Jornadas “Desafíos actuales de la Justicia porteña: Autonomía e Igualdad”

29, 30 y 31 de mayo de 2017. Facultad de Derecho, Universidad de Buenos Aires.

Ciudades inteligentes, biometría y detenciones arbitrarias

ANDRÉS PÉREZ ESQUIVEL

Eje temático: Control de agencias estatales sobre espacios públicos

Ciudades inteligentes, biometría y detenciones arbitrarias

Por **ANDRÉS PÉREZ ESQUIVEL**

Eje temático: Control de agencias estatales sobre espacios públicos.

Resumen: La ley nacional Nº 23.950, las normativas y jurisprudencia equivalente que permiten a los agentes policiales interceptar, bajo presunción de *peligrosidad*, la libre circulación de ciudadanos, y privarlos de libertad por horas en una comisaría en caso de no acreditar su identidad, son herederas de una tradición de detenciones ilegales y arbitrarias para el disciplinamiento social.

Mientras esta ley es un mecanismo legal-jurídico de poder, cuestionable desde su propio carácter legal-jurídico por ser contraria a la Convención Americana de Derechos Humanos, y por lo tanto parte de nuestra Constitución. Los jueces actúan más en función de que los agentes de la policía respeten las formalidades posteriores a la detención, que en función de determinar si existían las razones excepcionales que constitucionalmente deben verificarse para aceptar la injerencia en la libertad individual (Martín, 2010).

En poco tiempo los más de 44 millones de argentinos habremos obtenido el nuevo Documento Nacional digital de Identidad. Esto significa que nuestros datos biométricos habrán sido recolectados, digitalizados y luego centralizados en una sola base de datos del Registro Nacional de las Personas (RENAPER) al cual pueden acceder todas las policías del país en el marco del Sistema Federal de Identificación Biométrica (SIBIOS), creado para fines de seguridad pública por el Decreto PEN Nº 1766/11. Esto significa que las agencias policiales federales y provinciales hoy pueden realizar una identificación inmediata y remota de los individuos mediante una captura fotográfica del rostro o con la toma de huellas dactilares en dispositivos itinerantes que, al ser contrastadas en línea con la base de datos federal, permite obtener la identidad del individuo en cuestión.

Esta iniciativa y ciertos proyectos legislativos, apuntan a saldar la responsabilidad internacional de la Argentina sobre la vigencia de las detenciones arbitrarias de la Ley Nº 23.950 y equivalentes, argumentando que estos avances tecnológicos volverían innecesarios los procedimientos de detención. Más aún, si se tiene en cuenta el creciente paradigma de ciudades inteligentes y seguras, donde la conectividad es el eje central para una conciencia situacional basada en el intercambio rápido de información con centros de comando y control, y con sistemas y bases de datos múltiples.

En este trabajo introduciré a parte de la investigación que estoy realizando sobre cómo la posibilidad de aplicar tecnología digital para saldar una cuestión de derecho, puede abrir las puertas a una variante cualitativa de estas detenciones arbitrarias que, ante la falla contingente

(intencional o no) de los dispositivos digitales, sería capaz de disimular la histórica arbitrariedad policial detrás de una conjugación de supuesta neutralidad científico-tecnológica y de azar.

Ciudades Inteligentes

Las Ciudades Inteligentes (o digitales) son el resultado de dos procesos sociales internacionales centrales y simultaneos, y no excluyentes:

Por un lado el aumento de la cantidad y proporción de población urbana. Hoy más de la mitad de la población mundial vive en zonas urbanas, rondando los 3900 millones, y Naciones Unidas (2014) estima que en 2050 esta cifra ascenderá a 6.300 (un 65% de la población mundial estimada para ese año).

Por otro lado, el aumento de usuarios de internet y de dispositivos con acceso a internet. En el año 2000 había 400 millones de usuarios de internet y en 2015 ya alcanza los 3 mil 200 millones de usuarios en el mundo. Para fines de 2015 ya había más de 7 mil millones de suscripciones de teléfonos celulares y la proporción de población cubierta por la red de telefonía mobil 2G creció de 58% en 2001 a 95% en 2015. Mientras que el 89% de las poblaciones urbanas ya tienen cobertura 3G -unos 4 mil millones- (ITU; 2015).

Hoy se están incorporando dispositivos a la red con un ritmo más acelerado que el crecimiento de la población mundial, abriendo paso a lo que se ha dado en llamar *internet de las cosas*. Hablar de ciudad inteligente implica, entonces, definiciones políticas en materia de regulaciones de: comunicaciones, espectro, gestión de residuos de aparatos electrónicos, estándares abiertos y software público, neutralidad de la red, gobernanza de internet, delitos informáticos, seguridad de las TIC, servicios de *La Nube,* internet de las cosas, producción y uso de energía, régimen de importación y exportación, *Big Data*, *Ojo Satelital,* yciber crimen. Así como también de nuevas pautas de interacción social y con el medio urbano de la mano de tecnologías emergentes emblemáticas, tales como dispositivos inteligentes (teléfonos, tablets, televisores, heladeras, lavarropas, entre los más populares); Drones (robots diversos); impresoras 3D; aplicaciones peer to peer (uber, task rabbit, etc.); edificios ecosustentables; Circuitos Cerrados de TV (CCTV); identificación y/o transferencias monetarias por radio frecuencia (ej. tarjetas sube), etc.

