Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: Te veo, pero no me ves : tensión entre privacidad y vigilancia con la implementación del reconocimiento facial en CABA

Autores (en el caso de tesistas y directores):

Matías Ezequiel Furlanetto

Silvia Lago Martínez, tutora

Martín Gendler, co-tutor

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2021

UBA Sociales

FACULTAD DE CIENCIAS SOCIALES

Te veo, pero no me ves: Tensión entre privacidad y vigilancia con la implementación del reconocimiento facial en CABA

Ciencias de la Comunicación
Tesina de Grado

Autor: Furlanetto Matías Ezequiel
DNI:38.615.163
Mail: Matiasefurlanetto@hotmail.com

Tutora: Profesora Silvia Lago Martínez
Contutor: Profesor Martín Gendler

Contenido

Introducción

En el año 1998 se estrenaba en Estados Unidos la película "*Enemy of the State*" dirigida por Tony Scott con la actuación de Will Smith y Gene Hackman, entre otros afamados actores. En el film se narra la historia ficcional de un abogado norteamericano llamado Robert Clayton Dean, interpretado por Will Smith, quien sin saberlo, recibe la evidencia del asesinato del congresista Phil Hammersley por parte de agentes de la Agencia Nacional de Seguridad (NSA), después de que el político se negara a apoyar un controversial proyecto de ley que permitía a las agencias de inteligencia estadounidenses realizar un espionaje masivo sobre las comunicaciones de la población civil, lo que implicaría una violación a la privacidad de la misma.

Luego de recibir la evidencia, el abogado Robert Clayton Dean comienza a ser perseguido por la NSA desde las sombras a través de tecnologías de vigilancia y control como el sistema de posicionamiento global (GPS), cámaras de videovigilancia y el espionaje de su propia comunicación entre otras técnicas y herramientas de control.

Han transcurrido más de dos décadas desde el estreno del filme. Desde entonces, la población estadounidense comenzaba a visualizar las estructuras de control y vigilancia que operaban en la sociedad desde el secretismo y la falta de transparencia invadiendo su privacidad.

Un ejemplo que clarifica esta situación es el caso de Edward Joseph Snowden, analista de la NSA, quien antes de desertar brindó información a los medios de comunicación. Los diarios The Guardian[1] y The Washington Post[2] recibieron documentos clasificados sobre programas de espionaje y vigilancia masiva que la Agencia Nacional de Seguridad realizó sobre la población norteamericana.

Después de 22 años, a miles de kilómetros de distancia de los Estados Unidos de América y en el mundo real, la sociedad argentina experimenta una realidad con fuertes similitudes a las que se menciona en la película "*Enemy of the State*".

Actualmente, el habitante de Argentina es objeto de una vigilancia invisible y permanente por parte de las fuerzas de seguridad del Estado con la excusa de ser cuidada y protegida. El gran avance y desarrollo de la tecnología facilita a los gobiernos el seguimiento y la vigilancia de toda la población a través de su implementación como lo es el reconocimiento facial.

El mismo escenario de la película se vive hoy en el país y en especial en CABA hacia donde se enfoca la investigación. La población puede ser vigilada silenciosamente sin tener idea del

[1] Véase https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[2] Véase https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html

motivo que justifique esta acción; acción que, sin duda, implica una fuerte tensión con respecto a los derechos constitucionales. Este fenómeno no sólo tiene lugar en la ficción ya que actualmente, en pleno siglo XXl se vive en las distintas naciones del planeta.

Objetivos generales

Como objetivo general se plantea analizar las características que adopta la sociedad de control a partir de la tensión sobre el derecho a la privacidad e intimidad en la implementación de tecnologías digitales de reconocimiento facial en el año 2019 en la Ciudad Autónoma de Buenos Aires.

La tesina indaga la tensión generada entre privacidad y vigilancia en el contexto de la sociedad de control que impera en la mayoría de las sociedades contemporáneas. Específicamente, se enfoca en la sociedad argentina en 2019, recortando el objeto de estudio a CABA, donde a lo largo de los últimos gobiernos de la Ciudad, entre 2008-2020, se produjo una implementación sistemática y constante de tecnologías de vigilancia y control en los distintos espacios de la Ciudad Autónoma de Buenos Aires, como la vía pública y medios de transporte, entre otros. La instalación de cámaras de videovigilancia con reconocimiento facial se ha implementado por las dirigencias políticas con la promesa de aumentar la seguridad de la ciudadanía y son presentadas como herramientas para la prevención y erradicación del delito.

A lo largo de la tesina se ahonda en la problemática que provocan estas tecnologías en la privacidad e intimidad del individuo que circula por CABA teniendo en especial consideración la tensión ejercida por las prácticas de vigilancia sobre las legislaciones argentinas que garantizan el derecho a cada habitante de la Nación de vivir y gozar de su privacidad. Se observa si en la actual sociedad porteña ha desaparecido la presunción de inocencia y todos somos “potenciales culpables” que ameritamos la vigilancia constante por parte de las fuerzas de seguridad estatales, situación que suele pasar desapercibida por la población.

Objetivos específicos

- Realizar un análisis teórico del concepto de sociedad de control enfocando problematizaciones, críticas y aplicaciones en la actualidad.
- Investigar e indagar cómo el desarrollo de tecnologías de vigilancia y control es desplegado por las fuerzas de seguridad del Estado y el modo en que se emplean con fines de vigilancia y control de la ciudadanía.
- Examinar la aplicación de las nuevas modalidades y tecnologías de vigilancia en potencias mundiales como China y Estados Unidos y los avances sobre la privacidad de su población,

comparando el uso de la tecnología de reconocimiento facial entre estas naciones y la Argentina.

- Investigar la regulación que rige a nivel nacional y en CABA que apunta a normalizar el funcionamiento de las tecnologías de reconocimiento facial que operan en el país y a proteger el derecho a la privacidad e intimidad de la ciudadanía.
- Analizar la implementación de sistemas de vigilancia y control, como cámaras de reconocimiento facial en CABA, observando la tensión que se genera entre seguridad y privacidad en relación tanto con la vulneración de los derechos humanos fundamentales como de las legislaciones nacionales y de la Ciudad Autónoma de Buenos Aires.
- Indagar el tratamiento mediático por parte de los medios de comunicación argentinos en torno a los casos de dos ciudadanos: Rachel Holway y Guillermo Federico Ibarrola para analizar su contribución al despliegue de una "política del miedo" constitutiva de la sociedad de control contemporánea.

Metodología utilizada

Para su realización se utilizará la metodología cualitativa tomando específicamente *"La investigación documental"* (Valles, 1999) empleada como parte esencial del proceso de investigación científica que abordará el trabajo.

La investigación documental puede definirse como una estrategia de observación para relacionar en forma sistemática la realidad teórica y empírica que hacen al objeto de estudio. Para ello es necesario recurrir a diferentes tipos de documentos donde se indagan, interpretan y presentan datos e información sobre una determinada temática.

Se sostiene que los documentos constituyen una fuente de evidencia, de recogida de datos como cualquier soporte material en los cuales a través de distintos mecanismos tecnológicos se ha logrado imprimir, registrar y almacenar informaciones sobre fenómenos u objetos.

Para Valles (1999), la idea de documento también remite a las "vistas orales", a las declaraciones juradas de testigos o implicados en un hecho para determinar cuál de estas declaraciones merece el crédito. Al respecto, el autor sostiene que los medios de comunicación transforman a diario las declaraciones de los personajes públicos en documentos escritos, sonoros y audiovisuales que sirven para justificar y acreditar la noticia. También señala que en la investigación documental se genera la combinación entre observación y entrevista la cual se produce en la lectura de los materiales documentales. Retoma la idea de Ruiz Olabuenaga e Ispizua quienes apuntan que a los documentos

> "*En realidad se los puede entrevistar mediante preguntas implícitas y se los puede observar con la misma intensidad y emoción con la que se observa un rito nupcial, una pelea callejera, una manifestación popular. En este caso la lectura es una mezcla de entrevista/observación y puede desarrollarse como cualquiera de ellas*". (Ruiz Olabuenaga & Ispizua, 1989, p. 69)

La expresión más característica de esta opción metodológica se encuentra en los trabajos basados en documentos recogidos en archivos oficiales (públicos y privados). La idea de documentación debe ser entendida como una estrategia metodológica de obtención de información. Esta metodología también contempla el uso de documentos con propósitos de justificación, acreditación de los análisis e interpretaciones realizadas en la investigación con el objetivo de utilizarlos para crear reconstrucciones más o menos históricas. La amplitud de esta definición permite entender que, prácticamente, cualquier material del cual se pueda obtener información útil para la investigación se engloba en el concepto de documento.

En el manual anglosajón de investigación social, Valles (2000, p. 120) afirma que, *"la idea de documento se refiere a una amplia gama de registros escritos y simbólicos"*.

Los autores Amparo Almarcha, Amando de Miguel, Jesús de Miguel y José Luis Romero en "*La documentación y organización de los datos en la investigación sociológica" (1969*) sostienen que existen diferentes tipos de datos acerca de la realidad social estudiada.

En esta tesina se utilizarán los datos denominados como "datos primarios" que han sido construidos en base a fuentes secundarias. Estos datos son elementos de observación obtenidos intencionalmente por el investigador en la búsqueda de la hipótesis de trabajo. Esto se verá reflejado en la indagación y análisis exhaustivo de la jurisprudencia argentina en torno a las leyes que garantizan la privacidad de la población frente a los mecanismos de control y vigilancia.

Por otro lado, se empleará lo que los autores denominan "datos secundarios", los cuales son un cúmulo de informaciones recogidos y/o publicados por diversas instituciones, sin propósitos específicos de investigación social sino con el fin de proveer información o documentación. Tanto los datos primarios como los secundarios se tendrán en cuenta en el análisis y la reconstrucción de los casos periodísticos elegidos en la elaboración y desarrollo de la tesina.

Por lo tanto, para realizar el presente trabajo se ha recurrido a reconocer, identificar y acopiar fuentes documentales de carácter periodístico con enfoque en dos casos puntuales ocurridos en CABA en el transcurso del 2019. Estas notas, editoriales y relatos se observan y estudian para reconstruir los casos seleccionados y así poder examinar, describir y analizar la tensión que genera el derecho a la privacidad y seguridad de la población frente a la implementación de

tecnologías de control y vigilancia como son las cámaras de videovigilancia con reconocimiento facial que operan actualmente en la Ciudad.

Los casos elegidos son los de María Raquel Holway y Guillermo Federico Ibarrola, ciudadanos de la Ciudad Autónoma de Buenos Aires, víctimas de detenciones erróneas generadas por el sistema de vigilancia y control. Ambos casos fueron noticia y tuvieron gran difusión mediática a través de los medios tradicionales y digitales.

De esta forma, se recuperan y utilizan notas periodísticas de múltiples medios de comunicación que poseen líneas editoriales y posicionamientos ideológicos diversos entre sí.

Para el caso de María Raquel Holway se abordaron 9 notas periodísticas (Todo Noticias, Página 12, Clarín, La Nación, Vía País, País 24, RT, De la Bahía, Tú Mercedes) mientras que para el de Guillermo Federico Ibarrola se utilizó la cobertura de 11 medios (La Izquierda Diario, Diario Sur, Clarín, Página 12, Infobae, A24, La Brújula 24, Telefé noticias, Tiempo Argentino, Télam, Todo Noticias).

Para la elaboración de esta tesina se ha realizado un análisis documental de las regulaciones y legislaciones destinadas a configurar el sistema de videovigilancia en Argentina y también de las leyes que establecen el funcionamiento del sistema de reconocimiento facial que opera en CABA. Entre algunas de las legislaciones utilizadas se pueden mencionar:

- Legislaciones Nacionales: Constitución Nacional (Art 18, Art 19 y Art 43) y Ley de Protección de Datos Personales Nº25.326, Resolución 238/2012 Ministerio de Seguridad Presidencia de la Nación, Disposición 10/2015 DNPDP
- Legislaciones existentes en CABA: Ley Nº2602, Ley Nº2894, Ley Nº3130, Ley Nº5628 y la Resolución 298/12 del Ministerio de Justicia y Seguridad del Gobierno de la Ciudad, Decreto 119/09 GCABA, Resolución 410/MJYSGC, Resolución, 10/MJYSGC/11 Resolución 314/MJYSGC, Decreto 716/2009 156/PMCABA/12 para garantizar el derecho a la privacidad.

El objetivo del análisis de cada una de ellas fue investigar la codificación de la implementación de sistemas de vigilancia y control y a la vez analizar la tensión generada entre las prácticas de vigilancia y monitoreo de las fuerzas de seguridad respecto de la privacidad e intimidad de la sociedad. En otras palabras, la posible vulneración de los derechos humanos fundamentales con respecto a las legislaciones tanto nacionales como de CABA.

A través del análisis de los casos de Holway e Ibarrola se contempla cómo los derechos observados por estas legislaciones y regulaciones son puestos en fuerte tensión debido al despliegue de las nuevas tecnologías y modalidades de control y vigilancia.

Fundamentalmente, se indaga sobre cómo los sistemas de vigilancia y control que operan en el aparato represivo del Estado son capaces de pasar estos derechos por alto con el afán de seguir generando cada día una sociedad más controlada.

Estructura de la tesina

La presente tesina aborda de manera integral una investigación en torno a la aplicación de nuevas modalidades y tecnologías como el reconocimiento facial en la Ciudad Autónoma de Buenos Aires y los efectos que implica para el derecho a la privacidad e intimidad de la ciudadanía. Para lograr esta meta, ha sido estructurada en seis capítulos, cada uno de los cuales se articulan entre sí y cuyos ejes se comparten para una mayor comprensión de la temática del trabajo.

El primer capítulo *"Nuevas tiempos, nuevas sociedades, nuevos controles"* establece el marco teórico que regirá el desarrollo de esta investigación. Allí se analizan conceptos transversales al resto de la tesina tales como "control social", "sociedades de control", "panóptico digital" y su posible despliegue en las sociedades contemporáneas a la luz de los desarrollos tecnológicos aplicados recientemente con fines de control y vigilancia masiva.

Continuando este recorrido, en el segundo capítulo *"Policías, cámaras y videovigilancia*" se realiza un enfoque sobre el rol ejercido por las fuerzas policiales: las fuerzas de seguridad del Estado en el marco de las sociedades de control, la aplicación de nuevas tecnologías y modalidades de vigilancia masiva por parte de ellas, así como las características técnicas/tecnológicas que presentan, específicamente las del sistema de reconocimiento facial.

El capítulo tres *"Vigilancia a nivel global"* se centra en el concepto de "política del miedo" entendiéndolo como un concepto clave al hablar de sociedades de control tanto en Argentina como a nivel global. A su vez, aquí se estudian los cambios y las modificaciones en el paradigma de seguridad a partir de los atentados en países occidentales a comienzo del siglo XXl. Tanto "la política del miedo" como los cambios en el paradigma de seguridad permiten comprender la aplicación masiva de tecnologías de control y vigilancia a nivel global. En este capítulo se toman puntualmente ejemplos de dos potencias mundiales: la República Popular de China y los Estados Unidos para ilustrar la forma progresiva en que se ha extendido por el mundo el fenómeno de la vigilancia masiva a través de la tecnología propia de las sociedades de control afectando la privacidad e intimidad como derechos inherentes del ser humano.

El capítulo cuatro, "*Proteger la privacidad: Legislación argentina"* hace énfasis en uno de los conceptos claves presentes en esta tesina: la noción de privacidad como derecho inalienable de todo sujeto. Se estudia la legislación nacional que rige en Argentina, enfatizando en la Ley de

Protección de Datos Personales N°25.326 sancionada con el propósito de resguardar la intimidad y privacidad de los habitantes de la nación.

El quinto capítulo *"Situación en CABA en el 2019"* se centra en el escenario que atraviesa la Ciudad Autónoma de Buenos Aires durante los primeros meses luego de la implementación del reconocimiento facial. Se enfoca en el despliegue de las nuevas tecnologías de control y vigilancia en el entorno porteño, las características técnicas específicas del sistema implementado por el gobierno de la Ciudad y los aspectos técnicos/tecnológicos que han despertado fuerte críticas desde las ONGs. También se observan las voces a favor provenientes del sector gubernamental y empresarial y las voces opositoras (académicas, ONGs) a la implementación de estas tecnologías de control y vigilancia.

