

EL EMPLEO DE NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TICS) EN EL CAMPO DE LA SEGURIDAD. UN RELEVAMIENTO EXPLORATORIO EN TORNO A NORMATIVA ESPECÍFICA Y DEBATES PÚBLICOS EN EL ÁREA METROPOLITANA DE BUENOS AIRES,

ARGENTINA.

Alina Lis Ríos
alinalrios@gmail.com
CONICET / IIGG-UBA / IUPFA

Argentina

Lucía Cañaveral

luveral@gmail.com

IIGG-UBA / IUPFA

Argentina



RESUMEN

Dentro de las diversas transformaciones que viene atravesando la gestión de la seguridad en Argentina en los últimos años, la implementación creciente de estrategias apoyadas en el uso de tecnologías de la información y comunicación (TICs) es una de las más novedosas. Esta reconfiguración en el campo securitario, a su vez, no ha ido acompañada en el terreno local del suficiente desarrollo analítico y crítico que permita visibilizar sus efectos específicos en cuanto a formas de socialidad y control.

En este contexto, esta investigación se propone aportar a la problematización de la creciente utilización de tecnologías de la información y comunicación en el campo de las políticas de seguridad en el Área Metropolitana de Buenos Aires -AMBA-, desde la creación del Ministerio de Seguridad en diciembre del año 2010.

Nos proponemos para eso desarrollar un relevamiento exploratorio tanto de la normativa existente como de los debates públicos en torno a las aplicaciones securitarias de las TICs. Se considerarán aquellos usos asociados a la formación de las fuerzas de seguridad; la vigilancia de territorios; el seguimiento y control de circulaciones de personas y mercancías; la investigación criminal; la información criminal; la identificación de personas y bases de datos; la detención o inmovilización de personas.

En relación a la normativa, interesa sistematizar y analizar las normativas de nivel nacional y del AMBA que: instituyen nuevas estructuras gubernamentales (por ejemplo aquellas que dan lugar a la Autoridad Federal de Tecnologías de la Información y las Comunicaciones -AFTIC- y la conformación del Comité para la Seguridad de la Información); que crean nuevos dispositivos de intervención (por ejemplo el Sistema de Identificación Biométrica para la seguridad -SIBIOS- y el Registro Nacional de Datos Genéticos vinculados a Delitos contra la Integridad Sexual); que producen un marco regulatorio para la utilización de algunas de estas tecnologías (a modo de ejemplo, el Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos y el Reglamento Provisional de los Vehículos Aéreos No Tripulados -VANTs-).



En relación a los debates públicos, se trabajará con un relevamiento en medios gráficos de circulación nacional, Página12, La Nación, Clarín e Infobae, intentando dar cuenta de las formas de problematización social que emergen a partir de la incorporación de cada uno de estos nuevos usos. En ambos casos, no interesará analizar la eficacia en relación al objetivo que el uso de estas tecnologías se propone en términos de persecución y gestión del delito, sino más bien poner de relieve la dimensión política de su empleo, analizando el impacto que las mismas tienen en las formas de gobierno y control y en el modo en que se estructura un entramado de actores, prácticas y relaciones sociales específico.

ABSTRACT

(Resumen en Inglés)

Within the various transformations that have affected security management in Argentina in recent years, the growing implementation of strategies based on the use of information and communication technologies (ICTs) is one of the most innovative. At the same time this reconfiguration in the local security field, has not been accompanied by sufficient analytical and critical development to make visible its specific effects regarding forms of sociality and control.

This research aims to contribute to the problematization of the growing use of information and communication technologies in the field of security policies in the Metropolitan Area of Buenos Aires -AMBA-, since the creation of the Ministry of Security in December of the year 2010.

We propose an exploratory study of both the existing regulations and public debates around the security applications of ICTs. We will consider those uses associated with the training of security forces; the surveillance of territories; the monitoring and control of circulations of people and merchandise; the criminal investigation; the criminal information; the identification of people and databases; the detention or immobilization of people.

Regarding regulations, it is important to systematize and analyze national and AMBA regulations that: establish new governmental structures (for example, those that give rise to the Federal Infor-

XXXI CONGRESO ALAS
URUGUAY 2017
3 - 8 Diciembre / Montevideo

Las encrucijadas abiertas de América Latina La sociología en tiempos de cambio

mation and Communications Technologies Authority – FTIC- and the creation of a Committee for Information Security); that create new intervention devices (for example, the Biometric Identification System for security - SIBIOS - and the National Registry of Genetic Data linked to Crimes against Sexual Integrity); that produce a regulatory framework for the use of some of these technologies (for example, the General Protocol of Operation of Camcorders in Public Spaces and the Provisional Regulation of Unmanned Aerial Vehicles -VANTs-).

Regaarding public debates, we will work analyzing national graphic media, *Página 12, La Nación, Clarín* and *Infobae*, trying to account for the forms of social problematization that emerge from the incorporation of each of these new applications.

In both cases, it will not be interesting to analyze the effectiveness in relation to the objective that the use of these technologies is proposed in terms of prosecution and crime management, but rather to highlight the political dimension of their use, analyzing the impact they have in the forms of government and control and in the way in which a network of actors, practices and specific social relations is structured.