En la actualidad se reconocen cientos de proyectos de "ciudad inteligente". Según las estimaciones especializadas entre 2015 y 2019 el monto total de inversiones que acarrearán las tecnologías de internet de las cosas ascenderá a 97 mil millones de dólares[1]. Hasta hace pocos

1 "The Internet of Things is poised to create hundreds of billions of dollars in economic value for cities worldwide", 28 de julio de 2015, Business Insider. Disponible en línea en: http://www.businessinsider.com/internet-of-things-to-create-hundreds-of-billions-in-economic-value-for-cities-2015-7?op=1

años Europa y Estados Unidos estaban a la cabeza con cerca de medio centenar cada uno, pero la decisión de la India[2] de construir 100 ciudades inteligentes obligan a redibujar el mapa.

Ciudades Seguras

Dentro del paradigma de ciudades inteligentes ha surgido un abordaje sectorial ligado a la seguridad ciudadana. En 2011, con apoyo oficial de la Comunidad Europea se constituyó en Europa un consorcio público-privado denominado *Safe City*, para impulsar desarrollos conjuntos entre organismos de investigación y empresas de distintos paises. Según este consorcio el pilar principal para construir ciudades inteligentes es mejorar la seguridad pública (García: 2012).

"Para esta iniciativa europea, el propósito operacional es construir un modelo de recolección, intercambio y análisis de datos que permita -en tiempo real- tomar decisiones informadas y brindar una respuesta inmediata a incidentes y emergencias. El núcleo de su enfoque apunta a obtener una conciencia situacional común de la realidad delictiva entre los niveles que monitorean y deciden en forma remota y aquellos que se encuentran y actúan en el terreno, aprovechando un intercambio rápido y seguro de información entre sistemas y bases de datos múltiples" (Sibilla; 2012: 211).

Esto ha motivado a muchos gobiernos alrededor del mundo a desplegar entramados de sensores remotos para detectar en forma temprana pérdidas de gas, incendios, choques, accidentes, delitos y diversos eventos en pos de desplegar una respuesta inmediata.

Estos componentes inteligentes son capaces de ejecutar múltiples tipos de acciones de acuerdo a su entorno y diseño y *"paulatinamente se irán borrando los límites operacionales que hoy conocemos con dispositivos que podrán, por ejemplo, dirigir su propia movilidad, adaptar su respectivo entorno, autoconfigurarse y automantenerse"* (Sibilla; 2012: 208).

Los servicios integrales en función de seguridad los brindan pocas corporaciones privadas en el mundo (IBM, Siemens, Cisco, Motorola, etc.). Una de ellas es la corporación japonesa NEC, hoy dueña en Argentina de la empresa que instaló los CCTV de la CABA, Mar del Plata, Lomas de Zamora, Tigre, La Plata, Bahía Blanca y Rosario, entre otras. Según su sitio web *"'Ciudades Seguras' es una parte integral de la visión de Ciudades Inteligentes de NEC, donde la gente puede vivir, trabajar y jugar con seguridad y comfort mientras también coesxiste en armonía con el medio ambiente. NEC ofrece tecnologías avanzadas y soluciones para volver esto una realidad"*[3]. Esta empresa ofrece sus servicios en 7 pilares: gestión de la información; cumplimiento de la ley; gestión de emergencias y desastres; administración de servicios públicos; colaboración interagencial; gestión de infraestructura crítica.

---

2 *"Cities of the future? Indian PM pushes plan for 100 'smart cities'"*, 18 de julio de 2014, CNN. Disponible en línea en: http://edition.cnn.com/2014/07/18/world/asia/india-modi-smart-cities/index.html