En pocas palabras, este capítulo apunta a un análisis de la legislación de CABA sancionada para la implementación de las tecnologías de videovigilancia, protección del derecho a la privacidad e intimidad de sus habitantes y el rol de la ciudadanía para ejercer un control sobre el accionar de las fuerzas de seguridad encargadas de la operación de las nuevas tecnologías de vigilancia.

Finalmente, el sexto capítulo titulado *"Análisis de Casos*" concluye este trabajo de investigación tomando dos casos puntuales de ciudadanos argentinos: María Rachel Holway y Guillermo Federico Ibarrola, ambos detenidos por errores en el sistema de reconocimiento facial que opera en CABA y que a través de registros mediáticos se logra su reconstrucción. Aquí se retoma contenido del cuarto y quinto capítulo para analizar las leyes nacionales y de la Ciudad Autónoma de Buenos Aires que protegen la intimidad y privacidad de la ciudadanía en general incluyendo los casos específicos trabajados en esta tesina. También se prioriza el rol del aparato mediático en Argentina y su impacto en la realidad de la sociedad al abordar la cuestión de la inseguridad en el país y el despliegue de medidas implementadas por las autoridades gubernamentales para combatir esta problemática. Llegando al final del recorrido y a modo de síntesis de la temática contemplada en este trabajo de investigación, el capítulo presenta una comparación entre la idea de guerra tradicional y la idea de "guerra preventiva" anunciada por muchos de los gobiernos contemporáneos al momento de justificar el despliegue de nuevas medidas de vigilancia en el marco de las actuales sociedades de control.

Capítulo 1: Nuevos tiempos, nuevas sociedades, nuevos controles

Introducción

En este capítulo se abordan conceptos fundamentales para lograr comprender la nueva realidad que atraviesan muchas de las sociedades contemporáneas, incluida Argentina, donde se han implementado modalidades y tecnologías de control masivos.

En primer lugar, es necesario contemplar el concepto de control social y sus efectos en las sociedades actuales. Se define la noción de sociedad de control entendiéndola como la configuración social que posee una mayor presencia en la mayoría de las naciones en el período histórico que atraviesa el mundo y que supone fuertes transformaciones, producto de un fuerte desarrollo técnico/tecnológico que modula no solamente a las poblaciones, sino también a sus conductas debido al impacto que genera la vigilancia masiva en el espacio público. Se analiza la sociedad de control como aquella que se encabalga con la sociedad disciplinaria ya que supone una importante mutación dentro del sistema capitalista, por lo que importa repasar brevemente los cambios que presupone el pasaje del capitalismo industrial al capitalismo cognitivo. Finalmente, se observa el surgimiento de las nuevas tecnologías de control y vigilancia elaboradas en los últimos años del siglo XX y a lo largo del siglo XXI en el marco del nuevo paradigma de seguridad, lo cual lleva a preguntarnos si estos nuevos dispositivos de vigilancia podrían implicar la mutación del concepto de panóptico dentro de las actuales sociedades de control.

1. Control Social

De acuerdo con el trabajo "*Control, vigilancia y represión, el Estado en activo" (2007)* de Iñaki Gil de San Vicente se debe entender el concepto de control social como una forma de presión social informal y difusa cuyo objetivo es evitar la conducta delictiva.

"(....) Debemos entender la totalidad de sistemas, instituciones, colectivos y hábitos individuales que existen en todo grupo o sociedad destinados a su auto control". (G. de San Vicente, 2007, p. 4).

Toda colectividad realiza un control social de sus miembros para poder subsistir, asegurando las condiciones de reproducción de las formas sociales ya vigentes, las cuales deben ser internalizadas y naturalizadas por sus integrantes. Conforme a lo planteado por el autor, se deduce que toda sociedad necesita de un autocontrol mínimo pero suficiente que garantice la reproducción de sus valores y condiciones de existencia.

Este control social es implementado en el interior de las sociedades desde distintas fuentes como la religión, la cultura, las tradiciones o las fuerzas de seguridad de una sociedad, entre otras. Las fuentes que llevan a cabo esta práctica pueden ir mutando y modificándose de

acuerdo con el contexto espacio/temporal en el cual se halla la sociedad. Es importante remarcar que, si bien el control social puede ser realizado a través de medios coactivos o violentos, también puede implementarse mediante formas no coactivas como los prejuicios, valores y creencias presentes en una sociedad.

Este concepto implica, en primer lugar, todos los procesos y métodos a través de los cuales una determinada sociedad se asegura que los miembros se ajusten al "interés general" y, en segundo lugar, se refiere a las conductas consideradas como desviadas de la ciudadanía y los esfuerzos por encauzarla hacia dicho interés.

En su trabajo "*Término CRIMIPEDIA: Teorías del control social" (2014)* Rebeca López Puerta retoma el pensamiento de diversos autores sobre el concepto de control social. Una de las definiciones es el de la autora Muñoz Conde (1975) donde sostiene que el control social es la *(...) condición básica de la vida social pues a través de él se asegura el cumplimiento de expectativas de conducta y de los intereses contenidos en las normas sociales que rigen la convivencia"* (Conde, 1975 citado en López Puerta, 2014, p.4). Por lo tanto, este concepto implica un conjunto de medios a través de los cuales una sociedad garantiza que la conducta de sus miembros sea acorde a los parámetros conductuales previamente establecidos y a la capacidad de respuesta de dicha sociedad ante el incumplimiento de estos parámetros por parte de sus integrantes.

En el trabajo también se menciona la definición de control social elaborada por Manzanera (1991) quien apunta que

> "(…) *el control social puede entenderse como el conjunto de instrumentos (generalmente normativos) instituciones y acciones encaminadas al cumplimiento de los fines y valores propuestos por el sistema imperante, logrando de esta forma mantener el orden social*" (Manzanera, 1991 citado en López Puerta, 2014, p 7).

Para Manzanera, quien retomaría la línea de pensamiento de Durkheim, la finalidad del control social es mantener el orden social mediante la restricción de las conductas desviadas, lo que implicaría la puesta en funcionamiento de agencias e instituciones con roles implícitos y explícitos pero que busquen mantener dicho control social. De este modo, los controles sociales tienen como finalidad lograr que la sociedad en su conjunto sea lo suficientemente permeable al ejercicio del poder para que se detecte lo antes posible cualquier anomalía o rareza, incluso, en sus espacios más privados.

Indudablemente, para abordar el fenómeno de control social se debe retomar el concepto de poder tal como lo interpreta el pensamiento de Foucault. El texto *"El concepto de Poder en la Obra de Michel Foucault"* (2010) de Juan Pablo Arancibia Carrizo retoma la idea de Foucault y afirma

> *"(....) Se considera así que el poder efectivamente transita y circula, no se aloja ni se fija; el poder está en todas partes, o más bien dicho, siempre hay relaciones de poder; el poder no se posee sino se ejerce, el poder no es pura represión, sino produce, faculta, seduce; un poder que es relación."* (Arancibia Carrizo, 2010, p. 60).

Por lo tanto, para Foucault el poder es omnipresente, capilar y no es ejercido por un nivel social sobre otro sino que está presente en todos los niveles.

Carrizo (2010) retoma la definición de poder que Foucault hace en su trabajo "*Tecnologías del yo"* (1990) donde se afirma que

> *"(....) El poder no es una sustancia. Tampoco es un misterioso atributo cuyo origen habría que explorar. El poder no es más que un tipo particular de relaciones entre individuos [...] El rasgo distintivo del poder es que algunos hombres pueden, más o menos, determinar por completo la conducta de otros hombres, pero jamás de manera exhaustiva o coercitiva. Un hombre encadenado y azotado se encuentra sometido a la fuerza que se ejerce sobre él. Pero no al poder."* (Arancibia Carrizo, 2010, p. 61).

Entonces, para Foucault las estrategias empleadas para alcanzar estos objetivos son: la vigilancia, la recompensa y el castigo, entre otras.

Volviendo al concepto de control social, éste varía de acuerdo con el contexto espacio/temporal. Cualquier control social tiene la tarea de avisar a "instancias superiores" de las anomalías detectadas, lo que implicaría poner en funcionamiento diversos sistemas de vigilancia más complejos, especializados e intensos.

Estas vigilancias pueden no ser realizadas en forma exclusiva por las fuerzas de seguridad del Estado, sino que muchos controles sociales, sobre todo, los extraestatales y privados tienen sus sistemas de vigilancia y pueden recurrir a otros actores complementarios, como, por ejemplo, empresas privadas encargadas de realizar esta función.

En la medida en que aumenta la importancia de los problemas detectados y conforme dichos problemas interactúan con otros, comienza a verse involucrada la vigilancia estatal la cual podría desembocar en diversos grados de represión que difieren conforme a los diferentes casos. Así lo afirma Iñaki G. de San Vicente (2007) "(…) *Siempre existe una continuidad entre control y represión mediatizada por la vigilancia, aunque no es imprescindible que todo fallo detectado por un control termine a la fuerza en una práctica represiva."* (G. De San Vicente, 2007, p.6)

Al final de todos los análisis concretos de los controles y poderes funcionando por su parte se encuentra el Estado quien garantiza la efectividad del conjunto del sistema, supervisando el funcionamiento de los procesos que empiezan con los controles sociales cotidianos más imperceptibles, sigue con las prácticas de vigilancia y termina con las represiones.

De este modo, los controles sociales aportan a diferentes equipos gubernamentales o no, como sociólogos, psicólogos, miembros de las fuerzas de seguridad del Estado etc., un conjunto de

informaciones, datos y estadísticas los cuales son contrastados por otras informaciones que aportan sondeos y estudios de tendencias sociales de todo tipo.

Iñaqui G. De San Vicente (2007) sostiene que el control social está en aumento por diversas razones que se refuerzan mutuamente. En primer lugar, el capitalismo se complejiza cada vez más para responder a sus crecientes dificultades de acumulación ampliada tendiendo a aumentar las resistencias de todo tipo. Y, en segundo lugar, el desarrollo de múltiples tecnologías de vigilancia, controles y espionaje sobre los integrantes de las sociedades para hacer frente a estas nuevas resistencias se condice con la búsqueda de nuevas ramas productivas para abrir novedosos mercados y obtener ganancia. Estas razones, al interactuar entre sí, se refuerzan y originan que los Estados y gobiernos establezcan estrechas alianzas con las corporaciones y monopolios industriales del ramo para multiplicar la producción y venta de la tecnología necesaria para el control, vigilancia y represión, al tiempo que se expande un clima social de ansiedad, temor y miedo utilizado por parte de los mismos Estados mediante los denominados "discursos del miedo" para justificar dichos controles y la implementación de tecnologías de vigilancia sobre las sociedades. Se interviene rápidamente cuando surge un conflicto en el desarrollo productivo, por lo que los Estados necesitan dotarse de todos los controles, vigilancias y represiones que la tecnociencia pueda producir.

Para Iñaqui (2007) estos conceptos surgen del interior del mismo sistema y constituyen "(...) *la base teórica de las disciplinas de control"* (Iñaqui G. de San Vicente, 2007, p.17).

La globalización del capitalismo produce una mundialización de las contradicciones y la obsesión por el control ya que las resistencias y luchas emergen en todas partes con mayor o menor intensidad. Muchas empresas privadas[3] se están percatando del hecho de que la industria de la vigilancia y del control es un negocio rentable económicamente seguro y fiable, y deciden involucrarse en el mismo. Adquieren fuerza y ellas mismas elaboran metas y programas tecno/científicos más sofisticados para lanzar nuevas tecnologías al mercado de los controles, la vigilancia y la represión, por lo que el autor sostiene *"(...) El Estado toma parte en el proceso e interviene declarando esas empresas de "interés nacional" ayudándolas con generosas subvenciones y toda clase de protecciones en la investigación".* (Iñaqui G de San Vicente, 2007, p.17)

De esta forma, se podría presuponer que la tecnología del control social, la vigilancia y la represión contribuye en la constitución y refuerzo del capitalismo actual. Cada momento del proceso controlador, vigilante y represivo requiere de sus propias tecnologías de la misma

[3] Entre las que se podría mencionar a la empresa "G4S", la sueca "Securitas AB" o la compañía norteamericana "ADT".

manera que dentro de cada momento se requieren diversas tecnologías, objetivos de control, vigilancia y represión. Las relaciones con los aparatos estatales, las fuerzas armadas y agencias de inteligencia y espionaje son permanentes y desconocidas en la mayoría de los casos. Se crea así una red donde se produce una mezcla de intereses económicos y políticos que, en muchas ocasiones, opera mundialmente aprovechando legislaciones laxas y ambiguas.

Actualmente se puede apreciar que las relaciones entre agencias de inteligencia y espionaje y las grandes corporaciones comerciales son muy estrechas. Como ejemplo de ello se pueden mencionar las revelaciones que en el 2013 realizó el extécnico de la Agencia de Seguridad Nacional (NSA) de Estados Unidos, Edward Snowden, quien filtró la existencia de un programa de espionaje masivo llamado PRISM que le permite al gobierno norteamericano acceder a datos de usuarios de grandes empresas de Internet como Microsoft, Google, Facebook, Apple, entre otras, para llegar a sus datos privados. En base a las revelaciones de Snowden, el diario de Estados Unidos "The Washington Post" afirmó que la NSA almacenaba cada día 5000 millones de datos de localización de la población, equivalente a los movimientos de cientos de millones de teléfonos celulares. Esto posibilitaba establecer conexiones entre diferentes personas, obteniendo informaciones de las compañías de telefonía y de los smartphones de la población.[4]

2. Cambia el capitalismo, la vigilancia se mantiene: El pasaje del capitalismo industrial al capitalismo cognitivo

Para una mejor comprensión de la temática abordada en esta tesina es necesario contemplar la cuestión del paso del capitalismo industrial al capitalismo informacional o cognitivo que ha tenido lugar dentro de las sociedades contemporáneas.

Manuel Castells en "*La revolución de la tecnología de la información"* (2006) sostiene que la revolución de las tecnologías de información que ocupan un lugar en las sociedades actuales remite a las tecnologías de pensamiento de información y comunicación las cuales cobran tanta importancia en la actualidad como la tuvieron las fuentes de energía como el vapor y la electricidad en las anteriores revoluciones del capitalismo industrial.

En "*Comprensión espaciotemporal y condición postmoderna*" (1998), David Harvey afirma que para la década del 80 el capitalismo emprendió un proceso de reestructuración económica y organizativa donde las tecnologías de la información pasaron a ocupar un rol central dentro de la lógica económica. Esta transformación opera a nivel económico e implica consecuencias

[4] Nota publicada por la Agencia Télam el 16 de diciembre del 2013
https://www.telam.com.ar/notas/201312/44925-las-principales-revelaciones-de-edward-snowden.html

políticas y sociales ya que sus formas de regulación han ido mutando y adaptándose de acuerdo con cada contexto espacio/temporal.

De manera que, se puede afirmar que a fines del siglo XX se ha producido un pasaje del capitalismo industrial hacia el cognitivo o informacional en el cual se priorizan la información y el conocimiento como elementos cruciales en las prácticas económicas enmarcadas en un contexto de capitalismo globalizado.

El capitalismo industrial llega en la segunda mitad del siglo XVIII en medio de un proceso de revoluciones políticas y tecnológicas que tuvieron lugar en Europa, puntualmente en Inglaterra. A partir del año 1760 con el surgimiento y uso de tecnologías aplicadas a la producción industrial como el carbón, el hierro, la maquinaria y el vapor, Gran Bretaña experimenta la llamada Primera Revolución Industrial que fue la continuación de la primera fase del capitalismo conocida como mercantilismo surgido a fines del siglo XlV y se prolonga hasta el nacimiento del capitalismo industrial.

Como características centrales del capitalismo industrial se puede mencionar la producción masiva destinada a grandes mercados realizada mediante la implementación de la división del trabajo en las fábricas e industrias y la producción en forma rutinaria que conlleva un aumento de la producción.

