina.

Carli, V. (2008). *Valoración de la videovigilancia como una herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes*. Montreal: Centro Internacional para la Prevención de la Criminalidad. Recuperado el 10 de febrero de 2020: http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/Valoracion_del_CCTV_como_una_Herramienta_efectiva_de_manejo_y_seguridad_ESP.pdf.

Carroll-Mayer, M., Fairweather, B. y Carsten Stahl, B. (2008). CCTV Identity Management and Implications for Criminal Justice: some considerations. *Surveillance and Society, 5* (1), 33-50. Recuperado el 10 de febrero de 2020 de: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3438.

Comisión Interamericana de Derechos Humanos-CIDH- (2009*). Informe sobre seguridad ciudadana y derechos humanos*, OEA/Ser.L/V/II. Doc.57. Washington DC: OEA.

Cusson, M. (2005). La surveillance et la télésurveillance: sont-elles efficaces?. *Revue internationale de criminologie et de police technique et scientifique*, *58* (2), 131-150. Recuperado el 10 de febrero de 2020 de: http://classiques.uqac.ca/contemporains/cusson_maurice/surveillances_et_telesurveillances/surveillances_et_telesurveillances.pdf.

Dammert, L. y Silva, A. (2018). *Seguridad y tecnología en América Latina: Experiencias y desafíos*. Santiago de Chile: USACH. Recuperado el 10 de febrero de 2020 de: https://www.researchgate.net/publication/328602570_Seguridad_y_Tecnologia_en_America_Latina_Experiencias_y_Desafios.

Ditton, J. (2000). Crime and the city: Public attitudes towards open-street CCTV in Glasgow. *British Journal of Criminology*, *40* (4), 692-709.

Edmon, G. y San Roque, M. (2013). "Justicia's Gaze: Surveillance, Evidence and the Criminal Trial. *Surveillance and Society, 11* (3), 252-271. Recuperado el 10 de febrero de 2020 de: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/justicia.

Feenberg, A. (2012 [2000]). *Transformar la tecnología. Una nueva visita a la teoría crítica*. Bernal: UNQ.

Garibaldi, G. E. L. (2010). *Las modernas tecnologías de control y de investigación del delito*. Buenos Aires: Ad-Hoc.

Gill, M., and Spriggs, A. (2005). *Assessing the impact of CCTV*, Vol. 292. London: Home Office Research, Development and Statistics Directorate. Recuperado el 10 de febrero de 2020: https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf.

Ibarra, A. (2014). La innovación es posible cuando la creatividad se une a las posibilidades de las nuevas tecnologías de información y comunicación. En E. N. Martelli, P. Clusellas, M. J. Martelo, *Gestión documental electrónica* (pp. 15-16). CABA: Secretaría de Gobierno de la CABA.

Increasing Resilience in Surveillance Societies – IRIIS (2012). Deliverable D1.1: Surveillance, fighting crime and violence. Programa FP7-SSH-2011-2, Unión Europea.

Introna, L. D. y Nissenbaum, H. (2009). *Facial Recognition Technology: A Survey of Policy and Implementation Issues*. July, 22. Center for Catastrophe Preparedness and Response, New York University. Recuperado el 10 de febrero de 2020 de: http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

Introna, L. D. y Wood, D. (2004). Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance and Society, 2* (2/3), 177-198.

Kanashiro, M. (2008). Surveillance Cameras in Brazil: exclusion, mobility regulation, and the new meanings of security. *Surveillance & Society*, *5* (3), 270-289.

Lyon, D. (2010). 11 de Setembro, sinóptico e escopofilia: observando e sendo observado. En F. Bruno y otros (Comps.), *Vigilância e Visibilidade. Espaço, tecnologia e identificação* (pp. 115-140) Porto Alegre, Sulina.

_____ (2002). Surveillance Studies: understanding visibility, mobility and the phenetic fix. *Surveillance and Society*, *1* (1), 1-7. Recuperado el 10 de febrero 2020 de: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3390/3353.

Melgaço, L., Verfaillie, K. y Hildebrandt, M. (2013). CCTV and Smart CCTV effectiveness: a meta-level analysis. *SIAM-Security Impact Assessment Measures. Brussel: Vrije Universiteit Brussel*, 20. Recuperado el 10 de febrero de 2020: https://www.researchgate.net/publication/274077700_CCTV_and_Smart_CCTV_effectiveness_a_meta-level_analysis.

Nissembaun, H. (2011). *Privacidad Amenazada.Tecnología, política y la integridad de la vida social*. México DF: Océano de México.