3 Web oficial de NEC: http://www.nec.com/en/global/solutions/safety/index.html

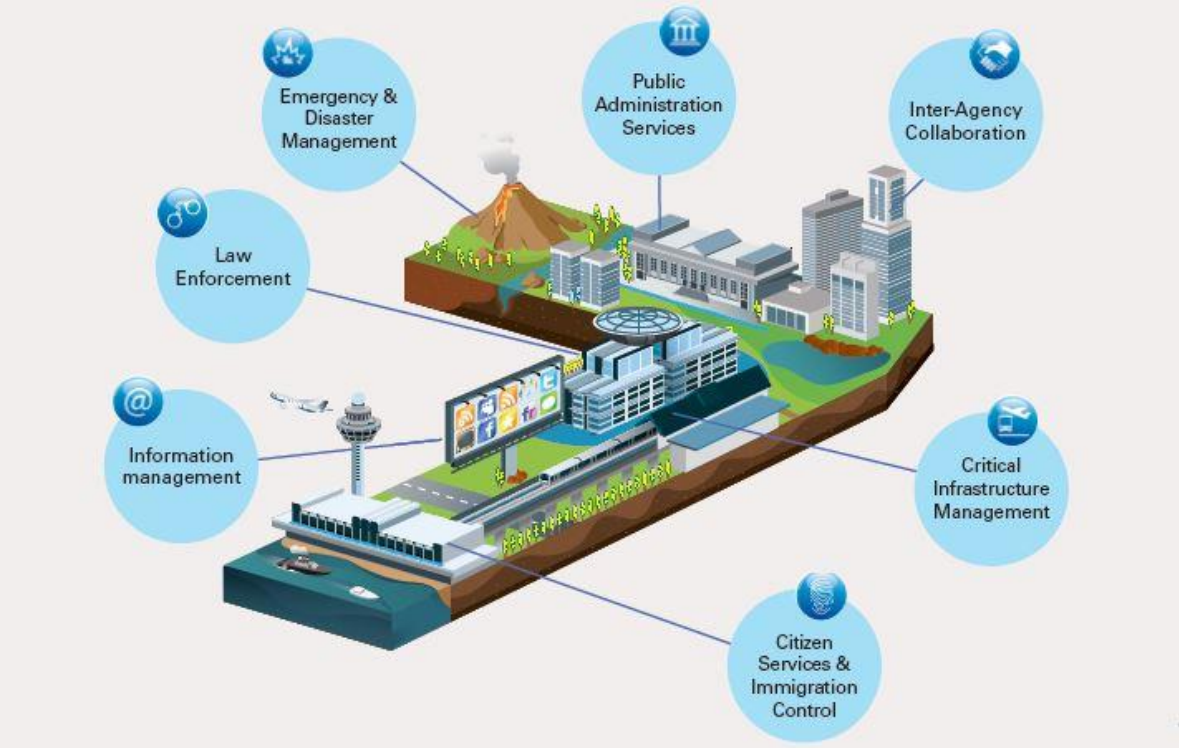

Imagen 1: Infografía extraída del sitio web de NEC.

Buenos Aires Ciudad Segura

La Ciudad Autónoma de Buenos Aires no sólo ha asumido explícitamente la identidad/proyecto de *Ciudad Inteligente*[4] sino que fue el primer distrito del país en conformar un *Ministerio de Modernización, Innovación y Tecnología* y una *Subsecretaría de Ciudad Inteligente* para lograr ese objetivo[5]. Esto la llevó a ocupar en 2014 el puesto número 28 en el ranking mundial de esta categoría, según un estudio de National Geographic[6].

En este marco, tanto las gestión porteña del partido Propuesta Republicana (PRO), como la administración nacional del Frente para la Victoria (FPV) con el Proyecto Buenos Aires Ciudad

4 Spot oficial promocional de *"Buenos Aires Ciudad Inteligente"*: https://www.youtube.com/watch?v=7JyGjN8TsDo

5 Web oficial del Gobierno de la Ciudad Autónoma de Buenos Aires: http://www.buenosaires.gob.ar/innovacion/ciudadinteligente.

6 "Buenos Aires, en el puesto 28 entre las ciudades más inteligentes del mundo", 29 de agosto de 2014, La Nación. Disponible en línea en: http://www.lanacion.com.ar/1722802-buenos-aires-entre-las-28-ciudades-mas-inteligentes-del-mundo

Segura (BACS)[7], implementaron en simultáneo a partir del año 2010 un despliegue de inversiones en tecnología para fines de seguridad en 6 niveles de infraestructura (García; 2012):

1. **Infraestructura urbana:** calles, parques, perímetros sensibles, espacios públicos en general de la Ciudad Autónoma de Buenos Aires

2. Sensores/Actuadores: Sensores fijos y móviles. Cerca de 4000 cámaras cámaras fijas en la vía pública de la Policía de la Ciudad de Buenos Aires (PCABA) en superficie y 360 en las estaciones de subterráneo. También cientos de cámaras de reconocimeinto de patentes.

Más de 500 de patrulleros inteligentes, que incluyen cámaras internas y externas al vehículo, además de un sistema de posicionamiento y geolocalización mediante GPS. Además de vehículos aéreos no tripulados, entre otras cosas.

Todo monitoreado desde los Centros de Comando y Control (CCC) de la PFA y el de la PM, hoy unificados en la Policía de la Ciudad de Buenos Aires.

3. Redes de entrada y acceso: Red inalámbrica Wi-Max (high mobility) para interconectar los patrulleros en movimiento con los CCC, permitiendo enviar y recibir video en alta velocidad, transmitir posición y trayectoria y procesar instrucciones en la consola de cada patrullero tecnológico.

4. Red central: Tendido de red de fibra óptica (GPON) de que interconecta los CCTV y las antenas de la red Wi-Max, los edificios del Ministerio de Interior, de Seguridad, de Gendarmería, Prefectura, Policía Federal y de la Ciudad.

5. Informática: Unidades de procesamiento centralizadas y distribuidas (fijas y móviles). Los CCC cuentan con *videowalls*, una mesa digital de situación que consolida toda la información relevante para la conducción estratégica operacional, etc.