Una de las principales características del capitalismo industrial es el uso y explotación de la mano de obra asalariada por parte de los dueños de las industrias quienes concentran los medios productivos y contratan trabajadores a cambio de un salario que les permita la subsistencia.

Por su parte, el capitalismo cognitivo es una categoría que se refiere conceptualmente a las prácticas económicas sobre las producciones del conocimiento enumeradas en el capitalismo globalizado de fines del siglo XX, principios del XXI y considerado como la base del capitalismo sobre bienes inmateriales. En este nuevo estadio del capitalismo, uno de sus principales ejes se basa en la producción de conocimiento que pasa a ser un eje de valorización del capital, constituyéndose así la sociedad de conocimiento donde la actividad productiva desborda los límites estrictos del trabajo asalariado. El capitalismo cognitivo generó cambios productivos importantes como la producción a través de actividades intensas en conocimiento y cooperación productiva. Las nuevas fuentes de productividad en este nuevo capitalismo pasan a ser los procesos donde interactúan los conocimientos dando origen a la "sociedad de la información" donde se considera al conocimiento como un bien inmaterial, el cual se convierte en el fundamento que reorganiza el mundo productivo y social.

De acuerdo con el trabajo de Carlos Valderrama *"Sociedad de la información: hegemonía, reduccionismo tecnológico y resistencias"* (2012) el proyecto de sociedad de la información

> *"(...) es un proyecto hegemónico construido de manera sistemática y calculada por lo menos desde las últimas cuatro décadas, bajo el liderazgo de los países del G-8, la OCDE y la complicidad de los sectores hegemónicos del tercer mundo".* (Valderrama, 2012, p.6)

Según Valderrama (2012), los reduccionismos y determinismos tecnológicos que fundamentan este proyecto va más allá del uso de la tecnología con fines policivos en el mundo online y offline, sino que se refiere a *"(...) la imposición de un modelo único de tecnologías de comunicación e información y a un modelo de producción de subjetividades tecnológicas"* (Valderrama, 2012, p.6).

Por su parte, Castells (2006) sostiene que una de las características más claras de la actual tecnología de la información es la aplicación del conocimiento, información, comunicación y su aplicación en un círculo de retroalimentación entre innovación y usos. El autor observa otra gran distinción en el pasaje del capitalismo industrial al capitalismo cognitivo que refleja el hecho de que la revolución de la tecnología de la información posibilita no sólo tecnologías para aplicar sino también procesos que desarrollan los propios sujetos: los usuarios y creadores de estas tecnologías pueden ser los mismos individuos.

En el capitalismo cognitivo el proceso productivo cuenta con una nueva materia prima: la tecnología y el conocimiento que se lleva a cabo mediante la investigación bajo las bases del saber, la comunicación e información; por lo que el trabajo se ha transformado en una permanente integración social, dando lugar a un sistema de reproducción de una sociedad de clases con nuevas características de control.

3. ¿Qué son las sociedades de control?

En *"Posdata sobre las sociedades de control" (1991)* Deleuze Gilles sostiene que Foucault situaba a las sociedades disciplinarias entre los siglos XVIII y XIX operando a través de la organización de grandes centros de encierro como la familia, la escuela y posteriormente la fábrica, donde el individuo ha transitado a lo largo de su vida. El proyecto ideal de los centros de encierro era concentrar, repartir en el espacio y ordenar en el tiempo, componiendo en el contexto espacio/temporal una fuerza productiva cuyo efecto debía superar la suma de las fuerzas componentes. Siguiendo a Deleuze, tras la Segunda Guerra Mundial, todos los centros de encierro experimentarían una crisis generalizada. Las autoridades anuncian medidas intentando prolongar su duración, como reformas en las fábricas, escuelas y fuerzas armadas, pero sólo es un paliativo que pretende gestionar la hegemonía de estos elementos de la sociedad disciplinaria ocupando a la población mientras se instalan "nuevas fuerzas".

Martín Gendler en *"Sociedades de control: Lecturas, diálogos y (algunas) actualizaciones*" (2017) debate el trabajo de Deleuze en lo referido a la instalación de estas nuevas fuerzas correspondientes a la sociedad de control. Para Gendler, llama la atención la casi completa falta de motivos, prácticas, relaciones y estrategias de poder, saber y verdad que ha generado este cambio de fuerzas, ya que, es como si las mismas estuvieran casi *(...) "destinadas a imponerse cual lógica evolutiva-positivista"* (Gendler, 2017, p.5).

La idea de control fue propuesta por Burroughs para designar lo que Foucault reconoció como nuestro futuro inmediato. En estas sociedades se adoptan formas ultrarrápidas de control al "aire libre" que reemplazan a las antiguas formas de control que en la sociedad disciplinaria actuaban en los sistemas cerrados (Deleuze, 1991). Este cambio hace referencia a una respuesta que no sólo implica un desarrollo tecnológico propio del hombre y de sus sociedades, sino que, además, implica una mutación profunda del sistema capitalista. Deleuze propone el concepto de "Sociedad de control" como la nueva sociedad en reemplazo a la disciplinaria la cual iba perdiendo vigencia.

Ahora bien, en "*¿Qué son las sociedades de control*?" (2008) el autor Pablo Esteban Rodríguez sostiene que el concepto de sociedad de control inevitablemente se relaciona con la vigilancia. Apunta que, para Foucault, la vigilancia, en un régimen disciplinario, es un fenómeno individualizador y masificante a la vez, un aparato institucional dedicado a lograr el autodominio del individuo y su sujeción mientras se recaban todos los datos posibles de la ciudadanía vigilada para hacerla entrar en otro régimen de visibilidad: la biopolítica.

Este concepto elaborado por Michel Foucault en 1976 implica una forma específica de gobierno que aspira a la gestión de los procesos biológicos sobre la población. Tiene como eje la regulación de la población, eje alrededor del cual se despliegan los mecanismos de poder sobre la vida de los sujetos. Concretamente, la biopolítica puede ser definida como el conjunto de cálculos y tácticas que intervienen sobre una población mediante la gestión de la vida. Esta noción permite comprender cómo se han generado la organización y el gobierno de nuestras sociedades, buscando promover determinadas formas de vida y dejando de lado otras.

Para Foucault, la vida, ya no del individuo sino de las poblaciones, se convirtió en un objeto político central en el gobierno y en la gestión de las sociedades humanas. Buscando aclarar el contexto en que el gobierno de la vida ocurre, Foucault se desplazó hacia el estudio de la "gubernamentalidad ", entendida como la forma en donde se conduce la conducta en diferentes dispositivos.

Por otro lado, Rodríguez (2008) remarca que dentro de estas sociedades de control no se necesita de la modalidad de encierro como ocurría en la sociedad disciplinaria ya que éstas, en

la actualidad, están relacionadas con las tecnologías y no tanto con las instituciones. La vigilancia es un fenómeno general dentro de las sociedades contemporáneas donde se ha producido una multiplicación tecnológica de dispositivos que permiten la vigilancia masiva.

Rodríguez menciona a su vez que, en el paso del panóptico a la idea de "Big Brother" de George Orwell aparece el paso de una vigilancia "encerrada" a una "vigilancia genérica" donde no existen límites para la visualización de la población y su vigilancia, la cual puede ser "más flexible" y ejercida de manera más discreta, incluso, contando con la aprobación de la ciudadanía vigilada como se observa al hablar de la "política del miedo".

Asimismo, Rodríguez retoma una afirmación de Diego Galeano de su libro *"Gobernando la seguridad: Entre políticos y expertos" (2003)* donde afirma *"(...) las sociedades de control son maquinarias de producción de miedos y de dispositivos para enfrentarlos"* (Rodríguez, 2005, p.120).La presencia misma del miedo como el terrorismo o la criminalidad se vislumbran dentro de las sociedades actuales.

También José Alcántara en su libro "*La sociedad de control: privacidad, propiedad intelectual y el futuro de la libertad"* (2008), define a la sociedad de control como un sistema social pensado para sustituir a las democracias del siglo XVIII y su asamblearismo y se basa en las posibilidades tecnológicas generadas por los desarrollos técnicos a partir de la segunda mitad del siglo XX. Siguiendo al autor, el éxito de su implementación y uso generalizado hoy tiene como uno de sus principales puntos de apoyo la falta deliberada de medidas legales que limiten su utilización para preservar el derecho a la privacidad de la ciudadanía.

La libertad de creación y comunicación que posibilita la sociedad digital y la promesa de crear comunidades más participativas y libres se encuentra condicionada por la vigilancia extensiva sobre la ciudadanía que conlleva un control generado, justamente, por la misma tecnología que profetizaba un futuro con mayor libertad pero que, ha dado como resultado una sociedad con una vigilancia estatal omnipresente. Se produce, entonces, un proceso creciente de desarrollo de estrategia e infraestructura para el control ciudadano por parte de los Estados instalando tecnología de vigilancia que monitorean el espacio público bajo el enmascaramiento de la idea errada, pero aludiendo que las cámaras de vigilancia suponen un instrumento de combate a las nuevas amenazas presentes en las sociedades.

De esta manera, para Alcántara, la sociedad de control es incapaz de defender la democracia porque no nace de ideales democráticos y, por lo tanto, es necesario evitarla mediante la interposición de acuerdos sociales que limiten su accionar y garanticen una sociedad libre que logre alcanzar y gozar de su derecho a la privacidad.

La realización de estas políticas de vigilancia y control suelen ser celebradas y aprobadas por la mayoría de los sujetos que creen que la implementación de estas tecnologías permitirá habitar en un contexto más seguro. Sin embargo, aún existen voces contrarias.

Gendler (2017) remarca este riesgo retomando la tendencia que observa Foucault a fines del siglo XIX: la tendencia a: "(…) *salir del encierro y dejar circular a los individuos en la figura de los dispositivos de seguridad los cuales determinan los espacios y formas de circulación a la vez que se efectúa un procedimiento de normalización"*. (Gendler, 2017, p.9).

Esto implica que las características establecidas de los dispositivos disciplinarios van cambiando y adaptándose a los criterios de normalidad y anormalidad de un determinado régimen configurando, lo que el autor denomina como *"(...)" lo deseable/ correcto", "lo posible" y "lo indeseable/ incorrecto".* (Gendler, 2017, p.9).

Esto se relaciona fuertemente a la gubernamentalidad de Foucault la cual debe ser entendida como

> *"(...) El conjunto constituido por las instituciones, los procedimientos, análisis y reflexiones, cálculos y tácticas que permiten ejercer esa forma bien específica, aunque muy completa de poder que tiene por blanco principal a la población, por forma mayor de saber a la economía política y por instrumento técnico esencial los dispositivos de seguridad".* (Foucault 2006:136).

Asimismo, implica una serie de posibilidades para la acción tanto correcta como incorrecta ante la ciudadanía. Gendler retoma la idea que señala Foucault y sostiene que "(…) *ya que los sujetos son libres de circular y libres de tomar riesgos, la figura del criminal se escinde del encierro para convertir a cualquier hijo de vecino en un potencial sospechoso"* (Gendler, 2017, p.11).

Aquellos que defienden las políticas masivas de vigilancia suelen acotar "si no tienen nada que ocultar, no tienen nada que temer", cuando la esencia de la democracia consiste en la posibilidad de que cada individuo pueda gozar de su privacidad.

A lo largo de este trabajo de investigación se logra percatar que la aplicación de las nuevas tecnologías de vigilancia masiva, propias de las sociedades contemporáneas, generan control, entendiéndolo como una forma de ejercicio del poder, como afirma Gendler en *"De ficciones, tecnologías, controles y errores psyco-pass entre el poder, producción, normalización y la resistencia"* (2017) y considera al poder no como una cosa material y tangible posible de poseer sino como algo que es ejercido

> *"(...) a través de múltiples redes, tecnologías y dispositivos conectados de forma productiva: produce cuerpos subjetividades/subjetivaciones, prácticas, disposiciones y campos para la acción, produce autoridad y disciplinas: produce saberes, deseos y verdades, produce normas y normalizaciones, en definitiva, produce "efectos de poder".* (Gendler, 2017, p 4).

Por lo tanto, para comprender la tensión que se produce entre la implementación de las nuevas tecnologías de control y vigilancia masiva frente al derecho a la intimidad y privacidad, es necesario recuperar la forma en la que Foucault concibe a la ley.

Ernesto Mieles en *"El concepto de derecho, Foucault, la ley y la crítica del paradigma liberal" (*2005) considera a la ley como un efecto del ejercicio del poder capaz de producir sujetos, subjetividades y cuerpos donde la capacidad de subjetivación generada por el poder se basa en una doble estrategia. *"los dispositivos de poder escinden a unos individuos de otros, los aíslan asignándoles unas características y de otro lado, estos dispositivos atribuyen una identidad al sujeto"* (Mieles, 2005, p 4).

El autor sostiene que en todo este proceso son fundamentales la vigilancia y el control desplegados en las sociedades contemporáneas, entendiendo que el poder es "*transversal, estratégico e inmediato*" (Mieles, 2005, p.4)

Por otro lado, Mieles remarca, retomando a Foucault en *"Defender la sociedad"* que el derecho supone una continuación de la guerra a través de otros medios, sosteniendo que la ley, como efecto de la guerra, también es productora de efectos en la sociedad *"Las relaciones de poder tal como funcionan en una sociedad como la nuestra tienen esencialmente por punto de anclaje cierta relación de fuerza establecida, en un momento dado, históricamente identificable en la guerra y por la guerra"* (Mieles, 2005, p.4)

La ley no es estática, sino que se encuentra en constante movimiento y cambio siendo *"un verdadero instrumento de guerra que encubre una estrategia de gubernamentalidad total sobre la sociedad".* (Mieles, 2005, p.5)

Es posible afirmar entonces, que la ley entendida como producción es resultado de batallas entre los ejercicios de saber-poder de actores sociales que conforman un "mapeo" de cómo podrían actuar y moverse los sujetos por la sociedad, pero sin determinarlo del todo, sino orientándolo o conduciéndolo.

4. Renovando lo viejo: El panóptico en la sociedad actual

Desde la aparición del ser humano han existido estrategias y técnicas de vigilancia dirigidas por unos grupos hacia otros. Esta característica es inherente a todas las sociedades humanas donde se produce la estratificación de clase social.

La vigilancia, como un rasgo institucional y omnipresente en las sociedades y como estrategia del ejercicio del poder se fue perfeccionando desde los inicios de la modernidad, vinculándose con el desarrollo de tecnologías que requiere el sistema económico/político capitalista.

En las sociedades contemporáneas y en sus estructuras sociales y políticas se combinan los principios democráticos juntamente con una lógica de vigilancia permanente lo que define a

un nuevo tipo de sociedad utilizado para los avances en el campo de las telecomunicaciones y de la informática.

Este tipo de sociedades evoluciona a la par del desarrollo tecnológico e implica la combinación de la mayor intensidad y sistematización de las tecnologías, siendo la vigilancia la estrategia que parece prevalecer y que podría reemplazar a la coerción física sobre los ciudadanos como un medio de mantener el orden y la armonía dentro de las sociedades.

Foucault en *"Vigilar y castigar*" (1975) sostiene que se ha asistido a la conformación de un nuevo tipo de estructura social que se encabalga con las sociedades de soberanía las cuales utilizaban el suplicio espectacular público como forma de ejemplificación para condicionar al pueblo. Esta configuración societal fue poco a poco perdiendo terreno frente a una nueva sociedad de "vigilancia" que fortalece el perfeccionamiento de los dispositivos disciplinarios que aseguren el control y la normalidad de los sujetos de una sociedad históricamente determinada.

También, Foucault en "*Seguridad, territorio y población*" (1977-1978) asegura que la disciplina actúa aislando a un espacio, a un segmento. La disciplina concentra, encierra, centra y se suscribe a un espacio dentro del cual, el poder y sus mecanismos actúan sin límites. Sostendrá que la disciplina no deja escapar nada, ni siquiera las cosas más pequeñas, sino que todo se encuentra sometido a ella. Afirma, a su vez, que la disciplina procede distribuyendo todas las cosas de acuerdo con un código (el sistema de la ley) que establece lo que está prohibido y lo que está permitido.