Pérez Esquivel, A. (2019). *Los usos políticos de los Circuitos Cerrados de TV en la Ciudad Autónoma de Buenos Aires, y sus efectos en los derechos y garantías de sus habitantes 2010-2015*. Tesis de Maestría. Universidad Nacional de San Martín, Argentina y Universidad de Georgetown, Estados Unidos de América. Recuperado el 10 de febrero de 2020 de: https://ri.unsam.edu.ar/handle/123456789/1096

_____ (2017). Ciudades inteligentes, biometría y detenciones arbitrarias. Ponencia presentada en *Jornadas APP/ADA Desafíos actuales de la justicia porteña: Autonomía e igualdad*, Facultad de Derecho, Universidad de Buenos Aires. Recuperado el 10 de febrero de 2020 de: http://www.adaciudad.com.ar/docs/Perez-Esquivel-Ciudades-inteligentes-biometr%C3%ADa-y-detenciones-arbitrarias.pdf

Perry, W. L., McInnis B., Price, C. C, Smith, S. C, y Hollywood, J. S. (2013). *Predictive policing. The role of crime forecasting in law enforcement operations*. Estados Unidos: Rand Corporation.

Regan, P. (2018). Legislating Privacy: Technology, Social Values, and Public Policy. En B. Van der Sloot y A. De Groot (Eds), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (pp. 63-136). Amsterdam: Amsterdam University Press. Recuperado el 10 de febrero de 2020 de: https://www.jstor.org/stable/j.ctvcmxpmp.5.

Rennó, R., Milanes, V., Peña, P. y Velasco, P. (2017). Ciudades inteligentes en Latinoamérica, el ciudadano vigilado. En C. Ríos, A., A. Pérez Esquivel, L. Lacaze y L. Albuquerque (Comps.)

¿Nuevos paradigmas de vigilancia? miradas desde América Latina: Memorias del IV Simposio Internacional Lavits, Buenos Aires, 2016 (pp. 213-218). Córdoba: Fundación Vía Libre. Recuperado el 10 de febrero de 2020 de: https://www.researchgate.net/publication/319482813_CIUDADES_INTELIGENTES_EN_LATINOAMERICA_EL_CIUDADANO_VIGILADO.

Smith, G. (2004). Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK, Surveillance and Society, *2* (2/3), 376-395. Recuperado el 10 de febrero de 2020 de: http://www.surveillance-and-society.org/articles2(2)/screens.pdf.

Ugarte, J. M. (2012). Hacia una doctrina de inteligencia criminal. *Cuadernos de Seguridad*, (15), 79-112. CABA: Ministerio de Seguridad de la Nación.

Valentine, T. (2015). *Forensic Facial Identification: Theory and Practice of Identification from Eyewitnesses, Composites and CCTV*. Reino Unido: John Wiley & Sons.

Van Der Sloot, B. (2018). Privacy from a Legal Perspective. En *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (pp. 63-136). Amsterdam: Amsterdam University Press. Recuperado el 10 de febrero de 2020 de: https://www.jstor.org/stable/j.ctvcmxpmp.6.

Webster, W. (2004). The diffusion, regulation and governance of closed-circuit television in the UK. *Surveillance & Society*, *2* (2/3), 230-250.

Welsh, B. C. and Farrington, D. P. (2003). Effects of closed-circuit television on crime. *The Annals of the American Academy of Political and Social Science*, *587* (1), 110-135.

Fuentes periodísticas consultadas

Garvie, C. (2019). You're in a Police Lineup, Right Now. New York Times. Recuperado el 10 de febrero de 2020: https://www.nytimes.com/2019/10/15/opinion/facial-recognition-police.html?smtyp=cur&smid=tw-nytopinion.

"Facial recognition wrongly identifies public as potential criminals 96% of time, figures reveal" ("El reconocimiento facial identifica erróneamente al público como posibles delincuentes el 96% de las veces, según revelan las cifras" – Traducción propia). (7 de mayo de 2019). *Independent*. Recuperado el 10 de febrero de 2020 de: https://www.independent.co.uk/news/uk/home-news/facial-recognition-london-inaccurate-met-police-trials-a8898946.html.

"The Best Algorithms Struggle to Recognize Black Faces Equally". ("Los mejores algoritmos luchan por reconocer las caras negras en igualdad" – Traducción propia) (22 de julio de 2019). *Wired*. Recuperado el 10 de febrero de 2020 de: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.

Pasó casi una semana preso por un error policial. Clarín. 2 de agosto de 2019. Recuperado el 10 de febrero de 2020 de: https://www.clarin.com/policiales/paso-semana-preso-error-policial-sistema-reconocimiento-facial_0_6KiuCu0fy.html