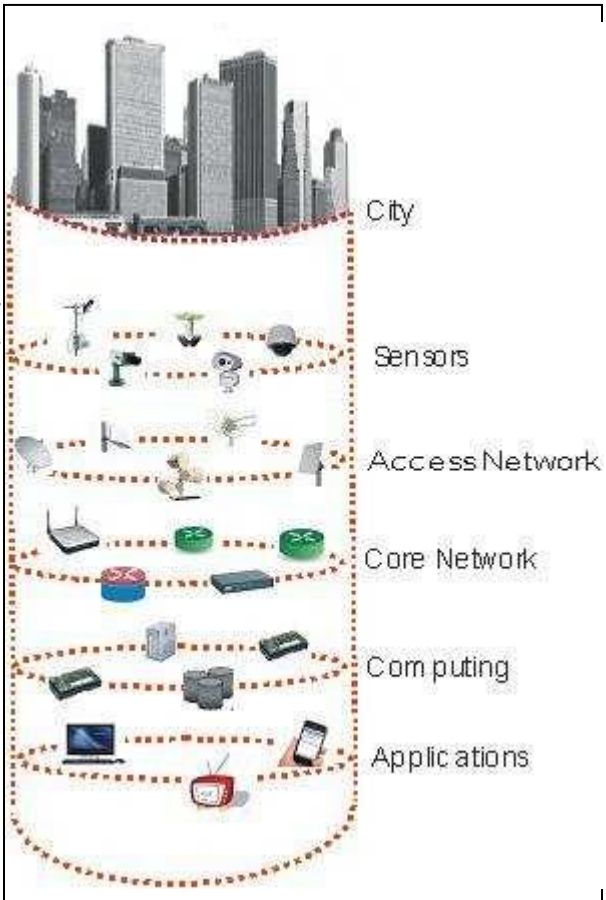

Imagen 2: Gráfico extraído de Sibilla (2012)

6. Aplicaciones: software de diseño propio para el registro protocolizado y auditable de eventos del sistema de llamadas de emergencia (911) (estándar NENA -National Emergency Numbers Association-). Sistemas CAD (Computer Aided Dispatch- despacho asistido por computadora-), AVL y trunking.

---

7 Sitio web oficial del programa BACS del Gobierno Nacional: http://911.ar/hoja/18241. Spot oficial promocional de *"Buenos Aires Ciudad Segura"*: https://www.youtube.com/watch?v=t9ocvm4A-UU

El espacio y ciber espacio urbano como arenas de disputa

Los centros urbanos se articulan y articularán siempre *"como una composición espacial de poder, de trabajo, de criterios de uso públicos y privados, y de gestión de sus diferentes indicadores."* (Mingolarra Ibarzabal; 2006: 12). Hoy la ciudad se ha instalado en el centro del debate de la constitución del sujeto actual, y bajo el paradigma de ciudad inteligente también se está redefiniendo el espacio público y el desarrollo democrático de la ciudadanía incorporando el ciber-espacio como arena de disputa de poder.

En su especificidad, las ciudades latinoamericanas siempre han tenido contrastes sociales muy marcados, en especial en momentos de crisis económica. La última fase de desarrolo urbano en la región desde los años 70's (Borsdorf; 2003), se ha caracterizado por la expansión de autopistas que acentuaron un esquema de fragmentación celular en escala pequeña. Así, un barrio de lujo hoy puede ser construído en una zona de pobreza, mediante el despliegue de modelos de barrios cerrados con murallas, elevado nivel de vigilancia, y un diseño espacial de inclusión/exclusión. Esto colabora en que el foco de políticas esté puesto más en los flujos y los puntos in (y no out) de la ciudad, que en un control territorial totalizante de la seguridad como era en otras épocas. Y en esas tareas las nuevas tecnologías juegan un papel central a la hora de redistribuir el poder de acceso.

El aumento de dispositvos para la recolección y procesamiento de información personal en pos de vigilar, monitorear y trazar la vida de los ciudadanos, hace que la vida urbana se convierta cada día más en un estilo de vida condicionado por una vigilancia total y permanente, conforme se incrementan y automatizan los artefactos estatales y privados, colectivos e individuales (hasta prendas de vestir), con capacidad de acceder a internet o de ser rastreables.

Esto ha generado que hasta el Banco Mundial advirtiera sobre el *"riesgo de que los Estados y las empresas puedan valerse de las tecnologías digitales para ejercer control sobre los ciudadanos y no para empoderarlos"* (Banco Mundial; 2016: 5). Y lo hace con razón, ya que el Director Nacional de Inteligencia de Estados Unidos, James Clapper, o sea, el máximo responsable de inteligencia del país con mayor poder de espionaje internacional demostrado en la historia de la humanidad, dijo en una audiencia frente al Senado de su país en febrero de 2016, que *"en el futuro los servicios de inteligencia podrían usar [internet de las cosas] para identificar, vigilar, monitorear, hacer trazabilidad, reclutamiento, ganar acceso a redes o credenciales de usuarios"*[8].

En este proceso de disputa de la urbanidad y el derecho a la ciudad, del que la Ciudad de Buenos Aires no escapa, debemos repensar las detenciones arbitrarias por averiguación de identidad de cara al actual proceso de gentrificación de la CABA (Di Virgilio; 2015) y sus consecuentes prácticas de "limpieza estética" de los centros turísticos; del fallo Vera[9] del Tribual

---

8 "US intelligence chief: we might use the internet of things to spy on you", 9 de febrero de 2016, The Guardian. Disponible en línea en: https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

9 "Vera, Lucas Abel s/ infr. art. 85, CC" Disponible en línea en:

Superior de Justicia; y de la nueva ley de seguridad pública N.º 5688 que, aunque con mayores restricciones, continúa legitimando en su artículo 91 las prácticas arbitrarias basadas en el *olfato policial* que aún se extienden a lo largo y ancho del país[10].

Detenciones arbitrarias contingentes

En el caso Bulacio *Vs.* Argentina del año 2003, además de otorgar responsabilidad internacional a la Argentina, la Corte Interamericana decidió que el Estado Nacional *"debe garantizar que no se repitan hechos como los del presente caso, adoptando las medidas legislativas y de cualquier otra índole que sean necesarias para adecuar el ordenamiento jurídico interno a las normas internacionales de derechos humanos, y darles plena efectividad..."*[11].