Este modelo de sociedad de disciplina descripto por Foucault puede denominarse "sociedad panóptica", la cual estaría caracterizada por reproducir la estructura y el funcionamiento del poder económico, social y político. El modelo panóptico debe ser comprendido como un modelo generalizable de comportamiento, una manera de definir las relaciones de poder en la vida cotidiana de los hombres. Entonces, de acuerdo con la teoría de panóptico de Foucault, dentro de la sociedad disciplinaria se produce la combinación de tres elementos: la vigilancia, el control y el moldeamiento del comportamiento ciudadano hacia uno visto como "correcto". El panóptico es una construcción de "celdas y espacios" donde cada prisionero está individualizado y visible en forma constante a los ojos de quien lo observa y vigila, pero que él no puede ver. El eje "ver sin ser visto" es fundamental en todo sistema de vigilancia.

El individuo que forma parte de esta estructura panóptica se sabe que está en un estado permanente de vigilancia y esto opera en pos de garantizar la docilidad y control de sus movimientos. La garantía de la posible existencia de este sistema alcanza para poner en marcha el engranaje de la relación entre dominante y dominado.

En las sociedades contemporáneas se produce una multiplicación y complejización de relaciones interindividuales que pueden atentar contra la convivencia de los sujetos por lo que es importante garantizar el orden social. Esto se logra mediante el sistema panóptico, el cual se ha visto modificado y transformado a través de la incorporación de nuevas tecnologías y modalidades de vigilancia propias de la sociedad de control, debido a que sus mecanismos de observación son capaces de penetrar en el comportamiento de los hombres produciendo moldear sus cuerpos y prácticas, y asegurar así el orden y la cohesión social. El poder panóptico afianza la docilidad y utilidad de todos los elementos que conforman el sistema capitalista, pero haciendo énfasis, sobre todo, en la vigilancia y el control de la población.

De acuerdo con el escrito de García Jiménez Ricardo "*El panoptismo: nuevas formas de control social,*" (2009), dentro de una sociedad de vigilancia, la burocracia es la cara visible del poder, el cual no es detectado por nadie, pero asegura su presencia mediante las redes por donde circula la información de los sujetos y mantiene alerta al sistema ante alguna señal de sentimiento, emoción o pensamiento propio.

Para Foucault el individuo forma parte de este engranaje de poder, que le marca y caracteriza dentro de un sistema determinando lo que es y no es normal y a partir de esta determinación establece pautas de comportamiento a seguir.

En una sociedad panóptica, el poder, basado en modalidades disciplinarias, se ejerce para intentar imponer una fuerza de homogeneización que garantiza su efectividad operando para desdibujar las singularidades. El poder opera en función de definir la individualidad de las personas en tanto que las clasifica y jerarquiza dándoles una utilidad dentro de un sistema, pero al mismo tiempo, les impide vivir esa singularidad que les concede.

La mirada panóptica cuenta con numerosas herramientas y aliados que garantizan su eficacia. Los mecanismos de vigilancia se han multiplicado al utilizar los medios de comunicación, las corporaciones de telecomunicaciones y la computación, originando que los mecanismos panópticos del poder se intensifiquen y extiendan sus redes atravesando la totalidad de la vida de los individuos y produciéndolos con su vigilancia y control.

Los hábitos de la ciudadanía cambian cuando el panóptico se convierte en una característica de la vida en comunidad y la distinción entre espacio público y privado se torna difusa.

El sujeto pasa a estar vigilado en todo momento y desde todos los ángulos posibles, no sólo en el ámbito público sino también en los espacios cerrados. La persona se halla inserta en un lugar fijo de la estructura social productiva y ante el menor de sus movimientos se encuentra vigilada, controlada y registrada. El control de los ciudadanos se muestra y se mantiene permanente. En

esta sociedad de vigilancia hay siempre una mirada que abarca y sabe todo, que se asemeja a un gran ojo que todo lo ve.

Este tipo de sociedad de vigilancia puede ser definida como una "sociedad de orden y progreso". Según el discurso oficial, este progreso trae beneficios para las grandes masas de sujetos que componen la sociedad, como, por ejemplo, mejoras en las comunicaciones, incremento de la capacidad salarial y aumento de los niveles de vida de los individuos y también para los dueños de los medios y dispositivos de control.

Después de todo, el poder circula por la sociedad. La presencia del poder es evidente en todos los niveles de la vida social, su profusión en redes lo convierte en una ausencia aparente y le otorga un status de inaccesibilidad para la ciudadanía que garantiza su eficacia y su existencia. Dentro del sistema capitalista, la vigilancia se ha institucionalizado y tornado omnipresente en las sociedades, por lo que la forma de control social está relacionada con el impulso de tecnologías y sistemas de creación de vigilancia que buscan la perpetuación del sistema capitalista en una sociedad.

4.1 Mutaciones del panóptico en las sociedades de control

Retomando la idea de panóptico, Vanesa Lío afirma en "*Ciudades, cámaras de seguridad y videovigilancia: Estado del arte y perspectivas de investigación*" (2015) que, a escala social y ampliada, el gen panóptico que existía en las sociedades disciplinarias de Foucault permite mantener una vigilancia constante sobre el conjunto de la población y así regular su accionar.

La autora reconoce que la crisis de las instituciones disciplinarias ha dado lugar a un tipo de control aplicado de manera sistemática en los espacios abiertos actuales originando lo que Deleuze denominó sociedad de control.

Por su parte, Gendler (2017) busca entender el por qué se produce la crisis en la sociedad disciplinaria lo cual no es explicado por Deleuze en su trabajo. El concepto de gubernamentalidad está basado en orientar y desplegar ciertas pautas para la acción, en lugar del "moldeado disciplinario" que ayuda a comprender la modulación constante. Por eso entiende el concepto de modulación constante como

> *"(...) no sólo una continua producción y modificación del cuerpo y de la subjetividad del individuo (apuntando el mismo como cifra) sino también a la producción y modificación constante de los posibles caminos y acciones a ejecutar de acuerdo a las pautas de normalización válidas en un momento determinado"* (Gendler, 2017, p.6).

Gendler (2017) sostiene que siempre existió modulación, incluso en la etapa disciplinaria, pero que la diferencia con la época actual sería la multiplicación de estímulos de información y un mayor refinamiento y domesticación de éstos, lo que da como resultado *"(...) mayor eficiencia y*

posibilidad de orientar los cambios en las individuaciones (producciones) de los cuerpos, subjetividades y accionares de los individuos" (Gendler, 2017, p.6)

Mientras tanto, Foucault sostiene que las ideas de seguridad y libertad no son naturales ni evidentes, sino que pasan a ser construidas en forma histórica dentro de cada sociedad enmarcada en un contexto espaciotemporal determinado. Si bien la aplicación de estas tecnologías de vigilancia, propias de la sociedad de control, permite la libertad de circulación para la población, actúa en forma conjunta con nuevas prácticas de seguridad características del nuevo paradigma de seguridad del siglo XXI como la vigilancia y control masivo de la población, amparados bajo el argumento de luchar contra las "amenazas internas" que pueden surgir desde el seno mismo de las sociedades. La implementación de nuevas prácticas de seguridad genera, por lo tanto, una reglamentación en la forma de circulación de los sujetos por parte del gobierno. Las nuevas medidas de seguridad aplicadas a partir de la implementación de estas tecnologías de control en CABA no implican la suspensión al derecho a circular de la población, pero sí suponen las formas de administrar el tránsito en el espacio público.

Como bien afirma Gendler (2017), en la sociedad porteña no se limita el derecho a la movilidad, sino que la figura del sospechoso se escinde de los espacios de encierro y se traslada al espacio público, donde cualquier *"hijo de vecino"* puede convertirse en un potencial sospechoso de delitos que legal y racionalmente pueden justificar o no el despliegue de estas tecnologías de control y vigilancia como el reconocimiento facial.

Concretamente, en este nuevo escenario, la población de CABA circula tomando en cuenta el despliegue de las tecnologías y prácticas de seguridad aplicadas por las fuerzas de seguridad y el hecho de que éstas no están destinadas exclusivamente a la búsqueda de delincuentes y criminales previamente identificados, sino que, el conjunto de la ciudadanía se constituye en objeto de esta vigilancia permanente en pos de crear una "sociedad más segura".

Esta tesina analiza no sólo el funcionamiento técnico de estos nuevos dispositivos de vigilancia sino también el rol de los actores humanos vinculados a ellos (fuerzas de seguridad y Poder Judicial) y las tensiones con las regulaciones que le dan un marco legal a las prácticas de los distintos actores.

Vanesa Lío (2015) vuelve a los conceptos de Foucault y remarca que son el marco mayormente utilizado para explicar los mecanismos de vigilancia y control dentro de las sociedades contemporáneas. Por eso invita a rever la noción de panoptismo, la cual debe ser revisada a la luz de las nuevas modalidades de vigilancia presentes a partir del desarrollo y expansión de la infra cultura digital. Para ella, ciertas tecnologías que acompañan el monitoreo de las cámaras

de vigilancia como son los sistemas de reconocimiento facial, pueden ser interpretadas como expresión del poder disciplinario del panóptico en los contextos urbanos actuales (CABA en 2019) remarcando que en el contexto posmoderno es necesario pensar también un mundo pos panóptico.

Mientras que el panóptico tradicional requería la presencia de los vigilantes en algún momento, hoy éstos aparecen como invisibilizados o fuera del alcance de la población y la vigilancia y pueden operar a distancia de tiempo y espacio. Por lo tanto, se evidencia que, si bien el panóptico es propio de las sociedades disciplinarias, autores como Vanesa Lío (2015) y Byung-Chul Han (2014) retoman el concepto buscando incorporarlo a la contemporaneidad.

Al profundizar en el escrito de Byung-Chul Han *"En el enjambre*" (2014) se vislumbra la idea de "panóptico digital", el cual se incluye como una especial estructura panóptica dentro de las sociedades de control. Para Han este tipo de panóptico se diferencia del de Bentham al hacer hincapié en que la transparencia no se da por medio del aislamiento de los sujetos entre sí, sino, por el contrario, se produce al aire libre. De esta forma, el control social total se genera por medio de la hiper comunicación y del enlace en red entre los individuos, rasgo predominante de las sociedades y que son características conformadoras del panóptico digital.

Han afirma que, en la actualidad, todo el mundo se ha transformado en un gran panóptico, lo que se puede evidenciar principalmente en las redes sociales, las cuales originalmente nacieron como espacios de libertad, pero, hoy adoptan características panópticas ya que la propia ciudadanía participa activamente en su construcción y conservación al exhibirse de manera voluntaria y sin coacción externa en ellas dejando de lado su privacidad e intimidad y brindando informaciones exclusivas que corresponden a su persona.

Conclusión

En el presente capítulo se ha establecido el marco teórico que se emplea a lo largo de este trabajo de investigación. En él hemos recorrido conceptos fundamentales sobre control social, sociedad de control y el pasaje del capitalismo industrial al capitalismo cognitivo que tiene lugar en el encuadre de las sociedades contemporáneas y que, se torna necesario para lograr la comprensión del fenómeno de la implementación de nuevas tecnologías de vigilancia y control masivo en las sociedades actuales. En particular, se retoma la noción de panóptico el cual, a la luz de los nuevos desarrollos tecnológicos y de las nuevas modalidades y tecnologías de vigilancia; propias de la sociedad de control en los contextos urbanos actuales cabe ser revisado, conservando ciertas características, pero también adoptando otras nuevas: un panóptico digital. Ahondar en estos conceptos es imprescindible para comprender el desarrollo

de esta tesina de investigación, ya que, como veremos, posibilitará el abordaje minucioso de otros ejes conceptuales como lo es el discurso de la política del miedo y el rol de las fuerzas policiales que forman parte de las sociedades de control que atraviesa tanto Argentina como la gran mayoría de las naciones del mundo. La incorporación de estos conceptos es fundamental para llevar a cabo el abordaje de los casos específicos que recupera la tesis para afrontar la problemática planteada. En la presente tesina se analizan los casos de Rachel Holway y Guillermo Federico Ibarrola mediante los cuales se busca demostrar la tensión entre la vigilancia derivada de la aplicación de las tecnologías de reconocimiento facial y el derecho a la privacidad, tirantez característica de la sociedades de control contemporáneas, siendo este un fenómeno que no sólo ocurre en la Argentina, sino que, como se verá a lo largo de este recorrido tiene lugar en múltiples países del planeta, incluyendo a las grandes potencias.

Capítulo 2: Policía, cámaras y videovigilancia

Introducción

A lo largo de este capítulo se realiza una breve genealogía y se abordan las características y particularidades del rol de la policía como la fuerza del Estado encargada del control social dentro de las sociedades contemporáneas. A su vez, se emprende un estudio detallado sobre el surgimiento e implementación de las tecnologías de control y vigilancia tales como: el reconocimiento facial y el sistema de cámaras de videovigilancia, las características técnicas que presentan y su inclusión como instrumentos de control al servicio de las fuerzas de seguridad del Estado. Por otro lado, también se aborda el rol que desempeñan los medios de comunicación, en especial aquellos circunstancialmente aliados del poder político de turno, para difundir discursos, sobre todo, los relacionados con la política del miedo que contribuyen para que la sociedad avale la implementación de nuevas tecnologías de vigilancia y control en el afán de sentirse "más segura".

1. Del rol de la policía

Foucault en *"Seguridad, territorio y población" (1977-1978)* se remite a la cuestión de la policía en relación con la internación de los locos, la medicina de las epidemias y la vigilancia generalizada de la población, principalmente enmarcados en un contexto disciplinario y, en "*Vigilar y Castigar" (1975)* aborda la noción de policía que dentro de sus planteamientos ocupa un espacio más extenso donde los desarrollos más relevantes conciernen a la relación de la disciplina y la ilegalidad.

Por otro lado, Edgardo Castro en *"La noción de policía en los trabajos de Michel Foucault: objeto, límites, antinomias" (2019)* sostiene que, según Foucault, la policía debe ser coextensiva al cuerpo de la sociedad, pero esta característica no es definida por los límites extremos de la misma ni por la totalidad del Estado sino por: *"(...) la minucia de los detalles de los que se encarga"* (Castro, 2019, p.6).

Es en este sentido que la policía podría ser concebida como el equivalente civil de la religión en el interior de las sociedades y por eso los lugares de encierro pueden ser vistos como su "símbolo más denso" y como aquello que, además, confiere una unidad institucional. De esta forma, el objeto de la policía es abordar y administrar todo lo que sucede por pequeño e insignificante que parezca.

Para alcanzar este objetivo las fuerzas policiales y de seguridad deben servirse de instrumentos y tecnologías que hagan posible una vigilancia permanente, exhaustiva y omnipresente capaz de hacer que todo sea visible e invisibilizado al mismo tiempo. Este tipo de vigilancia funciona

a modo de disciplina intersticial y meta disciplina operando entre y por encima de los espacios que conformaban la sociedad. Según Foucault, la policía se propone establecer un ejercicio del poder cuyo objeto sea el individuo y su integración a la totalidad estatal.

Para lograr entender la cuestión de la policía en el trabajo de Foucault es necesario apuntar al poder pastoral. Castro (2019) sostiene que, para Foucault, el poder pastoral se refiere a las formas individualizantes del poder porque en sus orígenes, el poder pastoral se trata de una de las especificidades que caracterizan al cristianismo; *"(...) se propone gobernar la vida de los individuos en sus mínimos detalles, en todas sus acciones, sirviéndose de una determinada verdad y proponiéndoles alguna forma de salvación y verdad a partir de la cual exigirles obediencia"* (Castro, 2019, p. 9-10)

El escrito de Castro retoma la conferencia de Foucault *¿Qu`est-ce que la critique? (1978)* donde se remarca que a partir del siglo XVI se ha producido una multiplicación de las formas del ejercicio del poder según la modalidad del "pastor" (pastoreo), tanto en la política como en la sociedad

> *"(...) Si el pastorado perdió en su forma estrictamente religiosa lo esencial de sus poderes, encontró en el Estado un nuevo soporte y un principio de transformación. La policía moderna es una de estas transformaciones que se define por ser una forma individualizante de ejercicio de poder en beneficio del Estado mediante la integración de los individuos en su totalidad"* (Castro, 2019, p.10)

Para Foucault tanto la policía como el aparato diplomático militar son dispositivos del cual se sirve la razón del Estado para consolidar, mantener y aumentar sus fuerzas.