Palabras clave

TICs – (In)Seguridad – Control

Keywords

ICT - (In) Security - Control



I. Introducción

(Descripción del tema o problema, objetivos e indicar si es resultado de una investigación en curso o concluida)

El presente trabajo aborda un análisis exploratorio de las formas de problematización social sobre el uso de TICs en el campo del gobierno de la seguridad. Dos hipótesis orientan nuestra investigación. Por un lado, consideramos que el estudio de la incorporación de nuevas TICs es una vía para comprender los cambios que afectan al campo del gobierno de la seguridad en general. Es decir, las tecnologías y sus usos se presentan como un analizador relevante de las relaciones de gobierno. Por el otro, la introducción de cambios tecnológicos puede significar cambios en las lógicas de las prácticas a las que se acoplan. Nos interesa particularmente comprender en qué medida la incorporación de nuevas TICs está asociada a mutaciones de las lógicas de control. Tal interrogante nos pone en camino de un plan de trabajo amplio, del cual este trabajo es sólo una primera aproximación exploratoria.

La exploración inicial aborda el modo en que se construye la relación TICs-seguridad-inseguridad, tomando como referencia dos campos de prácticas. Por un lado, el de la producción normativa. ¿Qué tipo de normas regulan los usos de TICs asociados al gobierno de la (in)seguridad? ¿Qué definiciones están implicadas en estas normativas respecto de la construcción de la (in)seguridad como objeto de gobierno? Y por contrapartida, ¿qué indefiniciones operan efectos de ambigüedad? Y además, ¿qué racionalidades atraviesan estas normas? ¿Cómo se relaciona esta producción normativa con el modo en que se organiza o estructura el campo del gobierno de la (in)seguridad? Por otro lado, abordamos el campo de los debates públicos. En esta primera etapa de trabajo sondeamos el modo en que se problematiza en los medios gráficos de comunicación el uso de tecnologías de videovigilancia. ¿Cuáles son los usos de cámaras de seguridad que se definen como apropiados y socialmente aceptables? ¿Cómo se justifican socialmente las prácticas de videovigilancia? ¿Qué tramas de sentidos asocian seguridad y videovigilancia?



Estas son las dos series de interrogantes que ordenan nuestra exploración. En los siguientes apartados explicitamos las principales coordenadas teóricas de nuestro análisis, describimos la metodología empleada y presentamos los principales avances obtenidos respectos de estas preguntas.



II. Marco teórico/marco conceptual

Resulta hoy incuestionable la relevancia que ha adquirido en las últimas décadas el desarrollo de nuevas tecnologías de la información y comunicación -TICs-, pues en torno a ellas se han producido importantes cambios que afectan la vida social (nuevas fuentes de energía, aplicaciones médicas, técnicas de fabricación de nuevos materiales, nuevas tecnologías de transporte y comunicación) y que resultan en transformaciones respecto de la estructuración de relaciones sociales (Castells, 2000, 2004). Existe hoy "una conciencia clara de que gran parte de los procesos productivos se van reconfigurando, aprovechando, maximizando y transformando a partir del potencial de estas tecnologías informacionales" (Becerra en Levis et al., 2008: 2). Las TICs abarcan al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro, difusión y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética (Finquelievich, 2016) De esa enorme variedad de tecnologías y dispositivos a que alude el término TICs nos interesa realizar un recorte, que no tiene que ver tanto con la "naturaleza" del objeto, como con la perspectiva de análisis que le imponemos. Nos interesa observar el modo en que las nuevas TICs se engarzan en las relaciones de gobierno, particularmente en lo que respecta al gobierno de la (in)seguridad.

Varios autores destacan la importancia de las TICs como recursos para el desarrollo social en múltiples aspectos (Gurstein, 1999; Proenza, 2002). Sin embargo, esto no resta importancia a la necesidad de reparar críticamente en los efectos que su utilización podría acarrear. Por el contrario, consideramos que la relación que se da entre la utilización de TICs y el desarrollo social no es una relación directa o inmediata, como parecería indicarlo una ideología del progreso de corte positivista (Becerra, 2003). Antes bien, esta relación se encuentra mediada por la posibilidad de un uso reflexivo de las mismas. Vale decir que el empleo de TICs no conduce por sí mismo a mayores oportunidades de desarrollo, sino que esta virtud aparece cuando tal utilización está orientada por



una intencionalidad crítica que sea capaz de poner en juego la consideración de la dimensión política de los efectos de la aplicación de estas tecnologías.

Al poner la mirada en la dimensión política de la aplicación de nuevas tecnologías resulta ineludible la referencia al filósofo francés Gilles Deleuze y sus reflexiones en torno a las sociedades de control, sociedades que funcionan "mediante un control continuo y una comunicación instantánea", que suponen un nuevo tipo de sanción, de educación y vigilancia (Deleuze, 2006: 273). Como destaca Deleuze, lo esencial de estas nuevas sociedades no está en las nuevas máquinas, aunque constituyan tecnologías verdaderamente nuevas. "Las máquinas no explican nada, es preciso analizar los dispositivos colectivos de enunciación de los cuales las máquinas no son más que una parte" (Deleuze, 2006: 274). Es preciso estudiar las sintaxis sociales que dan sentido, que ponen a jugar esas máquinas en formas específicas de producción de relaciones sociales. En definitiva, es preciso reparar en el estudio de los usos y las prácticas sociales que comprometen la aplicación de esas tecnologías.

Esta preocupación por los usos y aplicaciones es fundante de una perspectiva crítica que problematiza los efectos de tales empleos en las formas en que se estructura la vida social. Una perspectiva que propicia una reflexión *sobre* la técnica, que trascienda los límites de un discurso tecnologista, es decir, un discurso *de la* técnica (Schmucler, 1995, 1996). Este enfoque resulta particularmente relevante hoy, cuando la identificación del terrorismo como nueva amenaza mundial es el soporte de un nuevo paradigma seguridad, en el que cobran mayor relevancia los dispositivos de vigilancia en la vida cotidiana de los ciudadanos (Bauman y Lyon, 2012; Mattelart, 2009).