Pero tanto la Ley 23.950 como su reglamentación pueden considerarse inconstitucionales e inconvencionales porque no establecen condiciones de detención pormenorizadas y precisas sino más bien prescripciones genéricas e indefinidas[12]. *"En consecuencia a través de lo realizado u omitido por esos tres órganos del Estado argentino se ha continuado generando responsabilidad internacional por cientos de miles de privaciones de libertad arbitrarias e incluso también ilegales que la agencia policial efectuó y efectúa diariamente"* (Martín; 2010: 46).

Con el objetivo de saldar esta deuda fue creado en 2011 el Sistema Federal de Identificación Biométrica (SIBIOS), a través del Decreto PEN N.º 1667/11. Este sistema está recolectando en una base centralizada los datos patronímicos y biométricos de todos los argentinos para permitir que las agencias policiales federales y provinciales[13] pueden realizar una identificación inmediata y remota de los individuos mediante una captura fotográfica del rostro, o con la toma de huellas dactilares en dispositivos digitales itinerantes que, al ser contrastadas en línea con la base de datos federal, permite identificar *in situ* al individuo en cuestión. Hasta el momento cuenta con huellas de 16 millones argentinos, y han adherido todas las provincias excepto Córdoba y Formosa (ADC; 2017). Los fundamentos utilizados por el Gobierno Nacional fueron los siguientes: 1) Que resultaba *"…imprescindible usufructuar al máximo las herramientas tecnológicas en dotación, teniendo en cuenta que la utilización de técnicas biométricas resulta un aporte fundamental a las funciones de seguridad pública en materia preventiva y respecto de competencias de investigación y policía científica, conforme las*

---

http://www.pensamientopenal.com.ar/system/files/2016/01/fallos42743.pdf

10 Centro de Estudios Legales y Sociales, *Leyes que avalan la detención por averiguación de antecedentes o identidad en las distintas provincia y en el régimen federal*. Disponible en línea en: http://www.cels.org.ar/common/documentos/leyes_que_avalan_detenciones.pdf

11 Serie C No. 100 Corte IDH. Caso Bulacio Vs. Argentina. Sentencia de 18 de Septiembre de 2003. Párrafo 162, punto 5. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_100_espdf

12 Mant Comisión IDH inf. 66/2001.

13 De acuerdo al decreto modificatorio N.º 243/2017, estos permiso ahora pueden extenderse a cualquier órgano del Poder Ejecutivo o Judicial de la Nación.

directivas de las autoridades judiciales" y 2) que *"mediante la instalación de dispositivos remotos y móviles, este sistema reducirá la necesidad de trasladar a las personas para su identificación fehaciente, fortaleciendo de esta forma los derechos individuales y minimizando las posibles situaciones de abuso policial"* (Minseg; 2011: 52).

Imagen 3: Captura de imagen del video de presentación oficial de SIBIOS.

En el mismo sentido la actual Presidenta de la Comisión de Derechos Humanos de la Cámara de Diputados de la Nación, la Diputada Victoria Donda, presentó un Proyecto de ley para la *"Prohibición de detención por averiguación de antecedentes"* argumentando que *"desde que el Ministerio del Interior tomó la tarea de realizar los DNI, tiene los datos biométricos digitalizados de todas las personas, tal que en caso de duda, la tecnología disponible hace más que posible la averiguación rápida e instantánea de quién es cada cual, sin necesidad de llevárselo detenido largas horas como se ha descripto, haciendo valer y respetando lo que manda nuestra Constitución Nacional"*[14].

14 Ex N.º 1489-D-2016. Disponible en línea en: http://www.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=1489-D-2016&tipo=LEY

Imagen 4: Infografía sobre los patrulleros inteligentes de la Ciudad de

En teoría esta tecnología permitiría, entonces, que las personas interceptadas no requieran llevar el DNI consigo en la vía pública para mantener su estatuto de ciudadano en el proceso de identificación de averiguación de antecedentes, ya que podrán identificarse utilizando su propio cuerpo de manera expeditiva.

De esta manera, el Estado argentino está tratando de saldar un problema de seguridad y un problema de derecho constitucional a través del paradigma que subyace a los paradigmas de ciudades inteligentes: el de instrumentalización primaria de la tecnología (Feenberg, 2012; Simondon, 2008). Según el mismo, los objetos de la técnica son simplemente materias primas al servicio de objetivos extrínsecos, o en otras palabras, dice que las tecnologías son neutrales, ajenas a toda sinergia con el *entorno asociado* natural y social, y por lo tanto son capaces de encarnar una forma de gobierno técnico, racional y objetivo, capaz de eliminar o aplacar los problemas sociales si las

expandimos y usamos en su máxima expresión. Así pareciera que la tecnología podría frenar por sí sola la decisión política de ejercer un derecho penal de autor (Eilbaum; 2004), hasta ahora utilizado para aumentar las estadísticas de labor policial, y sembrar miedo y disciplina en los sectores sociales más vulnerables. Pareciera que podría neutralizar la arbitrariedad del *olfato policial* descansando la misma tecnología de gobierno (Foucault; 2006) de carácter anticipatorio (FP7 Unión Europea; 2012), pero con una novedosa técnica digital de intervención de seguridad.