Retomando el escrito de Louis Turquet de Mayerne "*La Monarchie Aristodemocratique" (1611)* afirma que el verdadero objeto de la policía es el hombre. A todos los hombres se les otorga lo que el autor denomina "suplemento de vida" que es utilizado a fin de acrecentar y consolidar las fuerzas del Estado. Castro (2019) define la policía como *"(...) el conjunto de leyes y reglamentos que conciernen al interior de un Estado, que tienden a afirmarlo y aumentar su potencia, a emplear de buena manera sus fuerzas procurando la felicidad de los hombres".* (Castro, 2019, p.14). Esta definición considera a la policía como una acción positiva del Estado cuyas intervenciones consolidan y acrecientan la vida social y la potencia de éste. Desde esta perspectiva, la policía puede ser vista como un conjunto de intervenciones y medios que aseguran que, el vivir y el más que vivir, el coexistir, será útil para la constitución y el fortalecimiento de las fuerzas del Estado.

El surgimiento y la presencia de la policía en las sociedades también responde a la necesidad de que existan dispositivos de seguridad (Foucault, 2006), mecanismos regulatorios que permitan el funcionamiento del "accionar libre" de los individuos centrado en su circulación.

Es en este sentido que Foucault considera a la policía como mecanismos que intervienen en la gestión de esta "libre circulación", como *"(...) la gubernamentalidad directa de los soberanos"* (Castro, 2019, p.18).

Para el abordaje de este capítulo es necesario analizar el pensamiento de Foucault respecto de la relación entre la policía y la legalidad. Para ello ayudará retomar el trabajo de Máximo Sozzo "*Policía, gobierno y racionalidad: Incursiones a partir de Michel Foucault"* (2011) donde se establece que los términos de la ley siempre son interpretados y la misma interpretación conlleva una actividad donde prima la creatividad y la subjetividad de los individuos a pesar de que la ley no dé lugar a una pluralidad infinita de sentidos posibles.

Sin embargo, esto abre un espacio para que "*diversos intérpretes postulen diversas formas de ver la actividad policial con relación a un mismo texto legal y ese conflicto sobre la interpretación legal es un conflicto político en el que se enfrentan actores que poseen diversas fuerzas"* (Sozzo, 2011, p.35).

A su vez, el autor afirma que las legislaciones, con respecto a las fuerzas policiales a lo largo de la historia y en la actualidad han estado marcadas por la laxitud y la falta de control.

> *"Los términos de la ley con respecto a la policía han sido y son, por lo general, suficientemente vagos y ambiguos para acomodar prácticamente cualquier actividad policial realizada en post fact. Y en esto mucho ha tenido que ver el rol de la misma institución policial"* (Sozzo, 2011, p.35).

Esto se verá más claramente analizado a lo largo de este trabajo, sobre todo, al enfocar los casos de análisis de Holway e Ibarrola donde se contempla el accionar de las fuerzas de seguridad y la tensión que conlleva estas prácticas con los derechos de la ciudadanía.

Jesús Requena Hidalgo en "*De la sociedad disciplinaria a la sociedad del control: la incorporación de nuevas tecnologías a la policía*" (2004) mira a la policía como fuerza que compone las fuerzas de seguridad del Estado y que se caracteriza por ser una institución que, a raíz de los cambios observados previamente en torno a la incorporación de tecnologías digitales, lleva a cabo una actividad de naturaleza eminentemente informacional que ha estado marcada por la incorporación de éstas.

Es decir, a lo largo de su existencia, la metodología de trabajo de la policía ha ido cambiando y modificándose y las formas de definir y controlar los espacios urbanos y su rol como depositaria del monopolio legítimo del ejercicio de la vigilancia sobre la población se ha visto trastocado.

En este sentido, Hidalgo (2004) afirma que, desde el surgimiento de los servicios de policía a mediados del siglo XlX, éstos han contribuido al mantenimiento de los aparatos estatales suministrándoles información a la vez que constituían un mecanismo de administración de la

violencia legítima. Esto es clave ya que la capacidad del Estado administrativo ha dependido, desde sus orígenes, del conocimiento de la sociedad y de sus miembros, en especial, sobre aquellos que se consideraba como portadores de una "conducta desviada". De manera que la policía vino a romper el monopolio que hasta ese momento había tenido el poder judicial en torno a lo que involucraba la desviación social pues se trata de poderes adjuntos diseñados para disolver el desorden de la ciudad.

Dentro de estos estados administrativos, el poder panóptico se reprodujo a través de instituciones como la policía, dando lugar en el siglo XX a un "poder sin afuera" donde las sociedades se constituirán como espacios abiertos a la vigilancia generalizada.

Con la sociedad de control, las fuerzas que conforman el aparato represivo del Estado han incorporado dispositivos que llegaron al campo de la seguridad desde el sector militar como la televigilancia, la videovigilancia o las bases de datos, tecnologías de alta eficacia que permiten la consolidación de dicha sociedad de control.

1.1 Mismos jugadores, nuevos juguetes: Tecnologías para la vigilancia policial

Dentro de las tecnologías centradas en la observación y el control de las personas se engloban las cámaras de videovigilancia que incorporan tecnología de reconocimiento facial permitiendo la identificación y seguimiento de la población.

El discurso más extendido sobre la incorporación de estos dispositivos tecnológicos a las fuerzas de seguridad radica en la creciente complejidad social, en la sofisticación de las prácticas criminales y en las exigencias que la ciudadanía transmite a sus gobernantes como resultado de la política del miedo. Estas tecnologías de control y vigilancia social han alumbrado una nueva manifestación espacial de poder.

Como se ha visto en el capítulo anterior, en la sociedad de control, la tradicional separación entre espacio público y privado se disuelve generando una publicitación del espacio privado y privatización del espacio público, lo que implicaría una desterritorialización y una des institucionalización del control permitiendo su presencia en todo espacio y lugar.

Hidalgo (2004) remarca que las tecnologías de información y comunicación admiten que el poder logra funcionar sin espacios que le sean propios, apropiándose de todos los espacios. La tecnovigilancia, propia de las sociedades de control, accede a los espacios donde anteriormente las prácticas del ejercicio del poder por medio de las fuerzas de seguridad no llegaban o donde la libertad podía ser legítimamente limitada pero que hoy, pueden ser espacios interpretados en la misma medida.

De acuerdo con el estudio del trabajo de Milton Lechner *"Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social"* (2016) se puede afirmar que las transformaciones ocurridas en las sociedades durante las últimas décadas han modificado la propia naturaleza del delito, produciendo que las propias instituciones cambiaran su mirada sobre la problemática delictiva.

El desarrollo de las tecnologías de información, comunicación y vigilancia se han ido aplicando paulatinamente como herramientas utilizadas para combatir la criminalidad y como respuesta a las demandas de seguridad de la población. En este sentido *"(...) Los estados se han tecnificado con métodos y diseños tanto de prevención como de punición contra los delitos"* (Lechner, 2016, p.4).

Para este autor, el desarrollo de las tecnologías digitales se complementa con las tecnologías de control y vigilancia para "(…) *generar una reducción de la incertidumbre y el riesgo social como una protección ante las amenazas".* (Lechner, 2016, p.5).

Muchas de las tecnologías de control y vigilancia con las que operan las fuerzas de seguridad han surgido con fines militares y posteriormente trasladado al ámbito civil. Algunas de ellas son el reconocimiento biométrico, los sistemas de geolocalización y el sistema de video vigilancia a los cuales se debe incluir el reconocimiento facial. Estas tres tecnologías de control y vigilancia se encuentran vigentes y operando por parte de la policía de la Ciudad en CABA desde el 2019 como se observará en los capítulos siguientes.

La presente tesina se centra en el uso de los sistemas de videovigilancia los cuales según Lechner *"(...) se constituyeron en una forma de vigilancia sobre la totalidad de sus ciudadanos y sus instituciones alcanzándose así niveles de control social nunca antes observados".* (Lechner, 2016, p.6).

Si bien los sistemas de videovigilancia y reconocimiento facial son implementados como herramientas de prevención y disuasión del delito, también pueden ser empleados como tecnologías de carácter represivo ya que resguardan la información por un tiempo determinado para luego aplicarla en el momento en que ocurre un delito.

Lechner (2016) asegura que en las fuerzas de seguridad se observa un avanzado desarrollo e innovación tecnológicos que permite la aplicación de estas tecnologías de control y vigilancia a dispositivos móviles como drones aéreos o patrulleros, posibilitando que los sistemas de videovigilancia no estén estáticos sino, por el contrario, posean movilidad dentro del espacio público ampliando así su alcance de acción.

2. Entre balas, cámaras y periodistas: Del rol de los medios de comunicación y la vigilancia en la sociedad de control

Al analizar la temática de la tesina es necesario volver a mencionar que, en el pensamiento de Michel Foucault, la idea de poder está más ligada a la producción que a lo represivo como lo corrobora Juan Fernando Delgadillo (2012) en *"Foucault y el análisis del poder"*.

El poder dentro de la lógica foucaultiana busca la producción de conductas, cuerpos y subjetividades dentro de la población. Para poder ejercerlo, el poder requiere una economía que Foucault denomina "discursos de verdad".

El trabajo de Delgadillo retoma una cita de Foucault que ilustra esta afirmación *"Estamos sometidos a la producción de la verdad desde el poder y no podemos ejercitar el poder más que a través de la producción de la verdad"* (Foucault, 1992 p.148).

Desde esta perspectiva de Foucault, la noción de verdad implica un conjunto de reglas que permite discriminar lo verdadero de lo falso. Un conjunto de procedimientos que se ven reglamentados por la producción, la circulación y la prensa en funcionamiento de los enunciados en un determinado momento histórico.

Por lo tanto, la verdad es presentada como un producto histórico originada a través de prácticas de poder e instituciones de naturaleza coactiva que configuran la conducta y los comportamientos de los sujetos, "*después de todo, somos juzgados, condenados, clasificados, obligados a competir, destinados a vivir de cierto modo o a morir en función de discursos verdaderos que conllevan efectos específicos de poder"* (Foucault, 1992 p.148)

Es posible sostener que el rol de los grandes medios de comunicación al desplegar discursos, específicamente, aquellos relacionados con la política del miedo, contribuyen a la producción de conductas de la población pudiendo generar como efecto una parcial pero potencial resignación de su derecho a la privacidad e intimidad frente a la aplicación de tecnologías de vigilancia masiva por el solo hecho de sentirse más segura frente a las amenazas internas de terrorismo o criminalidad que denuncia la dirigencia política. Es decir, al hacer referencia a la política del miedo; inexorablemente se debe mencionar el rol que juegan los medios de comunicación masivos. Cabe remarcar que ellos poseen su propia agenda temática y muchas veces también parecieran operar como repetidores y amplificadores del discurso transmitido por la clase política. Es decir, si bien los medios no son simples cadenas de transmisión de estos discursos, muchas veces colaboran con la clase dirigente en la producción de efectos de verdad respecto de varios tópicos, entre ellos "la política del miedo". El discurso transmitido por la dirigencia política y replicado o también producido por los medios de comunicación

masiva pasa a formar parte de la agenda mediática y de la agenda pública de las sociedades, las cuales determinan aquellos temas que serán debatidos en la misma.

Entonces, para entender correctamente el análisis del tema planteado en esta tesina, es necesario comprender el funcionamiento del aparato mediático y su impacto sobre la realidad de la sociedad.

Es interesante entender el trabajo de José María Rubio Ferreres *"Opinión pública y medios de comunicación. Teoría de la agenda setting"* (2009) donde se retoma la teoría de la construcción social de la realidad elaborada por Berger y Luckmann (2006) y se estudia en qué medida la imagen del mundo social es elaborada por la influencia de los medios de comunicación.

Dentro de esta teoría, el modelo más exitoso a la hora de explicar los efectos generados por los medios masivos y sus relaciones con la opinión pública ha sido la denominada "teoría de la agenda setting", la cual enfatiza el poder de los medios de comunicación para atraer la atención del conjunto de los sujetos hacia determinados temas o problemas (inseguridad/criminalidad) estableciendo marcos de interpretación de estas temáticas.

De acuerdo con la teoría del Framing los medios de comunicación actúan como intermediarios entre el hombre y aquella realidad externa que no puede captar por sí mismo. Los medios masivos le comunican al sujeto esa realidad a la que no puede acceder por sí mismo, realidad que está construida por la llamada frames (encuadres o marcos). Es como consecuencia de estos procesos que algunos aspectos de la realidad transmitida por los medios sean más prominentes que otros.

Así lo afirma Natalia Aruguete en *"¿Paraguas común o teorías independientes*? *El debate entre agenda setting, priming y framing*" (2017)

> *"El framing es definido como un proceso integral que atraviesa todas las instancias de la comunicación y como tal, aparece en la elaboración de las noticias, en los textos noticiosos, en los esquemas de cognición y percepción de las audiencias y, fundamentalmente en la cultura"* (Aruguete, 2017, p.98)

Como se viene analizando, la dirigencia política argentina y también la de múltiples naciones junto a otros actores sociales, como grupos empresarios y medios de comunicación, han recurrido a la política del miedo para obtener el consenso de la población a la hora de aplicar las tecnologías de vigilancia. Sin embargo, es imposible omitir el rol de los medios de comunicación masivos en este escenario que mediante sus coberturas periodísticas transmiten o producen construcciones de hechos delictivos enfatizando, sobre todo, aquellos *frames* que exacerban la sensación de peligro y amenaza hacia la sociedad, donde prima el relato

sensacionalista que contribuye a aumentar el alarmismo y el miedo de ser víctimas en todo momento.

Dentro de la agenda setting de los medios argentinos el delito ocupa un lugar central. Y si bien se sabe que la ciudadanía no es total y absolutamente manipulada por los medios de comunicación, la presentación constante de hechos de criminalidad, transmitidos mayormente desde una lógica amarillista y alarmista que, si no lo es, roza el sensacionalismo, contribuye a que la sociedad toda tenga como una de sus preocupaciones centrales la problemática de la inseguridad y exija al gobierno de turno la aplicación de medidas de prevención y combate (más cámaras, más policías, más móviles) que contrarresten la amenaza de la inseguridad.

Indudablemente los medios de comunicación poseen su propia agenda mediática a la hora de construir y transmitir las noticias, pero, es imposible omitir que en las sociedades democráticas se produce una alianza estratégica entre algunos medios de comunicación y el gobierno de turno, como sostiene Silvia Pellegrini en *"Medios de comunicación, poder político y democracia"* (1993) donde remarca que *"Los gobiernos y también los partidos políticos establecen verdaderos sistemas informativos dentro del sistema a través de las formas en que diseminan la información o se insertan en los medios para lograr la atención pública*". (Pellegrini, 1993, p.13)

A través de sus discursos, los medios buscan brindar a la ciudadanía la sensación de que el poder de turno está tomando las medidas pertinentes para neutralizar aquellas amenazas que se ciernen sobre la sociedad, pero omiten los riesgos que conllevan para la privacidad e intimidad enfatizando únicamente en los "beneficios" que implica establecer un mayor control sobre el espacio público.

No se desconoce que los temas presentes en la agenda mediática suelen ser bastante similares en los diferentes medios de comunicación de Argentina. Sin embargo, la cobertura periodística realizada acerca de la temática de inseguridad y despliegue de tecnologías de control y vigilancia es diferente de acuerdo con el medio que transmite y/o produce estos discursos y a los intereses económicos y políticos a los cuales responde.