Esto evidencia la particular pertinencia del campo específico que proponemos estudiar, el ámbito de las políticas de seguridad y el rol que en él desempeña la aplicación de nuevas tecnologías de información y comunicación. Proponemos el estudio de TICs aplicadas a políticas de seguridad pública, entendiendo por tales al "conjunto de estrategias e intervenciones públicas implementadas por diversos actores estatales y sociales a los efectos específicos de abordar y resolver aquellos riesgos y conflictos, concretos o previsibles, de carácter violento y/o delictivo, que lesionen los derechos y libertades de un determinado ámbito espacio temporal" (Sain, 2008: 67). Ámbito que a



los fines de nuestro estudio se limita al Área Metropolitana de Buenos Aires, desde diciembre de 2010 (a partir de la creación de Ministerio de Seguridad de la Nación) a la actualidad.

Ponemos de relieve que nuestro planteo no se recorta sobre los problemas de investigación que comúnmente se plantean en torno a la seguridad en el empleo de TICs, es decir, que no nos ocupamos primordialmente de los problemas de seguridad que puedan derivarse del empleo de nuevas tecnologías de la información, ni de cuán eficaces resultan estas tecnologías en la "lucha contra el delito". Antes bien, el problema que nos ocupa surge de la creciente utilización de estas tecnologías en relación a la implementación de políticas de seguridad pública. O mejor: apuntamos a fortalecer una perspectiva capaz de ver en las prácticas de aplicación tecnológica un problema sobre el que reflexionar. Se trata de apuntar a una desnaturalización del discurso tecnologista. Y en lo que respecta al campo específico de las políticas de seguridad, vincular esos usos y aplicaciones técnicas a las formas en que social y políticamente se estructura un campo de prácticas en torno a la cuestión del "gobierno de la seguridad". ¹

La innovación tecnológica ha acompañado históricamente los cambios en las formas de control social, fundamentalmente en lo que respecta a las técnicas aplicadas a la individuación o identificación de personas, desde la introducción de técnicas como el *bertillonage* (antropometría judicial) a la utilización del registro dactilar para la identificación de personas. En la actualidad cabe la pregunta de hasta qué punto la revolución cibernética iniciada durante la Segunda guerra mundial puede haber impulsado la renovación, si no es la metamorfosis, del paradigma del control social bajo el imperio de las redes (Pèriés, 2011).

A propósito de complejizar el análisis de este vínculo entre nuevas tecnologías y democracia, han sido de suma relevancia los estudios referidos a la utilización de TICs en la gestión urbana (Finquelievich y Schiavo, 1998). Estos estudios han contribuido a desmitificar el vínculo entre nuevas tecnologías y desarrollo, evitando al mismo tiempo caer en la demonización de las nuevas tecnologías.

-

¹ Como ejemplos de TICs aplicadas a la seguridad pública se pueden citar: el empleo de Circuitos Cerrados de TV con fines de videovigilancia; implementación de sistemas de reconocimiento facial; implementación de sistemas de información georeferenciales (GIS); utilización de técnicas de biometría (morpho tuch); identificación de patentes; el desarrollo de vehículos aéreos no tripulados; el empleo de foros o comunidades en soporte web.



En este sentido, buscaremos explorar la posibilidad de un análisis similar en lo que respecta específicamente al empleo de TICs en políticas de seguridad. Se trata de cuestionar la "transparencia" del uso de estas tecnologías en ambos sentidos: por un lado, poner en duda la mítica creencia en la introducción de nuevas tecnologías de control y vigilancia como "la" solución a las formas contemporáneas de la criminalidad; por otro, explorar la potencialidad y limitaciones de la introducción de nuevas tecnologías en un modelo de seguridad democrática.



III. Metodología

El empleo de TICs en el campo del gobierno de la seguridad ha sido una cuestión explorada en distintos países europeos, pero no así en nuestro país, donde se mantiene como un tema muy poco desarrollado. Por este motivo nuestro trabajo se desarrolla inicialmente como un estudio exploratorio, orientado a precisar las coordenadas de abordajes ulteriores. Es así que, como parte de esta exploración inicial, se llevaron a cabo dos actividades cuyos resultados sientan las bases de proyecciones futuras de investigación.

En primer lugar, se realizó un rastreo de las distintas normas (leyes, decretos, disposiciones y resoluciones) que regulan (condicionan, limitan, definen) la utilización de TICs y su aplicación al gobierno de la seguridad (regulaciones generales y específicas a esta aplicación) en el Área Metropolitana de Buenos Aires (AMBA), incluyéndose tanto las normas dictadas por el gobierno nacional, como aquellas dictadas por los gobiernos de la Ciudad Autónoma de Buenos Aires (CABA) y de la Provincia de Buenos Aires (PBA). El período considerado va desde la creación del Ministerio de Seguridad en diciembre de 2010 hasta diciembre de 2015. Queda pendiente, en la continuación del análisis propuesto, dar cuenta de las transformaciones que pueden haber aparecido a partir del cambio de orientación política del gobierno nacional el 10 de diciembre de ese año.

Creemos que en el marco de un estudio exploratorio el rastreo normativo permite aproximarnos a las formas en que una sociedad problematiza una cuestión en un momento dado de su historia, permitiendo también identificar qué prácticas no alcanzan aún esas modalidades de tematización. En ese sentido, la normativa interesa en tanto forma particularmente cristalizada de modalidades sociales de problematización.