Con la intención de reducir la capacidad de control arbitrario del Estado sobre la población, la Argentina está expandiendo esa capacidad a una escala mucho más amplia, ya no sólo sobre grupos sociales vulnerables, sino también con una perspectiva anticipatoria sobre toda la sociedad. Esto significa que no se trata de una medida preventiva que, sobre la base de actos delictivos ocurridos, trata de que no vuelvan a suceder con medidas afirmativas sobre toda la población, o medidas negativas focalizadas en los ofensores como solía ser la extracción, registro y guarda de sus huellas dactilares, fotos, etc. Tanto la detención por averiguación de antecedentes como la base nacional de datos biométricos para uso policial, son políticas complementarias de control y vigilancia que se aplican de manera grupal o universal sobre inocentes, para anticiparse ante la presunción de que pueden volverse criminales.

El punto de inicio de la vigilancia son los identificadores que uno no elige y son lanzados por otros para un proceso de identificación, la tecnología de identificación hace que el poder del Estado se vuelva más efectivo para ese monitoreo (Lyon, 2009).

En este sentido se debe problematizar este concepto, partiendo de la idea de que las actividades de vigilancia, volcadas a individuos o poblaciones humanas envuelven, de modo general, tres elementos centrales: observación, conocimiento e intervención. Y que ni la observación ni el conocimiento se caracterizan como vigilancia si no hay una perspectiva de intervenir sobre los individuos o poblaciones en foco (Bruno, 2013). Intervención que es, sobre todo, del orden de gobierno, entendido como arte de conducir las conductas (Foucault, 2006).

Cuando el Estado no cree si alguien dice que es quien es, cuando tampoco cree en la tarjeta identificadora que él mismo Estado le ha otorgado a la persona para identificarla y, además de quién es, comienza a exigirle que demuestre *qué es* para poder ejercer sus derechos; el resultado es una redefinición del vínculo entre el Estado y la ciudadanía. Así el Estado comienza a tratar a su población desde su animalidad, o su *zoé* como diría Agamben (2006), como condición para permitirnos tener acceso a nuestro *bios*: una historia, a una ciudadanía y sus consecuentes derechos. Esto nos obliga a replantear el problema del principal-agente, de quién debe servir a quién, y de qué lugar le queda al principio de presunción de inocencia cuando la *securitización de la identidad* de la que habla Niklas Rose (2000), nos requiere cada día más probar la legitimidad de

nuestra identidad para poder ejercer nuestra libertad y nuestros derechos (trabajar[15], cobrar jubilación[16], viajar[17], etc.).

El Programa Barrios Seguros, implementado por el Ministerio de Seguridad de la Nación, pone a la Policía Federal Argentina a realizar controles biométricos a quienes ingresan y egresan de "Villas Miseria" de la Ciudad Autónoma de Buenos Aires, criminalizando la pobreza con controles que pueden no estar limitados meramente a la identificación sino también a generar nuevos subregistros, nuevos perfilados de peligrosidad por ser parte, o por encontrarse en diálogo directo con las poblaciones y zonas ya consideradas como peligrosas.

Imagen 5: Afiche y hashtag del programa extraído del sitio web del Ministerio de Seguridad de la Nación

La particularidad de los sistemas de control biométrico es que pueden exacerbar las desigualdades y las injusticias del lugar donde se implementan de maneras sutiles, sin que necesariamente haya una intención por parte de sus promotores o implementadores (Lyon, 2009). Esto puede suceder por los riesgos de la selectividad automatizada, ya que algunas diferencias tribiales en los criterios de reconocimiento algorítmico facial o dactilar del sistema informático, pueden de hecho generar falsos positivos o falsos negativos con una implicancia

15 "CUIT, con foto y huellas dactilares", Clarín, 29 de mayo de 2010. Disponible en línea en: https://www.clarin.com/politica/CUIT-foto-huellas-dactilares_0_H1xQ9oWRvmg.html

16 "Los jubilados y pensionados tendrán que registrar sus huellas digitales para cobrar sus haberes", La Nación, 30 de diciembre de 2014. Disponible en línea en: http://www.lanacion.com.ar/1756361-jubilados-y-pensionados-huellas-dactilares-anses

17 *"Presentaron el nuevo Sistema de Identificación Aeroportuaria"*, 22 de diciembre de 2005, Aeropuertos Argentina 2000. Disponible en línea en: http://www.aa2000.com.ar/aa2000_sp_gacetilla_int.aspx?idNoticia=31

política (ética) importante dentro de un abanico de prácticas de vigilancia socio-técnicas[18] (Introna en Lyon, 2009).

Las detenciones arbitrarias seguirán enmarcadas en una estrategia de poder en pos del disciplinamiento social, en sentido foucaultiano, pero con la novedad de que ahora pueden enmascararse detrás de la contingencia y el azar tecnológico. Hoy una persona puede ser retenida por el criterio arbitrario de cualquier policía, y detenida si no tiene su DNI para identificarse. La contingencialidad de esta detención arbitraria descansa en que la persona interrogada puede tener o no su identificador. La identificación biométrica hace que la responsabilidad de la detención pueda no ser atribuida a ninguno de los actores, sino a alguna falla contingente en la conectividad de la red o los dispositivos digitales para identificación. Esta falla puede ser real o puede ser fabricada por el agente policial, la novedad en ese último caso es el nuevo recurso que logra el Estado de poder conectar o desconectar la ciudadanía. Un poder de desresponsabilización que colabora en enmascarar las detenciones arbitrarias detrás de prácticas tecnoburocráticas.