Los medios de comunicación desempeñaron un rol muy importante en la guerra de Vietnam (1955-1975) ayudando a conformar a través de su contenido periodístico una opinión pública estadounidense cada vez más contraria a la guerra denunciando el accionar de las fuerzas militares y siendo uno de los factores fundamentales en la primera derrota militar de la historia de Estados Unidos. Los medios estadounidenses no se contentaron con realizar coberturas esporádicas de la guerra de Vietnam. La cobertura de la realidad del conflicto en el sudoeste asiático fue constante hasta que la opinión pública norteamericana se despertó y se movilizó para exigir al gobierno el fin de un conflicto que tuvo un alto costo para los Estados Unidos.

Esto se refleja en el trabajo de Leyre Merino Fernández *"La influencia de los medios de comunicación en el desarrollo de las guerras contemporáneas*" (2018) donde el autor retoma el pensamiento de Luis Martín Aragonés (1998) *"La formación de la opinión pública contraria a la guerra que presionó al gobierno y propició el final de la misma, no se habría configurado sin las imágenes proporcionadas por los medios de comunicación".* (Fernández, 2018, p.26)

Idealmente, los medios de comunicación masivos deberían cumplir un rol central dentro de esta "guerra preventiva" llevada a cabo en las sociedades actuales, y unirse a las voces de las ONGs y de los académicos, asumiendo la naturaleza crítica que les corresponde por su protagonismo social para alertar a la ciudadanía sobre los riesgos que implican las tecnologías de control y vigilancia sobre los derechos. Sin embargo, conocemos que esta afirmación remite más a un escenario que puede rozar con lo utópico y no ignoramos que los medios de comunicación, como actores sociales, también responden a sus diversos intereses en el contexto de las sociedades contemporáneas.

3. Características de los nuevos sistemas de seguridad

El desarrollo de las tecnologías de control y vigilancia, como los sistemas de reconocimiento facial o de control biométricos, actualmente son implantados en las sociedades con el argumento de que serán utilizadas para aumentar y garantizar la seguridad de la ciudadanía, combatiendo y previniendo los actos delictivos.

La Real Academia Española en su diccionario define la palabra "*seguridad"* como "cualidad de seguro" mientras que califica al término *"seguro*" como "libre" y "exento de todo *peligro, daño o riesgo"* entendiendo al "*riesgo"* como "*contingencia o proximidad de un daño".*

Sin embargo, en el texto *"Las Nuevas Tecnologías Aplicadas a la Seguridad" (2007)* los autores Félix Martínez, Francisco Blanco Ruiz y Juan José Prieto Viñuela afirman que estas definiciones son perfectas desde el punto de vista semántico, pero distan de ser cercanas a la realidad de las sociedades contemporáneas ya que, la libertad y la extensión de todo riesgo implican un estado de perfección imposible de ser alcanzado por el individuo. Para ellos la seguridad total no existe y por más que se implante un conjunto de medidas y desarrollos tecnológicos que busquen aumentar la protección, siempre seguirán existiendo "riesgos residuales" entendiéndolos como contingencia o proximidad de daños que el ser humano tendrá que asumir de alguna forma.

En el caso de las tecnologías digitales como el reconocimiento facial, estas contingencias o daños colaterales para la población serán la pérdida de su privacidad, el robo y/o el mal manejo de sus datos personales y sensibles por parte de las grandes corporaciones comerciales o del

aparato represivo del Estado. Y aunque en muchas ocasiones, estos "daños colaterales" son "invisibilizados" en las comunidades, no son motivo de tratamiento mediático por parte de los medios masivos y, por ende, la mayoría de la ciudadanía los termina ignorando.

De manera que, Martínez, Blanco Ruíz y Prieto Viñuela (2007) sostienen que la seguridad es la sensación de protección frente a riesgos y amenazas que sean deliberadas o no y que logren ser percibidas por el ser humano, las comunidades o Estados. Para ellos el concepto de seguridad y defensa hace referencia al Sector de la Seguridad "*las actividades englobadas en las áreas de Seguridad Pública y Colectiva, gestionadas directamente por las autoridades y el área de la Seguridad Privada"* (Martínez, Blanco Ruiz, Prieto Viñuela, 2007, p.3).

Este sector es muy vasto y encierra múltiples áreas, con fronteras difusas entre sí y por eso puede resultar complicado establecer en qué áreas se encuadran determinadas actividades del sector. Sin embargo, las relaciones entre los subsectores de la Defensa y Seguridad son tan significativas que no es fácil marcar su separación.

Los autores enumeran una serie de características respecto a la aplicación en las tecnologías en el Sector de la Seguridad:

- ***Utilización masiva de las Tecnologías de la información y Comunicaciones (TIC):*** La introducción de estas tecnologías en el sector se ve justificado por generar un incremento en la productividad de estos sistemas de vigilancia. La implementación de las TIC permite romper con las barreras espacio temporales y posibilita la adaptabilidad a situaciones cambiantes.
- ***Sinergias con las tecnologías desarrolladas en el ámbito de la defensa:*** Las fronteras entre Seguridad y Defensa son permeables. Buena parte de las funcionalidades requeridas por los sistemas de Seguridad son las mismas empleadas por las defensas, por lo que puede hablarse de una convergencia entre ambos sectores, la cual no es total sino parcial porque no puede alcanzarse en otros campos de actividad de estos sectores como los sistemas de armamento.
- ***Dualidad tecnológica entre Defensa y Seguridad***: Pese a que se afirma que hay un proceso de convergencia entre ambos sectores en cuanto a tecnología de vigilancia como son los sistemas de reconocimiento facial y los sistemas biométricos, los sistemas de seguridad no cuentan con especificaciones tan exigentes como en el caso de los sistemas militares.
- ***Disponibilidad de tecnología:*** Existe el sentimiento de que casi todas las tecnologías son accesibles tanto para los gobiernos como para las empresas privadas pero que el reto de éstas radica en su aplicación de manera eficiente.

- ***Tendencia a la actividad de integración de sistemas***: Las empresas del Sector de Seguridad están tendiendo a la adquisición de componentes y tecnologías en el mercado para obtener el valor añadido en el diseño, instalación y mantenimiento de los sistemas. Esto se ve justificado porque son enormes mercados globalizados o tecnologías muy sofisticadas de grandes costos de desarrollo. En la mayoría de los casos se trata de tecnologías procedentes del ámbito de la Defensa o de aplicaciones críticas para la seguridad que cuentan con financiamiento o subsidio por parte de organismos oficiales de los Estados.
- ***Influencia de la legislación sobre la aplicabilidad de las tecnologías:*** Las soluciones tecnológicas a los problemas de seguridad o vigilancia no pueden ser aplicables debido a limitaciones asociadas a las legislaciones correspondientes a cada país. La normativa jurídica sería, en muchos casos, la que definiría qué tecnologías son útiles y cuáles no. Sin embargo, en el caso argentino, el manejo poco claro y transparente del Estado en el uso de las tecnologías de reconocimiento facial y sistemas biométricos podría implicar violaciones a las legislaciones argentinas que fueron elaboradas para salvaguardar la privacidad y la confidencialidad de los datos personales y sensibles de la ciudadanía. Las leyes de protección de privacidad quedarían subordinadas al sistema de vigilancia y control implementado desde el Estado y ejecutado por las diversas fuerzas de seguridad que componen su aparato represivo bajo el argumento de estar generando una sociedad más "segura".

3.1 No mires y no sonrías, te estamos filmando: Cámaras y videovigilancia

De acuerdo con el trabajo de Lío (2015) la incorporación de los sistemas de vigilancia y control que utilizan imágenes para realizar sus prácticas no es nueva "*(...) la primera técnica fotográfica comercialmente viable fue patentada en París en 1839 y para mediados de la década siguiente ya había sido descripto su potencial para identificar y capturar criminales."* (Lío, 2015, p.2)

Situación similar se vivió con el desarrollo de la TV en el siglo XX con la idea de que las imágenes en vivo podían desempeñar un rol central en la rutina de los patrullajes. Por lo tanto, la relación entre imágenes, fuerza de seguridad y seguridad en el espacio público se ha ido profundizando en las inmediaciones del siglo XXI como afirma la autora:

> *"(...) La relación entre las imágenes, la policía y la seguridad pública se profundizó en dimensiones impensadas. Las políticas de seguridad gubernamentales incorporaron sistemáticamente los circuitos cerrados de televisión (CCTV) para monitoreo del espacio público entre sus tecnologías para el control social y la prevención situacional del delito"* (Lío 2015, p.2)

En los últimos años esta situación se complejiza con el desarrollo de tecnologías como las de reconocimiento facial que permiten la identificación de los individuos y su seguimiento. Es posible observar la fuerte vinculación que se produce entre las tecnologías para el control social, la prevención situacional del delito y las tecnologías que funcionan por medio de imágenes. Lío (2015) afirma que, si bien estas tecnologías para control social comenzaron a implementarse en países del primer mundo, posteriormente comienzan a utilizarse en todo el resto. *"(...) Utilizada inicialmente en Europa y en América del Norte, la videovigilancia se ha expandido hacia los cinco continentes, convirtiéndose en una de las principales herramientas al servicio de la seguridad ciudadana"* (Lío, 2015, p.3).

Como se verá a lo largo de los capítulos, a estas tecnologías se las puede considerar como un arma de doble filo que pone en grave peligro la privacidad. El uso de estas técnicas de vigilancia y control social se ha ido complejizando con la utilización de diversas tecnologías de seguimiento y recolección de datos sin consentimiento de la población ya que no sólo obtienen información sensible de los individuos, sino que actúan complementando los sistemas de monitoreo.

La vigilancia se ha transformado tecnológicamente con el paso del tiempo y presenta particularidades de acuerdo con cada contexto local y a cada cultura, por lo que las respuestas sociales y políticas pueden variar de acuerdo con el país.

La videovigilancia comenzó formando parte de las tecnologías desarrolladas para el control de los reclusos y el éxito obtenido en el ámbito carcelario hizo pensar a las autoridades que su utilización también daría buenos resultados al aplicarse a la ciudadanía, considerada como mucho más numerosa pero más mansa y menos conflictiva que los presos. Actualmente, debido al costo relativamente bajo, estas tecnologías de control y coacción se han instalado en el espacio público de las metrópolis, y se aplican a una población que goza del principio de inocencia como si se tratara de un ámbito carcelario. Lío (2015) sostiene que la aplicación de sistemas de monitoreo con cámaras de seguridad en el espacio público puede remitir a la realidad que George Orwell describió en 1984 donde existía el ojo del "Gran Hermano" que todo lo veía.

Según su visión, los sistemas de monitoreo CCTV han pasado de utilizarse para monitoreo de flujo de la población a ser usados para la identificación de individuos puntuales y funcionan como la interface humana para nuevas aplicaciones de banco de datos. Esto permite contextualizar el desarrollo de los sistemas de monitoreo como una tecnología de vigilancia que se inserta en el modelo de poder descripto por Foucault acerca de la división de los grupos en unidades medibles. Asimismo, sustenta que la inclusión de estas tecnologías de control y

vigilancia cambia la forma en la cual es ejercido el poder, modificando las experiencias emocionales en el espacio urbano y afectando la forma en la que la realidad es conceptualizada y estudiada.

Por su parte, Alcántara (2008) apunta que, en muchos gobiernos de sociedades contemporáneas, con el argumento de aumentar la seguridad de la población, se ha recurrido a la implementación de tecnologías de control y vigilancia que en su función original respondían a una técnica represiva dirigida a poblaciones mayoritariamente conflictivas, como, por ejemplo, los reclusos del sistema penitenciario. Sostiene que a partir de la década de 1980 se ha incrementado la implementación de sistemas masivos de vigilancia con control biométricos y de cámaras con reconocimiento facial no sólo en países centrales como China o Estados Unidos, sino también en países periféricos como Argentina. Esto responde a la necesidad de los gobiernos de llevar a cabo una vigilancia de todo lo que sucede tanto en el ámbito privado de la ciudadanía como en el público. Para el autor, ello implicaría poner en suspenso el principio de inocencia del que gozan todos los habitantes de la nación ya que los sistemas de vigilancia masiva instalarían una lógica donde se presupone de antemano la culpabilidad de todos los sujetos y, por ende, la necesidad de una férrea vigilancia sobre cada uno.

Esto se vincula a lo mencionado por Gendler (2017), que como hemos visto, retoma esta cuestión al afirmar que, en las sociedades contemporáneas, todo ciudadano es susceptible de ser considerado como sospechoso por las fuerzas de seguridad.

La potencialidad de culpabilidad de toda la ciudadanía y la necesidad de imponer sobre ella un control, necesariamente obliga al Estado a delegar la función de vigilancia en los dispositivos mecánicos, como cámaras, que incluyan funciones de reconocimiento facial y/o sistemas de control y vigilancia biométrica. Debido a la gran cantidad de población que se debería vigilar, estos dispositivos informáticos reemplazarían y complementarían a los integrantes de las fuerzas de seguridad que componen el aparato represivo del Estado.

Los nuevos desarrollos e innovaciones aplicados a tecnologías de vigilancia permiten que los gobiernos realicen en sus espacios públicos prácticas de vigilancia masiva de la ciudadanía con relativa facilidad y rapidez.

Alcántara reconoce que

> "(…) c*on el aumento de la capacidad de cálculo de las computadoras y la mejora del software de reconocimiento de objetos y rostros en fotografías y grabaciones de video, esta tecnología se presenta como un arma potencial de represión, dada la posibilidad de comunicarle al sistema en tiempo real dónde estamos y qué estamos haciendo*". (Alcántara, 2008, p.170).

A pesar de que en las sociedades contemporáneas parecería que la mayoría de la población expresa su conformidad con la aplicación de estas nuevas tecnologías de control, el desconocimiento y opacidad del funcionamiento de estos sistemas de vigilancia y la creciente desinformación de la ciudadanía ante su instalación en el espacio público brinda como resultado un sistema institucionalizado de vigilancia que puede escapar al control civil pero avalado por ella por medio de la política del miedo. De este modo, el sistema de videovigilancia en espacios públicos ha logrado un gran avance en los países donde la mayoría de los sistemas de vigilancia y control son operados por autoridades locales pero sustentadas por una política clara de gobierno central como el caso de la República Popular China, Estados Unidos de América o Argentina.

Sin embargo, a pesar de la instalación masiva de estos sistemas, ello no implica necesariamente una efectiva reducción del crimen. La introducción de cámaras de videovigilancia y reconocimiento facial podrían no eliminar la criminalidad sino desplazarla a otros sectores no controlados por éstas, por lo cual el crimen no sería eliminado sino corrido de sitio. El recurso político de estos sistemas de vigilancia y control no tienen que ver solamente con su efectividad como instrumento para combatir el delito, ya que su valor simbólico radica en la sensación que logra la ciudadanía de saber que la dirigencia política está implementando políticas en relación con el problema, generando en las personas una sensación de protección. Este punto conforma una explicación para el masivo crecimiento de los sistemas de videovigilancia y reconocimiento facial pues se recurre al sentido común de los habitantes que indica que "estos sistemas de vigilancia deben funcionar". Su popularidad y la necesidad de las gestiones políticas de turno de ser vistos como "activos" en el combate de la criminalidad, por un lado, y la publicidad generada alrededor del tema en casos específicos por otro, tiene un alto impacto mediático[5]

[5] Un ejemplo de estos acuerdos se observa en el encuentro realizado entre el presidente de Argentina, Mauricio Macri y el presidente de los Estados Unidos, Barack Obama entre el 23 y 24 de marzo del año 2016. Entre los diversos puntos tocados en la reunión, se destaca el convenio de intercambio de información entre ambos países en delitos tales como el narcotráfico, así como también la capacitación y el entrenamiento de las fuerzas de seguridad de la Argentina en el combate de este delito por parte de las fuerzas estadounidenses. Ambos mandatarios acordaron establecer una "colaboración bilateral en la creación de un Centro de Fusión de Inteligencia a través del cual se concentrará la información de las distintas agencias de seguridad, en vistas a que dicha información sea compartida entre las distintas fuerzas de seguridad de los dos países, la cual permitirá ganar eficacia en la lucha contra el crimen organizado**.** De igual modo, resulta muy importante la asistencia que los Estados Unidos brindarán al país para mejorar la seguridad fronteriza." Véase: https://www.cancilleria.gob.ar/userfiles/prensa/c-16-082_0.pdf

4. Características técnicas del reconocimiento facial

En los últimos años, el reconocimiento facial se ha convertido en una de las aplicaciones más estudiadas en campos como la biométrica, procesamiento de imágenes, reconocimiento de patrones, visión por ordenador y redes neuronales.