Posteriormente se inició un relevamiento de debates públicos acerca del empleo de TICs en el campo de la seguridad. Para nosotros es absolutamente relevante esta cuestión ya que compartimos una perspectiva no-determinista, desde la cual "la tecnología no es un destino sino una escena de lucha" (Feenberg, 2012). Por lo tanto, las formas en que se codifican los usos apropiados y socialmente aceptables de estas tecnologías no es algo dado sino en permanente construcción.



Observar las disputas que se establecen en torno a este punto permite identificar horizontes posibles para la dinamización de este campo de prácticas.

Hasta ahora hemos dado inicio a la primera etapa de este trabajo de relevamiento de debates públicos, consistente en la recolección y análisis de las notas de la prensa gráficas que tematizan el uso de cámaras de seguridad para videovigilancia, publicadas desde 2011 en los siguientes medios: Página12, La Nación, Clarín, e Infobae. Para este trabajo, utilizamos específicamente el material extraído de Infobae.

Realizamos este relevamiento con el objetivo de observar el modo en que se problematizan socialmente las nociones de vigilancia, control y seguridad. El objetivo es identificar cuáles son los principales factores que obstaculizan el desarrollo de estas discusiones, y condicionan el modo en que socialmente se problematiza el empleo de nuevas tecnologías, fundamentalmente vinculado a prácticas de control y vigilancia.



IV. Análisis y discusión de datos

Siguiendo las transformaciones producidas en la gestión de la seguridad en los últimos años, se han relevado normas sancionadas por distintos niveles de gobierno, nacional, provincial y municipal. En todo el mundo, y Argentina no es excepción, los gobiernos locales han ido adquiriendo un nivel de incidencia cada vez mayor en la gestión securitaria, como parte de un proceso más general en el cual se transforman los actores y objetos involucrados en el gobierno de la seguridad. (Garland, 2003)

En torno a nuestro objeto, en el nivel nacional se destaca una producción normativa que apunta a regular el empleo de TICs en términos generales, pero poco se detiene en definir específicamente los usos pertinentes al gobierno de la seguridad. Como desarrollamos más adelante, el problema-horizonte de esta normativa es la protección de datos personales.

En CABA se presenta la particularidad de que existen leyes que enmarcan la función securitaria y que específicamente regulan el empleo de TICs al respecto (La Ley de Seguridad Pública y la Ley de Seguridad Integral que la reemplaza recientemente).

A nivel municipal, se dictan ordenanzas que en general son de carácter operativo refiriéndose al modo en que se organizan ciertos dispositivos de seguridad administrados por los gobiernos locales, fundamentalmente los centros de monitoreo de videovigilancia.

En su mayor parte, las normas que regulan la aplicación de TICs al campo de la seguridad, constituyen resoluciones y disposiciones de las distintas instancias administrativas de los poderes ejecutivos. Son pocas las normas sancionadas con fuerza de Ley por los respectivos poderes legislativos. En el año 2015 se observa un incremento de la actividad normativa.

Según su objeto y finalidad, diferenciamos tres tipos de normas, cada uno de los cuáles plantean problemas diferentes y nos abren a nuevas posibilidades de indagación:

En primer lugar, las *normas instituyentes*. Hemos llamado así a las normas que apuntan a la organización de una estructura institucional estatal que articule las prácticas de regulación de empleo de TICs. Por ejemplo, la creación de la Autoridad Federal de Tecnologías de la Información



y las Comunicaciones (AFTIC), establecida en la Ley 27.078 "Argentina Digital", aprobada por el Congreso de la Nación en diciembre de 2014. Así también, la conformación del Comité para la Seguridad de la Información aprobada por Resolución 970 / 2014 de la Jefatura de Gabinete de Ministros de la Nación. Muchas de las normas instituyentes relevadas han sido objeto de importantes modificaciones a partir del cambio de gobierno ocurrido en diciembre de 2015, modificaciones cuyo sentido y alcance será preciso estudiar para analizar de qué manera se reorganiza la partición público-privado, o qué modelo de desarrollo tecnológico se impulsa, siendo estas sólo algunas las dimensiones que resultan relevantes.

En segundo lugar, reconocemos un conjunto de normas orientadas a la *creación de nuevos dispositivos y programas* orientados al gobierno de la seguridad, que suponen el empleo de TICs. Entre ellas se destacan la creación del Sistema de Identificación Biométrica para la Seguridad (SIBIOS) creado por el Decreto 1766/2011 del Poder Ejecutivo Nacional y La Ley 26.879 que crea el Registro Nacional de Datos Genéticos vinculados a Delitos contra la Integridad Sexual, sancionada en julio de 2013. Respecto de éstas caben preguntas que van mucho más allá de su definición normativa, orientadas a estudiar las distintas instancias de su implementación, los alcances e implicancias de las mismas.

En tercer y último lugar, diferenciamos un conjunto de normas orientadas a la *regulación de ciertos usos tecnológicos*, restringiendo las condiciones en que pueden ser realizados, marcando un límite para la protección de derechos que podrían ser vulnerados, como el derecho a la privacidad. Así, por ejemplo, la definición de las condiciones de licitud para recolección y tratamiento de datos de videovigilancia establecidas en la Disposición 10 /2015 de la Dirección Nacional de Protección de Datos Personales (PDP). Asimismo, esta misma de la Dirección Nacional de Protección de Datos Personales (PDP) en su Disposición 20/2015 estableció las condiciones de licitud para la recolección de datos personales a través de VANT o drones. Respecto de esta misma tecnología la Administración Nacional de Aviación Civil dicta la Resolución 527/2015, que sanciona el Reglamento Provisional de los Vehículos Aéreos No Tripulados (VANTs).