Entonces, cuanto más usemos nuestra biología como identificador, más posibilidades habrá de que prospere esta forma de detención arbitraria que se esconde detrás de un manto de neutralidad científica. Por eso la paradoja de saldar este problema del derecho con tecnología, es que llevar el DNI siempre con nosotros, puede terminar resultando el mejor anticuerpo para que la arbitrariedad policial pueda seguir siendo considerada como tal, y se le pueda seguir exigiendo al Estado que no se desentienda de sus responsabilidades en materia de derechos humanos.

Y este es un dilema muy porteño porque no todos los países tienen DNI, porque son muy pocos los que tienen bases nacionales centralizadas con los datos biométricos de su población, y porque CABA es la primer y más importante ciudad inteligente del país.

Próximo paso: la identificación genética

Debemos tener en cuenta que las tecnologías favorecen condiciones de visibilidad (Deleuze, 1998) de la que también participan prácticas, reglas y discursos, que están articulados a formaciones de saber y juegos de poder (Foucault, 1983). Creando un régimen de visibilidad que consiste, no tanto en lo que es visto, como en lo que hace posible lo que se ve.

La vigilancia está en un constante estado de flujo, en términos de características técnicas, de la reacción del público, de su uso y manejo por las autoridades y de la naturaleza de la seguridad (Carli, 2008). En términos de Bruno (2013), hoy estamos viviendo una *vigilancia ampliada,* entendida como la circularidad que genera la asociación de las lógicas del riesgo, de la seguridad y de la vigilancia, que convierte toda falla de este modelo en un motivo para ampliarlo todavía más.

18 Según la Universidad de Georgetown los algoritmos que usa el FBI en Estados Unidos son inexactos aproximadamente en un 15% de las oportunidades y son más propensos a identificar erróneamente a los afroamericanos (ADC; 2017).

Primero se extraían huellas dactilares a las personas que cometían delitos, luego comenzamos a extraer, digitalizar y centralizar todas las huellas y fotos de todos para reconocimiento automatizado dactilar y facial con fines de seguridad, y *"se encuentran en etapa experimental (identificación de voz e iris)*" (Minseg; 2011: 52). Detrás de esta racionalidad instrumental de convertir por defecto los cuerpos en identificador para la confirmación de identidad, y para el ejercicio de otros derechos, también comenzaron a avanzar propuestas legislativas anticipatorias para crear padrones genéticos con fines de seguridad. Incluso con ese objetivo fue presentado inicialmente SIBIOS.

En la sesión del día 03 de julio de 2013 de la Honorable Cámara de Diputados de la Nación, en la que se creó un registro de huellas genéticas de violadores, la Diputada Patricia Bullrich, actual Ministra de Seguridad de la Nación, dijo lo siguiente: *"Así como la Argentina fue pionera en cuanto al suministro de datos personales que ayudaron a la identificación de los delitos con las huellas digitales* [en referencia al sistema dactilográfico creado por el argentino Juan Vucetich], *hoy estamos generando un avance similar pensando en las posibilidades que existen en este mundo en que vivimos.*

Por eso, generar este avance implica que a partir de este registro de datos genéticos podamos pensar que de manera rápida se extienda esta herramienta de prueba tan importante, que ya está siendo utilizada aunque no está del todo legislada, en una gran cantidad de delitos para ayudar a esclarecerlos. De modo que no utilizaríamos esta herramienta del ADN para un tipo específico de delito sino que sería la herramienta de identificación del siglo XXI, así como la huella dactilar lo fue en el siglo XX".

Sólo dos años pasaron a esta frase y la Legislatura de la Provincia de Buenos Aires, la más poblada del país con 15 millones de habitantes, dictaminó y aprobó en la orden del día de una sesión legislativa de fines del año 2015, un proyecto de ley[19]para crear un banco genético de todos los habitantes con fines de seguridad pública. Si bien finalmente no fue tratado en sesión, logró abrirse paso[20] ampliando aún más los márgenes de lo decible y lo pensable.

Conclusiones

I. Evitar caer en la trampa de pensar que existen soluciones biométricas a problemas de derecho, y recordar que si el Estado asume y afirma la existencia de ciertos atributos inviolables de la persona humana, los derechos humanos, entonces la Ley Nº 23.950 debe neutralizarse desde el derecho.

Las nuevas tecnologías no son garantía de nada si no hay decisión política, organismos de control externos con sólidas atribuciones, y si falta investigación de los fiscales y los jueces para evitar la impunidad de estos abusos y deje ser ser una práctica naturalizada.

---

19 Expediente D- 373/14-15- 0 / LPBA.

20 *"Crearían un banco genético de todos los bonaerenses"*, La Nación, 15 de septiembre de 2015.

II. Tener en cuenta que la expansión de los sistemas biométricos implican nuevos desafíos para la protección de derechos relativos a la privacidad. El SIBIOS viola el art. 19 de la Constitución Nacional, el art. 11 de la Convención Americana de Derechos Humanos y el art. 12 de la Declaración Universal de Derechos Humanos; agravado por el hecho de que falta al prinicpio de legalidad porque no fue aprobada por una ley nacional que especifique la necesidad excepcional de limitar un derecho en pos de otro, ni tampoco mecanismos de control explícitos.