Una de las razones que ha llevado al crecimiento y empleo de estos sistemas de vigilancia y control social es la necesidad de mayores aplicaciones de seguridad y vigilancia para ser utilizadas en diferentes ámbitos sociales.

Cuando se menciona a los sistemas de vigilancia y control basados en el reconocimiento facial, se habla de aplicaciones dirigidas por ordenadores que permiten la identificación automática de ciudadanos en imágenes digitales captadas por el sistema de cámaras que tiene integrado este sistema[6].

De acuerdo con el trabajo de David Leonardo Castaño Saavedra y Juan David Alonso Sierra *"Sistemas de reconocimiento facial para control de acceso a vivienda"* (2019), el reconocimiento facial es una tecnología que está siendo implementada en múltiples áreas de investigación como análisis de imagen o extracción de características de archivos digitales. Según los autores, esta tecnología puede emular la capacidad del ser humano de reconocer personas imitando un funcionamiento específico de partes puntuales del cerebro humano.

> "*Los neurocientíficos las llaman áreas faciales. Estas zonas toman ciertas características faciales de la persona a reconocer como el color de la piel, tamaño de ojos, nariz y características únicas de cada persona y todo esto es un actividad semiinconsciente dado que en algunas ocasiones el cerebro hace este reconocimiento sin que la persona se percate, teniendo esto en cuenta esta tecnología quiere replicar esta función siguiendo una serie de pasos como detención facial, análisis de características, comparación con base de datos*."(Castaño Saavedra y Alonso Sierra, 2019, p.41).

Estos sistemas, con el objetivo de determinar la identidad de una persona, pueden tener en cuenta el análisis de múltiples características del sujeto que busca identificar. Las características pueden ser físicas (el análisis de las pupilas o la geometría del rostro) donde la cara del individuo se convierte en un objeto tridimensional sujeto a variaciones de luz y también psicológicas (los gestos que realiza el sujeto).

Estas propiedades implican sus propias peculiaridades que pueden ser analizadas siguiendo determinados criterios que, conforme al trabajo de Carmen Sánchez Ávila "*Aplicaciones de la biometría a la seguridad"* (2012) son:

- ***Universalidad:*** Indica características comunes en todas las personas u objetos que buscan ser reconocidos.

[6] Véase http://www.emb.cl/channelnews/articulo.mvc?xid=2209

- ***Carácter distintivo:*** Indica una propiedad diferente entre un conjunto de personas u objetos.
- ***Permanencia***: Indica la estabilidad temporal de una determinada característica.
- ***Colectividad***: Indica si la característica es fácilmente adquirida y medida por el sistema.
- ***Rendimiento:*** Indica la precisión, velocidad y costo de recursos necesarios para llevar adelante el reconocimiento.
- ***Aceptabilidad:*** Indica la disposición de la ciudadanía para aceptar la implementación de estas medidas de vigilancia.

  Estas propiedades permiten describir bien las características que buscará implementar el sistema de reconocimiento facial y determinar si es adecuado o no para este tipo de aplicaciones.

  De esta manera, los sistemas de vigilancia pueden operar de diferentes modos:
- ***Verificación o autentificación de caras***: Compara imágenes de un determinado rostro con la cara de la cual se quiere conocer la identidad. El sistema de reconocimiento facial confirmará o rechazará la identidad de la cara[7].
- ***Identificación o reconocimiento de caras***: Comparará la imagen de una cara desconocida con todas las imágenes de rostros conocidos que se encuentran en la base de datos que utiliza el sistema para determinar la identidad.

El reconocimiento facial se destaca por ser una técnica con una alta capacidad de respuesta frente a las múltiples características biométricas de los individuos que son objeto de identificación del sistema. Pero, las aplicaciones basadas en este sistema presentan inconvenientes a la hora de llevar a cabo las identificaciones porque puede generar errores, los denominados como "falsos positivos". Existen factores que pueden generar error en el sistema de vigilancia[8]. Cabe mencionar entre ellos:

- Orientación del rostro del sujeto cuando es captado por el sistema
- Ruido
- Iluminación
- Expresiones faciales
- Oclusión debido a objetos o accesorios que los sujetos pueden utilizar en sus rostros (anteojos de sol, sombreros, etc.)

---

[7] Véase https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial
[8] Véase https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial

- Vello facial

Algunos de estos factores que pueden llevar al error del sistema, como el envejecimiento de los individuos, se logran solucionar mediante la aplicación de un algoritmo que interprete el paso de los años en la persona que se busca identificar, aunque esta solución no es del todo fiable. Una forma eficaz para resolver este inconveniente es la actualización de las bases de datos que utilizan los sistemas de vigilancia para realizar las identificaciones.

Esto implica que necesariamente las fuerzas de seguridad de los Estados deban realizar sistemática y periódicamente una actualización de los datos del conjunto de los habitantes de una sociedad, sean éstos posibles sospechosos o no de actos de criminalidad y delincuencia ya que a través de la aplicación de estos sistemas los gobiernos dicen buscar, enfrentar y prevenir dichos actos.

Conclusión

En este capítulo hemos recorrido el concepto de fuerza policial aplicado al contexto de las sociedades de control en el mundo contemporáneo, las cuales han llevado a cabo una fuerte incorporación de nuevas tecnologías de control y vigilancia como el reconocimiento facial y nuevas modalidades de ejercer el control en el espacio público, sea la población digna de sospecha o no. Profundizar en el concepto y rol ejecutado por las fuerzas policiales en las sociedades de control es necesario para la comprensión de la temática de esta tesina debido a que, serán las fuerzas policiales las encargadas de ejercer, al menos en parte, el control social que impera en las sociedades actuales.

Además, y entrando en diálogo con otros conceptos que serán presentados en capítulos posteriores, aquí se enfatizó el rol de los medios de comunicación en el marco de las sociedades de control entendiéndolos como un factor fundamental en el proceso de implementación de las nuevas tecnologías de control y vigilancia y también respecto de sus efectos. En este sentido; la operatoria suele ser caracterizada por una alianza estratégica entre algunos medios de comunicación y la dirigencia política de turno de manera que, respondiendo también a sus propios intereses, logran difundir los discursos transmitidos por parte de la dirigencia política de turno (o crear posicionamientos propios) sobre el fenómeno de la inseguridad y narcotráfico en la Argentina. De este modo, los medios de comunicación masiva en muchas oportunidades contribuyen a exacerbar los discursos de la práctica de gubernamentalidad, llamada “política del miedo” instalando en la agenda mediática y social el temor a las amenazas internas que plantea el nuevo paradigma de seguridad del siglo XXl el cual se trata en el próximo capítulo.

El temor a estas amenazas provoca que la sociedad exija un accionar por parte de la dirigencia política y, por ende, otorgue a cambio una mayor aceptación hacia la implementación de nuevas tecnologías y modalidades de vigilancia que derivan en un mayor auge de las sociedades de control y el consiguiente proceso de tecnologización de las fuerzas policiales como se ha analizado. También, en este capítulo se ha profundizado en las características técnicas propias de las nuevas tecnologías de vigilancia como el reconocimiento facial, las cuales establecen una serie de riesgos para los derechos inalienables de todo ser humano, como lo es el derecho a la privacidad e intimidad.

A lo largo de los próximos capítulos se aborda específicamente la operatoria de las fuerzas de seguridad y de las tecnologías de vigilancia, además de los discursos de la dirigencia política argentina y la cobertura mediática de algunos de los casos más relevantes de CABA en el 2019 en los que se centra esta tesina. Asimismo, se enuncian otros casos a nivel global con el objetivo de demostrar que la sociedad de control es una configuración de poder (Deleuze, 2017) desplegada a nivel global para luego verse traducida a nivel nacional y local adaptando las particularidades en cada territorio.

Capítulo 3: Vigilancia a nivel global

Introducción

Este capítulo aborda y profundiza sobre el cambio de paradigma de seguridad implementado en el mundo contemporáneo a finales del siglo XX y comienzos del XXI. Los cambios en la doctrina de seguridad que llevan a la práctica las naciones a través de un íntimo vínculo con las tecnologías digitales generando como efecto la aplicación de sistemas de vigilancia y control como las cámaras de reconocimiento facial y nuevas modalidades de vigilancia por parte de las fuerzas de seguridad son respaldadas por la llamada "política del miedo" mediante la cual, un amplio abanico de actores sociales, incluyendo las dirigencias políticas, buscan exacerbar y aumentar los miedos de las sociedades (miedo al terrorismo o a la criminalidad) y obtener así el respaldo de la ciudadanía frente a la implementación de tecnologías aunque éstas pongan en jaque el derecho a su privacidad.

Esta nueva realidad encuadrada dentro de la lógica de la sociedad del control poco a poco empieza a extenderse e implementarse en gran parte del planeta. Aquí se hará referencia a casos específicos de Estados Unidos y China, dos naciones que han implementado la nueva doctrina de seguridad y han desplegado una vigilancia masiva sobre su población a través de la aplicación de tecnologías de control dentro del espacio público.

1. Contame una historia de terror: El discurso de la política del miedo y los cambios en el paradigma de seguridad

José Alcántara en "*La sociedad de control" (2008)* afirma que "(…) *en todas las sociedades y los Estados siempre ha existido un cierto nivel de vigilancia"* (Alcántara, 2008, p.75)

La vigilancia puede convertirse en una herramienta provechosa cuando es bien empleada, ya que, en caso de sospecha sobre alguien o algo, permitirá mantener un cierto orden social en las comunidades. Sin embargo, a lo largo del siglo XX y XXI, diversos gobiernos, en múltiples naciones, han implementado la idea de utilizarla como parte de una política de seguridad y la han empleado contra la oposición política, social, cultural o minorías étnicas y raciales, como se verá en el presente capítulo al observar los casos de China y Estados Unidos.

En numerosas sociedades contemporáneas, incluida la comunidad argentina en 2019, la clase política utiliza lo que Alcántara (2008) y Gendler (2017) denominan "Política del miedo", la cual constituye una nueva forma de entender a la política.

> *"(…) Los discursos políticos no enfatizan las promesas de un futuro mejor, sino que abundan en profetizar el catastrofismo derivado de no obedecer al pie de la letra lo que nos está ordenando el político de turno. Si tradicionalmente la política ha consistido en desarrollar acciones que desembocarían en un futuro mejor y en*

> *explicarlas al pueblo para ganar su apoyo, la política del miedo recurre a la seguridad (generalmente la seguridad nacional) para obtener el apoyo incondicional de la ciudadanía a una serie de medidas políticas que de otra forma no serían respaldadas"* (Alcántara, 2008, p.78).

Eventualmente se presenta al pueblo una serie de amenazas que lo ponga en riesgo (terrorismo o criminalidad) y acepte así un avance sobre sus derechos esenciales con la promesa de poseer a cambio una sociedad más segura, mediante la implementación de tecnologías de vigilancia masiva.

Alcántara remarca que la aplicación de la "política del miedo" responde a una realidad social en la cual, la dirigencia política ha incumplido las promesas realizadas a la población a lo largo de décadas, lo que ha ocasionado un descreimiento de los discursos políticos, por lo que *"(...) Los políticos necesitan algo más para recobrar su influencia y es ahí donde la generación de miedo les gana la partida a las simples promesas de bonanza económica y social"* (Alcántara, 2008, p.78).

Esta afirmación se puede verificar claramente en la sociedad argentina, donde uno de los principales ejes en los discursos de los políticos, se encuentren o no en campaña electoral, es el combate a la criminalidad e inseguridad. Estas temáticas toman un lugar central dentro de las preocupaciones de la sociedad por lo que el autor menciona *"(...) a diferencia de las promesas de antaño, ahora los más influyentes no serán aquellos que prometan el mejor futuro, sino aquellos que azuzando los miedos más oscuros puedan conseguir más concesiones de la población"* (Alcántara, 2008, p.86)

En los primeros años del siglo XXI, a raíz de los atentados que golpearon a las principales potencias occidentales, como el caso del ataque al World Trade Center en Estados Unidos el 11 de septiembre del 2001, se han implementado una gran cantidad de medidas que generaron una vigilancia masiva y sistematizada sobre las poblaciones en nombre de la seguridad. Estas políticas ya venían siendo planeadas y desarrolladas por los Estados con anterioridad a ser víctimas del terrorismo, pero los ataques perpetrados constituyeron la excusa perfecta y la coyuntura ideal para implementarlas en forma masiva, consolidando una política de restricción de los derechos y libertades de la ciudadanía.

El texto de José María Blanco Navarro *"Seguridad e Inteligencia 10 años después del 11-S" (2011)* aborda los cambios en el paradigma de seguridad luego del ataque terrorista del 11/9/2001. En ese sentido, el atentado a las torres gemelas del World Trade Center sacudió al mundo entero e implicó fuertes cambios en las sociedades. Afectó múltiples aspectos como los derechos y libertades de los ciudadanos, generando una "*cultura de la seguridad"*, instalando una sensación de temor constante en los habitantes. Los cambios en el paradigma de seguridad, ocurridos a principios del siglo XXl crearon cambios no sólo en el nivel práctico de la vigilancia

que llevan a cabo las naciones, sino que provocó también fuertes transformaciones en torno a las políticas de seguridad implementadas por lo que, Alcántara expresa

> *"(...) Tras este cambio en la forma de hacer política, la doctrina de guerra preventiva se hace más fuerte y se aplica tanto en los ámbitos internos como externos. La idea de que para prevenir atentados desde dentro hace falta controlar qué hacen los ciudadanos del propio país gana cada vez más adeptos entre los dirigentes políticos de todo el mundo"* (Alcántara, 2008, p.86-87).

La idea de poder ser alcanzados en todo tiempo y lugar por un acto de terrorismo o de crimen y el cambio en el paradigma de seguridad afecta aspectos éticos y legislativos de las sociedades contemporáneas. En este sentido, *"el miedo produce un efecto demoledor en ellas transformándolas en manipulables"* (Navarro, 2011, p.6). Por lo tanto, el miedo actúa como un factor central que le otorga a los gobiernos una capacidad de ejercicio del poder desplegada en forma de instalar dispositivos de vigilancia y control masivos como cámaras de videovigilancia y reconocimiento facial que pueden implicar una pérdida de los derechos a la privacidad e intimidad que poseen los ciudadanos.

Justamente, el gran temor social que impera en la actualidad en cuanto al delito o al terrorismo ha llevado a que los gobiernos limiten, con la aplicación de tecnologías de vigilancia, algunos de los derechos básicos de la población. Esta situación ha generado posiciones encontradas. Por un lado, se genera la postura de que una ciudadanía sufra una progresiva limitación de sus derechos y que se manifiesta para lograr recuperarlos en contraposición a otra postura que, frente al miedo que experimenta, acepta de buen grado limitaciones en sus derechos siempre que éstos le brinden una "mayor seguridad".

Del atentado del 11/9/2001 se deriva el surgimiento de múltiples reformas legislativas orientadas a disponer de mecanismos adecuados para que los gobiernos enfrenten la amenaza tanto en el plano internacional como en el interior de las propias sociedades. Los ataques terroristas sufridos produjeron fuertes transformaciones y cambios en el paradigma de seguridad no sólo en los Estados Unidos sino a nivel global.

Una de las leyes más emblemáticas establecidas por el gobierno de George W. Bush en octubre del mismo año fue realizada con el objetivo de prevenir y combatir los actos de terrorismo provenientes tanto del interior como del exterior del país norteamericano. Esta ley denominada "*Linting and strenathening América providing aproprinte tods required to intercep and obstrvet terrorism act*" (USA patriot act)[9] permitió ampliar las capacidades de control de las

[9] Reforzar y fortalecer a América proporcionando los documentos apropiados y necesarios para interceptar y obstruir el acto terrorista (Acta Patriótica de Estados Unidos)

diversas agencias de seguridad del país y dotarlos de nuevas capacidades de vigilancia para combatir la amenaza terrorista interna y externa. Sin embargo, la Ley de Acta Patriótica ha recibido fuertes críticas por haber avanzado contra derechos humanos tales como la privacidad y las libertades civiles establecidas por la Constitución estadounidense.