Aunque la normativa citada refiere a usos tecnológicos que no son exclusivos al gobierno de la seguridad, sí son cada vez más recurrentes en este campo. En el caso del uso de videocámaras



queda específicamente establecido el Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos aprobado por Resolución 283/2012 del Ministerio de Seguridad de la Nación. El análisis de este tercer tipo de normativa nos revela un nuevo problema que está relacionado con la necesidad de regular diferencialmente el empleo de TICs por parte de las fuerzas de seguridad.

A los fines de identificar las principales normas que regulan el empleo de TICs en el gobierno de la (in)seguridad comenzamos por identificar tres actividades que hacen a este campo de prácticas: control y vigilancia de personas, policiamiento de territorios e investigación criminal. Estas tres actividades han incorporado en los últimos años varias tecnologías novedosas. Así por ejemplo, el uso de tecnologías que permiten la digitalización de identificadores biológicos (huellas digitales, adn, iris). El desarrollo de videovigilancia, vigilancia satelital y el uso de drones amplían la capacidad de registro de imágenes con fines de vigilancia. Tanto los registros biométricos como de videovigilancia se utilizan, a su vez, como fuentes para la investigación criminal. En este sentido, el análisis específico de la normativa en torno a la videovigilancia permite ver el cruce entre estas distintas esferas propias del gobierno de la seguridad.

En nuestro país, la utilización de circuitos cerrados de televisión (CCTV) para la prevención de delitos comenzó a utilizarse hacia fines de los años 80, acrecentándose su uso en el transcurso de los años 90. Pero se mantuvo mayormente como una estrategia privada de protección a distancia de bienes (ciertas mercancías y objetos culturales) y espacios (comercios, viviendas). Desde fines de la primera década de este siglo comienza a darse un cambio significativo. Claramente, porque crece el número de cámaras usadas para la videovigilancia. Pero no se trata de un cambio meramente cuantitativo. De la videovigilancia como protección de puntos estratégicos al modelo de la vigilancia total que parece encarnar una ciudad como Londres (y que muchos políticos de la arena local enuncian como la panacea perseguida), cambia el sentido de a videovigilancia.

Fundamentalmente, por el enorme desarrollo de la vigilancia pública. Pública en dos sentidos: porque es el Estado el que vigila, y porque son los espacios públicos los que se vuelven objeto de esta actividad.



En nuestro país este desarrollo estuvo fuertemente incentivado por la inversión pública del gobierno nacional, ya que desde el 2009 el financiamiento en seguridad pública para los municipios que supone la creación del Programa Integral de Protección Ciudadana comprende en uno de sus rubros fundamentales el desarrollo de la videovigilancia (Galvani, Rios, & Cañaveral, 2015). Y ya no se trata de CCTV situados, locales, sino de redes de videocámaras que transmiten esas imágenes a un Centro de Monitoreo, donde la ciudad se compone como mosaico de imágenes en movimientos, recibidas en "tiempo real". Es el Estado que multiplica sus ojos. Y frente al avance del Estado se despliega la advertencia liberal clásica, el derecho como protección del individuo y su correlato: la protección de datos personales.

La principal regulación nacional que afecta el ejercicio de la videovigilancia ha sido encarada por la Dirección Nacional de Protección de Datos Personales (DNPDP), y tiene por fin, precisamente, garantizar la protección de datos, pero no conceptualiza explícitamente la videovigilancia como función de gobierno. Lo hace por medio de disposiciones administrativas que buscan establecer cuándo y cómo es lícito recolectar datos de videovigilancia, y cuáles son los usos que se pueden hacer de ellos. La Disposición 10 de 2015 (Boletín Oficial: 27-2-2015) se dicta en consonancia con la Ley de protección de datos personales (Ley N° 25.326, B.O) y parte de reconocer que las actividades de videovigilancia quedan alcanzadas por las regulaciones establecidas en esa Ley. Porque, en tanto supone la construcción de datos (imágenes) que comportan la posibilidad de determinación de la identidad de las personas, la videovigilancia redunda en la producción de bases de datos personales. De manera análoga, esta misma Dirección, en su Disposición 20/2015 estableció las condiciones de licitud para la recolección de datos personales a través de vehículos aéreos no tripulados (VANT o drones).

A pesar de la extensión de la videovigilancia como práctica de control, no existe una ley nacional que regule las condiciones en que puede realizarse esta actividad, que ordene sus alcances y límites. La principal disposición administrativa, la mencionada Disposición 10/2015DNDP, se plantea en términos que se corresponden con la forma en que socialmente se plantea la cuestión: cuando se problematiza el uso de estas tecnologías se hace en términos de "derecho a la privacidad", derecho individual de las personas que debe ser resguardado. Pero no se problematiza la vigilancia como



forma de gobierno, y tampoco se regula a nivel nacional el modo en que esta actividad se despliega: no se define el modo en que se decide la localización de las cámaras, la forma en que se realiza la actividad de monitoreo, o el lugar de la participación y control ciudadano en esta actividad, tampoco se establece la definición de diferentes condiciones para el desarrollo de la videovigilancia según las características de los distintos espacios y sus usos sociales (espacios públicos, espacios privados cerrados, espacios de recepción de públicos, sean estos públicos o privados, etc.).