En esta labor, el derecho a la protección de datos personales no debería ser pensado solamente como un derecho liberal clásico para que la esfera individual íntima no sea invadida por el Estado, sino que, cada día más debe ser pensado también desde la perspectiva del derecho de los pueblos a la autodeterminación informativa. Más aun teniendo en cuenta que hoy distintos países del tercer mundo, como la Argentina, han creado bases nacionales donde centralizan en un disco duro una copia fiel de la biología de pueblos enteros. Y que el sector privado también está creando estas bases a nivel mundial.

III. Evitar caer en la trampa de pensar que la tecnología digital vino a resolver los problemas de seguridad ciudadana. La biometría puede ser de mucha ayuda para la investigación judicial y para evitar casos de suplantación de identidad. Pero usar tecnología biométrica no garantiza nada si no existe la decisión política de atacar las redes de delito, ni implica necesariamente un uso desproporcionado con fines anticipatorios. Entenderla de esta manera puede incluso generar nuevos problemas de seguridad, no sólo porque son datos biométricos falseables (ADC; 2017), o porque el Estado no brinda detalles técnicos sobre la seguridad de los servidores para usar SIBIOS (ADC; 2017), sino porque tiene acceso irrestricto y no hay mecanismos de control normados, ni control judicial de acceso a la base, con lo cual el robo o acceso indebido a esa base podría poner en riesgo información sensible e inmodificable de los argentinos. Por esta razón la República de Francia consideró un riesgo para la seguridad nacional la creación de una base biométrica de los franceses y anuló la normativa que la creaba[21]. SIBIOS está poniendo en riesgo a todos los argentinos a cambio de una política securitaria que no evidencia logros y viola el principio de inocencia.

Bibliografía

- Agamben G. 1998 (2006). *Homo Sacer. El poder soberano y la nuda vida* (España: Giulio Einaudi).

- Asociación por los Derechos Civiles (2017) *La identidad que no podemos cambiar*.

- Banco Mundial (2016) *Dividendos Digitales. Informe Sobre el Desarrollo Mundial 2016*.

- Borsdorf, A. (2003) Cómo modelar el desarrollo y la dinámica de la ciudad latinoamericana en *EURE* V.29 N°86 (Santiago de Chile).

21 *"La nouvelle carte d'identité biométrique jugée inconstitutionnelle"*, Le Monde Diplomatique, 23 de marzo de 2012.

Normativa. Décision n° 2012-652 DC du 22 mars 2012. Loi relative a la protection de l'identité.

- Cardoso, B. De V. (2014). Todos os olhos. Videovigilância, voyeurismos e reprodução imagética. (Río de Janeiro: UFRJ).

- Carli, V. (2008). Valoración de la video-vigilancia como una Herramienta efectiva de manejo y seguridad para la resolución, prevención y reducción de crímenes. Centro Internacional para la Prevención de la Criminalidad.

- Deleuze, G. 1987 (2005). *Foucault* (Buenos Aires: Paidós).

- Di Virgilio, M.; Herzer, H. y Rodriguez C. (2015). "Gentrification in Buenos Aires: global trends and local features" en Global gentrifications. Uneven development and displacement (Gran Bretaña: Policy Press).

- Eilbaum, L. (2004). "La sospecha como fundamento de los procedimientos policiales", en *Cuadernos de Antropología Social* No 20, p 79-91. Disponible en línea en: http://www.scielo.org.ar/pdf/cas/n20/n20a06.pdf.

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

- Foucault, Michel 2004 (2006). *Seguridad, Población y Territorio* (Buenos Aires: Fondo de Cultura Económica).

- García, F. (2012). *SafeCity: Vision, Mission Strategy. The main pillar to build smart cities is the enhancement of the public safety.*

- Internacional Telecommunication Union (ITU). Statistics and Database. Disponible en línea en: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

- Martín, A. (2010) *Detenciones policiales ilegales y arbitrarias en la jurisprudencia de la Cámara Nacional de Casación Penal 1994-2007* (CABA: Del Puerto).

- Mingolarra Iarzabal, J. A. (2006). Prontuario Interrumpido de la ciudad. p 11-23 en *Revista internacional de Estudios Vascos* N°51.

- Ministerio de Seguridad de la Nación (2011*). El modelo argentino de seguridad democrática*.

- Naciones Unidas (2014) La situación demográfica en el mundo 2014.

- Rose, N. (2000). "Government and control" en *Brit. J. Criminol.* N.º 40, p 321-329.

- Seventh Framework Programme de la Unión Europea (2012). "Deliverable D1.1: Surveillance, fighting crime and violence" del programa *Increasing Resilience in Surveillance Societies*, proyecto Nº 290492.

- Sibilla, G. (2012) Proyecto Buenos Aires Ciudad Segura: su racionalidad y puesta en marcha, P 203-228 en *Cuadernos de Seguridad N°15*, Instituto Nacional de Estudios Estratégicos de la Seguridad (CABA, Ministerio de Seguridad de la Nación).

- Simondon (2008). *El modo de existencia de los objetos técnicos* (Buenos Aires: Prometeo).