Otra de las cuestiones fundamentales que se desprenden del análisis es la falta de regulación específica para el uso de TICs por parte de las fuerzas de seguridad. Así, por ejemplo, el Reglamento Provisional de los Vehículos Aéreos No Tripulados (VANTs) no realiza especificaciones relativas al uso policial de estos artefactos. Todas las condiciones están referidas al uso civil en general. La norma que regula las condiciones de licitud en la recolección de datos personales a través de VANTs especifica que "cuando la recolección de los datos la realice el ESTADO NACIONAL en el ejercicio de sus funciones", entonces no será preciso el consenso previo del titular del dato para que su recolección sea lícita. Y en esta categoría queda comprendido el accionar de las fuerzas de seguridad.

Una excepción la constituye la sanción del Protocolo de funcionamiento de videocámaras en espacios públicos, por parte del Ministerio de Seguridad de la Nación, donde quedan establecidas pautas que específicamente apuntan a regular las prácticas policiales en lo que respecta al empleo de videocámaras.

En definitiva, se advierte un déficit normativo en lo que respecta a la regulación específica del empleo de nuevas tecnologías por parte de las fuerzas de seguridad.

Debates públicos sobre el uso de la videovigilancia

El estudio iniciado en relación a los debates públicos sobre el uso de TICs en el campo de la seguridad, aunque aún en curso, arroja algunas saliencias que vamos a presentar. En primer lugar, cabe destacar que en la prensa gráfica el debate propiamente dicho es prácticamente inexistente.



La sociología en tiempos de cambio

Antes bien, lo que encontramos es una serie de publicaciones que naturalizan la incorporación de nuevas tecnologías como solución al problema de la (in)seguridad.

En efecto, podemos reconocer dos tipos de notas que, en conjunto, constituyen casi la totalidad de las publicaciones sobre el tema. Por un lado, aquellas que refieren a sucesos delictivos "controlados" o "descubiertos" gracias a la mediación de cámaras de seguridad.²

Se trata de crónicas que "muestran" la efectividad de la videovigilancia como medio para la resolución de la investigación criminal. Las notas se acompañan con fotos editadas, recortes de las imágenes extraidas de las cámaras de videovigilancia con remarcados en rojo que se utilizan para enfatizar lugares o actores. Se apela a la imagen como evidencia. El enunciado asume la transparencia de las imágenes, su univocidad, y oculta la sobrecodificación que impone el relato, sobreescribiendo identidades, reponiendo las ausencias, reponiendo en la secuencia las imágenes que faltan.

Por otro lado, se habla de cámaras de seguridad en una serie de notas que dan a conocer medidas gubernamentales implementadas para paliar el problema de la seguridad. Incluso, en muchos casos se refiere a medidas que se implementarán a futuro. Son anuncios de iniciativas de gobiernos que se presentan como una solución al problema de la inseguridad. En la mayoría de los casos, se trata de medidas han sido (o lo serán en un futuro inmediato) implementadas por los gobiernos locales (municipales). Hay un énfasis puesto en la novedad, "¡A partir de ahora!", que se presenta como respuesta urgente. Sin embargo, llegamos a identificar que algunas intervenciones se anuncian dos veces, pero con un año de diferencia. Es el caso de la instalación de cámaras de videovigilancia en los colectivos.³

² Sólo a modo de ejemplo:

INFOBAE, 10 de enero de 2014, Cámaras de seguridad registran a un travesti ladrón en Constitución. https://www.infobae.com/2014/01/10/1536225-camaras-seguridad-registran-un-travesti-ladron-constitucion/

INFOBAE, 7 de marzo de 2014, Violento "ataque piraña" en La Boca quedó registrado por las cámaras de seguridad. https://www.infobae.com/2014/03/07/1548541-violento-ataque-pirana-la-boca-quedo-registrado-las-camaras-seguridad/ cámaras INFOBAE, de octubre de 2015, Video: deseguridad registraron https://www.infobae.com/2015/10/07/1760839-video-camaras-seguridad-registraron-un-asesinato/

³ INFOBAE, 28 de julio de 2017, *Inseguridad en los colectivos: colocarán cámaras en las unidades de la Ciudad y el* https://www.infobae.com/sociedad/2017/07/28/inseguridad-en-los-colectivos-colocarancamaras-en-las-unidades-de-la-ciudad-y-el-conurbano/

INFOBAE, 10 de octubre de 2014, Provincia: los colectivos nuevos tendrán cámaras de seguridad, https://www.infobae.com/2014/10/10/1600772-provincia-los-colectivos-nuevos-tendran-camaras-seguridad/



El permanente relanzamiento de la novedad, reeditada, es la estrategia enunciativa que da actualidad a la acción de gobierno, "estamos trabajando", se remarca. Este tipo de notas incluye la voz de los funcionarios que enuncian la urgencia y gravedad del problema de la seguridad. El registro general de relato se acerca mucho al de propaganda de gestión. Y esto se refuerza con el uso de imágenes, que en general muestran grandes cantidades (de patrulleros, de uniformados, etc) de recursos movilizados.

En todo el período estudiado son pocos los acontecimientos que introducen otro orden de problematización respecto del uso de la videovigilancia. Uno de ellos tiene lugar en mayo de 2011: el Ministerio de Educación de la Ciudad de Buenos Aires notificó a las escuelas públicas porteñas que se colocarían cámaras de seguridad en la periferia de los establecimientos (administradas estas por empresas privadas)⁴. Asimismo, la notificación aclaraba que si la comunidad escolar lo deseaba, se procedería a colocar cámaras en el interior del edificio. Para tal fin, los directivos deberían mandar una nota a la Dirección General de Bienes manifestando su aceptación. Es importante destacar que la colocación de estas cámaras y su monitoreo se realiza por fuera del sistema de videovigilancia coordinado entonces por la Policía Metropolitana, y estarían vinculadas a centros de monitoreo a instalar en la Dirección de Custodia y Seguridad de Bienes del gobierno porteño. Esto dio lugar a una serie de discusiones acerca de la colocación de cámaras de seguridad en las escuelas. Marina Ghía (2014) estudió el modo en que se problematiza socialmente la colocación de cámaras de seguridad las escuelas en este contexto y como las principales saliencias del análisis señala que se naturaliza el monitoreo en el espacio público ejercido por el Estado, y que la colocación de cámaras al interior de las escuelas no se descifra por los directivos escolares o funcionarios gubernamentales como un avasallamiento al derecho a la intimidad, por el contrario se presenta reiteradamente como una eficaz respuesta al problema de la (in)seguridad. No obstante, como resultado de estos debates el Gobierno de la Ciudad detuvo la instalación de cámaras al interior de

⁴ En de Abril de 2011 el Jefe de Gobierno de la Ciudad de Buenos Aires (por entonces, Mauricio Macri) estableció la contratación del Servicio de Seguridad y Vigilancia Física y Electrónica para proteger las dependencias y bienes del Gobierno de la Ciudad Autónoma de Buenos Aires. Para tal fin, se procedió a dividir la ciudad en 4 zonas y a cada una de ellas se le asignó una empresa diferente, prestadora de servicios de seguridad privada.



las escuelas. La intervención de algunos padres que judicializaron su reclamo, y los fallos judiciales que hacen lugar a las acciones de amparo interpuestas fueron decisivos.

El otro acontecimiento lo constituye la publicación del libro de Natalia Zuazo *Guerras de internet*, en 2015. Este libro enuncia una posición crítica respecto del uso de nuevas tecnologías, particularmente en relación a la seguridad. Esta publicación es cubierta por los medios gráficos, aparecen reseñas y notas de opinión que reflejan la vocación crítica de la autora. Pero no incide en la manera en que se construyen las notas sobre uso de cámaras de seguridad.

En términos generales, podemos afirmar que los medios de comunicación muestran un alto grado de naturalización del empleo de cámaras de seguridad como estrategia de prevención del delito. Y casi todas las notas periodísticas se vinculan al marketing político de gestiones gubernamentales. Esto ya ha sido señalado tanto en el trabajo de Natalia Zuazo (Zuazo, 2015) como en la tesis de Florencia Botta (Botta, 2014).



V. Conclusiones

(Principales resultados y discusión)

En términos generales, el análisis de los debates públicos en medios de comunicación y de la normativa existente para regular el uso de TICs en seguridad, permite dar cuenta de cierto estado de situación en las modalidades sociales de problematización sobre la cuestión.

Ambas estrategias nos permiten deconstruir el modo en que se plantea la relación TICs-seguridad-inseguridad. Subyace en ambos casos la construcción de un doble vínculo entre seguridad y nuevas tecnologías. Por un lado, se reconoce que el uso de nuevas tecnologías acarrea nuevas vulnerabilidades. Por otro, las nuevas tecnologías aparecen como medios para más seguridad, de forma relativamente acrítica. En este sentido, las referencias a la *eficiencia* y la *eficacia* como lógicas explicativas de la inclusión de TICs en el gobierno de la seguridad aparecen de forma predominante. De este modo, aquello que se plantea como límite al accionar de las TICs tiene que ver exclusivamente con el derecho a la privacidad y su traducción en términos de bases de datos personales. El foco, en este caso, está puesto en los peligros que puede acarrear para el individuo la disponibilidad de esta información, sin que aparezcan elementos orientados a dar cuenta de los efectos colectivos del avance de estas tecnologías en materia de seguridad.

Así, no aparece en las modalidades de problematización analizadas un debate en torno a las formas de politicidad implicadas en el uso de estrategias tecnológicas en materia de seguridad. Esto permite, creemos, validar socialmente una mirada *tecnologista* sobre la cuestión que a su vez produce efectos a los que es necesario prestar atención, particularmente la equiparación entre individuos particulares y agentes estatales a la hora de reflexionar sobre algunos de estos usos.

Nos interesa, a partir de esta sistematización inicial y exploratoria, profundizar el análisis en este sentido.



VI. Bibliografía

(Incluir sólo la citada en el texto)

- Becerra, M. (2017). Macri y lo que sigue. En *Medios en guerra. Balance, crítica y desguace de las políticas de comunicación 2003-2016* (pp. 135–151).
- Becerra, M., & Mastrini, G. (2015). Nuevas reglas de juego en telecomunicaciones en la Argentina. Recuperado a partir de http://www.observacom.org/nuevas-reglas-de-juego-en-telecomunicaciones-en-la-argentina/
- Beck, U. (1986). La sociedad del riesgo. Hacia una nueva modernidad. Barcelona: Ediciones Paidos.
- Bigo, D., & Walker, R. B. J. (2006). Liberté et Sécurité en Europe : enjeux contemporains. *Cultures & Conflits*. Recuperado a partir de http://conflits.revues.org/2040
- Botta, M. F. (2014). Cámaras, discursos, y públicos en elk devenir biopolítico: el caso de la videovigilancia gubernamental en espacios públicos (Gran Buenos Aires. 1998-2014). Universidad de Buenos Aires.
- Bruno, F., Kanachiro, M., & Firmino, R. (2010). Introducción. En F. Bruno, M. Kanachiro, & R. Firmino (Eds.), *Vigilância e Visibilidade. Espaco, tecnologia e identificacao* (p. 296). Porto Alegre: Sulina.
- Califano, B. (2015). Políticas públicas para la convergencia : la regulación de las TIC en la Argentina. En *9th CPR LATAM Conference* (pp. 261–271). Cancun, July 13-14th, 2015.
- Califano, B., & Bizberge, A. (2016). Hacia un negocio más concentrado. *Bastión Digital*, (enero de 2016), 26–28. Recuperado a partir de http://ar.bastiondigital.com/notas/hacia-un-negocio-mas-concentrado
- Callon, M. (1998). El proceso de construcción de la sociedad. El estudio de la tecnología como herramienta para el análisis sociológico. En M. Domènech & F. J. Tirado (Eds.), *Sociología Simétrica: Ensayos sobre ciencia, tecnología y sociedad*. Barcelona: Gedisa.
- Castel, R. (2004). La inseguridad social. ¿Qué es estar protegido? Buenos Aires: Manantial.
- Ceyhan, A. (2006). Technologie et sécurité: une gouvernance libérale dans un contexte d'incertitudes. *Cultures & Conflits*, 64(hiver 2006).



- Chaparro, E. A. (2014). "Argentina Digital": Una oportunidad perdida. Buenos Aires: Fundación Vía Libre. Recuperado a partir de https://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwivzNzhltzWAhXGiZAKHaZzANkQFgguMAE&url=https%3A%2F%2Fwww.vialibre.org.ar%2F2014%2F12%2F16%2Fargentina-digital-una-oportunidad-perdida%2F&usg=AOvVaw34LJ_qyrt0GkpwlGVDKbJu
- Feenberg, A. (2012). Transformar la tecnología. Bernal: Universidad Nacional de Quilmes.
- Finquelievich, S. (2016). *I-Polis. Ciudades en la era de internet*. Ciudad Autonoma de Buenos Aires: Diseño.
- Foucault, M. (2001). El sujeto y el poder. En H. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: más allá del estructuralismo y la hermenéutica*. Buenos Aires: Ediciones Nueva Visión.
- Foucault, M. (2004). Sécurité, territoire, population. Cours au Collège de France, 1977-1978. (Gallimard-Seuil, Ed.), Hautes études. Paris: Gallimard-Seuil.
- Galvani, M., Mouzo, K., Ortiz Maldonado, N., Rangugni, V., Recepter, C., Rios, A., ... Seghezzo, G. (2010). A la inseguridad la hacemos entre todos. Prácticas académicas, mediáticas y policiales. Buenos Aires: Hekht libros.
- Galvani, M., Rios, A., & Cañaveral, L. (2015). Seguridad, policía y gobiernos locales: El Programa Integral de Protección Ciudadana. Colección Becas de investigación. Buenos Aires: CLACSO.
- Ghia, M. L. (2014). Cámaras y escuelas. Un análisis acerca de la problematización social entorno a la instalación de cámaras de seguridad en los alrededores y al interior de las escuelas de la Ciudad Autónoma de Buenos Aires Marina L. Ghia *. *AVATARES de la comunicación y la cultura*, *Nº* 7(Junio de 2014), 1–15. Recuperado a partir de http://ppct.caicyt.gov.ar/index.php/avatares/article/view/3592/pdf
- Pegoraro, J. (2000). A modo de presentación: el síndrome de Aladino y la inseguridad ciudadana. En *Delito y Sociedad. Revista de Ciencias Sociales Nº 14*. Buenos Aires: UNL.
- Périès, G., & Chardel, P.-A. (s/f). Control coerción y excepcionalidad en la era de las redes. Recuperado el 3 de enero de 2017, a partir de http://www.revistapersona.com.ar/Persona84/84Peries.htm
- Rangugni, V. (2009). Emergencia, modos de problematización y gobierno de la in/seguridad en la



- Argentina neoliberal. En *Delito y sociedad. Revista de Ciencias Sociales. Año 18, nro. 27* (pp. 23–44). Santa Fe: Ed. UNL.
- Rios, A. L. (2010a). Gubernamentalidad y poder de policía: la articulación de un modelo de policiamiento dual en Buenos Aires, 2004-2007. *CADERNO CRH*, 23(60), 487–510. Recuperado a partir de http://www.cadernocrh.ufba.br/include/getdoc.php?id=2262&article=797&mode=pdf
- Rios, A. L. (2010b). La Guardia Urbana: Estado, policía y gobierno local (Ciudad Autónoma de Buenos Aires, 2004-2008) Tesis para optar por el título de Magister en Investigación en Ciencias Sociales. Facultad de Ciencias Sociales. Universidad de Buenos Aires, Buenos Aires.
- Rios, A. L. (2016). El traspaso de la Federal: policía y orden social. En A. Lijalad (Ed.), *Macri lo hizo* (pp. 139–150). Buenos Aires: Continente, Peña Lilo.
- Rios, A. L., & Pegoraro, J. (2012). Policía, gobierno local y seguridad en la ciudad de Buenos Aires, desde su autonomización a los sucesos de Parque Indoamericano (1994-2010). Tesis para optar por el título de Doctora en Ciencias Sociales. Facultad de Ciencias Sociales. Universidad de Buenos Aires, Buenos Aires.
- Siri, L. (2015). "Argentina Digital", o cómo regular para no regular. *Bastión Digital*, (febrero de 2015). Recuperado a partir de http://ar.bastiondigital.com/notas/argentina-digital-o-como-regular-para-no-regular
- Zuazo, N. (2015). Guerras de internet. Buenos Aires: Debate.