Esta situación se refleja en el trabajo de Franklin Barrientos Ramírez *"La política antiterrorista de Estados Unidos"* (2008), donde se retoma el pensamiento de Donohue (2005) al afirmar que

> *"Todo gobierno liberal y democrático está obligado a responder ante una amenaza como el terrorismo o la delincuencia mediante leyes especiales, leyes de excepción, pero transitorias. El gobierno, a su vez, está obligado a balancear la tensión entre democracia liberal y seguridad porque puede ocurrir que pasada la emergencia sea muy difícil revocar las medidas transitorias que limitaban la libertad y los derechos civiles"* (Barrientos Ramírez,2008, p.16)

Barrientos Ramírez (2008) también enfatiza en los efectos que la Ley de Acta Patriótica provocó en el derecho a la privacidad e intimidad de la población cuando retoma el trabajo de Meeropol (2004) *"El Acta Patriótica atenta contra la libertad y privacidad de las personas permitiendo un incremento de los poderes de vigilancia y espionaje electrónico a las agencias encargadas de cumplir la ley, especialmente al FBI". (*Meeropol, 2004 citado en Barrientos Ramírez, 2008, p.18)

Debido a los nuevos poderes concebidos, muchos derechos individuales de la población podían ser vulnerados en ausencia de dispositivos judiciales, lo cual ha originado que estas medidas sean fuertemente criticadas por los defensores de los derechos y libertades civiles.

El atentado asimismo trajo otro cambio significativo: la denominada "cultura de la seguridad" observada en declaraciones de organismos internacionales años antes del ataque a las torres gemelas.

El Consejo de Seguridad de la ONU, el 31 de enero de 1992 ya advertía que "*las fuentes no militares de inestabilidad en los ámbitos económico, social, humanitario y ecológico se han convertido en amenazas para la paz y la seguridad".* (Navarro, 2011, p.16).

Dentro de estas fuentes no militares se podría incluir al terrorismo y a la criminalidad consideradas como grandes amenazas dentro de las sociedades contemporáneas. Esto llevó a que la mayoría de las estrategias de seguridad nacional configuren sistemas de prevención y protección basados en la aplicación simultánea de nuevas herramientas las cuales pueden tornarse en instrumentos de vigilancia y control policial como son las cámaras de video vigilancia y de reconocimiento facial.

En Argentina, muchos de los discursos de "la política del miedo" se refieren al combate de la inseguridad y narcotráfico presentes para obtener el apoyo del pueblo en la implementación de

medidas políticas que, de otra manera no serían posibles debido al rechazo popular, ya que implican un recorte al derecho de la privacidad y una vigilancia masiva de la población.

Alexis Romero, Raima Rujano y José del Nogal en *"Control social: nuevas realidades, nuevos enfoques" (2002)* sostienen que

> *(...) "La alta prevalencia de delitos violentos condiciona la vida pública de las sociedades contemporáneas. Esta situación se agrava por la incapacidad del Estado para garantizar las funciones del sistema judicial y del aparato de seguridad, los cuales están comprometidos en la prevención, detención y captura de los criminales".* (Romero, Rujano, Del Nogal, 2002, p.4).

Para los autores, tanto el poder judicial como las fuerzas de seguridad del Estado han experimentado una crisis de legitimidad debido a los resultados negativos en su lucha contra la criminalidad y su participación en actos de corrupción. En un intento por limpiar su imagen y mostrar una mayor eficacia en estos asuntos, desde los Estados y específicamente, desde el Estado argentino, se impulsa la implementación de tecnologías de vigilancia y control masivos, que afirman ser poderosos instrumentos tecnológicos para la identificación y captura de prófugos de la justicia.

El ejemplo más reciente se refleja en CABA, en el 2019 donde, en el marco de las elecciones generales del 10 de octubre, el jefe de gobierno porteño Horacio Rodríguez Larreta afirmó "*Gracias a las nuevas cámaras de seguridad que pusimos con reconocimiento facial apresamos a 1600 delincuentes que estaban prófugos, violadores, ladrones, asesinos que caminaban libremente por las calles. Yo propongo que en el próximo mandato vamos a instalar 10 mil nuevas cámaras más con reconocimiento facial"*[10].

Gendler (2017) sostiene la importancia del miedo como mecanismos de gubernamentalidad que permite justificar muchas de las tecnologías, regulaciones legales y prácticas implementadas y que aseguran su legitimación. Estas políticas de las sociedades actuales enfatizan el terror, incentivado por grupos que amenazan al conjunto de la sociedad como delincuentes o terroristas. Vistos como "puntas de lanza" para lograr la implementación de políticas de vigilancia y control sobre la ciudadanía albergan el potencial de violar la privacidad personal.

El autor también menciona que la política del miedo da "luz verde" a los gobiernos contemporáneos para instaurar medidas de vigilancia y control masivo como es la instalación de cámaras de videovigilancia con reconocimiento facial que permiten la identificación y monitorización de los ciudadanos en todo tiempo y lugar, lo que ha modificado el concepto de

[10] Véase https://informepolitico.com.ar/ciudad-chicanas-entre-larreta-y-lammens-en-el-debate-entre-candidatos

seguridad y pasa a establecer un "Estado de seguridad" (Agamben 2015), generando que el Estado de excepción se torne una regla *"(...) la seguridad que está hoy en cuestión, hoy no apunta a prevenir los actos de terrorismo sino a establecer una nueva relación con los hombres que es la de un control generalizado y sin límites"* (Gendler, 2017, p.11).

Si bien la tesina analiza la implementación de las tecnologías de videovigilancia y reconocimiento facial en CABA en 2019, observando puntualmente las tensiones producidas entre el derecho a la privacidad y la vigilancia constante desempeñado por los dispositivos de seguridad en el espacio público, a lo largo de este capítulo se contemplan algunos casos significativos de la República Popular China y los Estados Unidos de América, naciones que han sido pioneras en desplegar e implementar el nuevo paradigma de seguridad, ejerciendo una vigilancia generalizada sobre sus poblaciones.

Se toman como ejemplo el caso de estas dos naciones que poseen fuertes diferencias políticas, ideológicas y culturales pero que se encuentran a la vanguardia en múltiples áreas, en especial, en lo que respecta a la vigilancia. Tanto China como Estados Unidos son potencias mundiales que se disputan la supremacía a nivel global en numerosos campos: económico, político, militar y tecnológico. Los dos países han enfatizado fuertemente el desarrollo tecnológico aplicándolo a áreas como la producción industrial pero también al área de defensa, innovación militar y vigilancia.

Estos elementos constituyen factores interesantes para observar la implementación de las cámaras de videovigilancia y reconocimiento facial en ambas naciones, las cuales, a pesar de sus múltiples diferencias, realizan una vigilancia y control masivo sobre su población en el espacio público, lo que permite conocer en tiempo real en qué lugar físico se encuentran y con quién, aun cuando la ciudadanía, susceptible de ser vigilada, no ha cometido falta alguna que amerite un control omnipresente de las fuerzas de seguridad del Estado.

La aplicación de estas tecnologías mencionadas opera sobre la población mediante el registro y almacenamiento de grandes cantidades de datos privados de los sujetos. Estos datos contienen información de naturaleza sensible y privada sobre cada habitante, la cual es almacenada en grandes bases de datos estatales sin que la ciudadanía tenga claro con qué fin es utilizada o qué información personal se encuentra en poder del Estado.

Al tomar como ejemplo del nuevo paradigma de seguridad tanto a Estados Unidos como a China, es importante recordar que ambas potencias mundiales actúan marcando tendencias y rumbos en materia de seguridad, las cuales pueden ser implementadas por otras naciones en mayor o menor medida.

Abordar y recorrer ambos casos en este trabajo de investigación ayuda a visualizar a nivel mundial la puesta en práctica y la materialización de la configuración de las sociedades de control y su implementación, como la puesta en funcionamiento en los ámbitos diarios y cotidianos de las poblaciones de múltiples países más allá de las particularidades sociales e ideológicas de cada nación.

Según Lío (2015), Argentina, país periférico, ha implementado las nuevas tecnologías de control y vigilancia de forma posterior a otras regiones del mundo, así como también la adaptación de nuevas modalidades de control por parte de las fuerzas de seguridad que ya existían previamente en las potencias mencionadas.

> *"(...) El monitoreo de espacios públicos en manos del Estado aparece ya avanzada la primera década del siglo XXI, alcanzándose mayores niveles de extensión y cobertura en los últimos años. Esta difusión de los CCTV tuvo como marco la profundización en Argentina del modelo preventivo en torno a las políticas públicas de seguridad"* (Lío, 2015, p.21)

2. No es un cuento chino, la vigilancia es real: República Popular de China y el control de la población.

La República Popular China es una nación que ha iniciado una carrera vertiginosa para consolidarse como una de las principales potencias del planeta. Su exponencial desarrollo económico y tecnológico la ha posicionado en el centro de las miradas mundiales. Sin embargo, su desarrollo tecnológico aplicado a las fuerzas armadas y de seguridad también le posibilita al país llevar a cabo una extensa gestión sobre su población mediante tecnología de vanguardia como el reconocimiento facial. El control realizado por el gobierno ha despertado fuertes críticas y cuestionamientos por parte de reconocidos organismos como Human Rights Watch.

De acuerdo con el texto de Oscar Aribau Sorolla "*Las TIC y la ciber soberanía en China, la base del presidente Xi Jinping para perfeccionar el control social Maoísta" (2018)*

> *"(...) Las estructuras de poder de cualquier sociedad independientemente del sistema político elegido para su organización han mirado con desconfianza el ámbito privado de los ciudadanos y lo ha considerado como una parte oculta e inaccesible donde podría gestarse y germinar cualquier revuelta que terminara con el sistema político vigente*" (Sorolla, 2018, p.3).

El gobierno chino ha implementado sistemas de vigilancia masiva para monitorear, rastrear y perseguir a millones de ciudadanos tanto a nivel general como también particular, como el caso de aquellos que conforman minorías étnicas y grupos religiosos, como la minoría islámica etnia uigur en la región de Sinkiang. China ha recurrido al uso de tecnologías y sistemas de vigilancia y control masivo como la utilización de la inteligencia artificial (IA) para procesar y analizar

grandes cantidades de datos obtenidos por medio del reconocimiento facial instalado en cámaras de videovigilancia, biometría, GPS y cámaras CCTV de alta resolución.

Estos sistemas de vigilancia y control masivo instalados en todo espacio disponible se complementan con redes de informantes y presencia policial constante, lo que genera una sociedad de control muy invasiva que pone en jaque el derecho a la privacidad de la ciudadanía.

La actual situación que atraviesa China se contradice con lo expuesto en el Pacto Internacional de Derechos Civiles y Políticos (ICCPR) establecido por la resolución 2200A (XXI) de la Asamblea General de Naciones Unidas en 1966, puesto en vigor en 1976 y firmado por China en 1998.

En pocas palabras, el ICCPR tiene el objetivo de reconocer los derechos civiles y políticos y los mecanismos para garantizar su efectivo cumplimiento y protección. En el preámbulo del pacto se afirma que los derechos contemplados en el mismo son derivados en forma inherente de la dignidad de la persona humana y reafirma que "*la carta de Naciones Unidas impone a los Estados la obligación de promover el respeto universal y efectivo de los derechos y libertades humanas*"[11]. Tanto el ICCPR como la Declaración Universal de los Derechos Humanos conforman lo que se denomina Carta Internacional de Derechos Humanos. El Pacto Internacional de Derechos Civiles y Políticos en su artículo N°17 protege el derecho a la privacidad del hombre al establecer que:

1) *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o correspondencia ni de ataques ilegales a su honra y reputación".*
2) *"Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."*

El ICCPR ha tenido una fuerte aceptación internacional ya que 167 estados lo han ratificado. De acuerdo con el trabajo de Sorolla (2018) los gobiernos de la República Popular China han buscado avanzar sobre el derecho a la privacidad de su población desde mitad del siglo XX

> *"(...) Desde su llegada al poder en 1949, el partido comunista chino (PPch) ha definido la intimidad y el círculo privado de los ciudadanos como los grandes enemigos del sistema. Durante casi 70 años el PPch y sus diferentes líderes han basado su hegemonía y legitimidad en la eliminación del adversario y de la crítica, en el control absoluto de todos los ámbitos de la sociedad, la desaparición del ámbito privado de los ciudadanos transformando en público todos los ámbitos sociales e individuales al transformar lo privado en público, el partido ha conseguido extender su control a todas las esferas de la sociedad*". (Sorolla, 2018, p.4)

Según la mirada del autor, la implementación de nuevos mecanismos de control y vigilancia dentro de la sociedad china tiene sus orígenes en los cambios económicos que ha

[11] Véase http://www.derechoshumanos.net/normativa/normas/1966-PactoDerechosCivilesyPoliticos.htm

experimentado la nación y la consecuente apertura de su economía hacia el mercado internacional, lo que implicó que el aspecto económico antes controlado y planificado por el gobierno necesitara de un intercambio constante de información.

Si bien en el trabajo se afirma que en un primer momento el gobierno chino resistió la idea de incorporar en forma masiva las tecnologías de digitalización, la llegada al poder en 2012 del presidente Xi Jinping cambió el escenario en el interior del gigante asiático.

> *"(...) No fue hasta la llegada al poder del presidente Xi Jinping en 2012 cuando el gobierno chino empezó a utilizar toda la potencialidad de las TIC en su propio beneficio, es decir, como arma para mantener y recuperar la legitimidad perdida desde el inicio de las reformas económicas".* (Sorolla, 2018, p.5).

El sistema de vigilancia chino está compuesto por 3 ejes centrales: la recopilación masiva de datos, la vigilancia casi total mediante medios técnicos y humanos y el análisis y gestión de datos de la ciudadanía a través de operaciones avanzadas de inteligencia artificial y coordinación de naturaleza militar.

Esta combinación resulta en una sofisticada base de datos nacionales que les permite a las fuerzas de seguridad que conforman el aparato represivo del Estado, rastrear, analizar y controlar a la población en tiempo real.

China ha instalado 176 millones de cámara de vigilancia para controlar una vasta población que ronda más de 1000 millones de habitantes. Para el año 2020 busca aumentar la cantidad de cámaras a 626 millones e incorporar más cámaras CCTV en zonas rurales y cámaras con reconocimiento facial más avanzado y con "reconocimiento de marcha" (software que permite la identificación de un ciudadano por su forma de caminar).

Estas tecnologías están expandiéndose en forma silenciosa e invisible pero rápidamente en ciudades como Shanghái y Pekín haciendo que China se transforme en uno de los lugares más vigilados del mundo.

Por otro lado, en el gigante asiático también se ha implementado un plan masivo denominado *Ranking de seguro social*[12] y es aplicado por parte del gobierno. Consiste en la creación de un "sistema de crédito social" a través del cual se colocan puntos por el comportamiento individual a los millones de habitantes del país de acuerdo con sus conductas, generando así un "Ranking de confianza". La información recogida por el gobierno chino proviene de múltiples aspectos de la vida social: pago de impuestos, multas y la forma de obtención de los títulos académicos. El proyecto fue presentado en el 2014 por el Consejo de Estado Chino. Este plan permite a aquellos ciudadanos que posean una buena puntuación acceder a una serie de beneficios como

[12] Véase: https://www.bbc.com/mundo/noticias-internacional-41970041

descuentos en hoteles, accesos a planes de seguro u obtener visados en forma más ágil. En cambio, si la puntuación del sujeto baja de cierto nivel, las consecuencias podrían llevar a perder el acceso a determinadas instituciones educativas, trabajos o créditos hipotecarios. Esta medida implica que la población china se encuentra bajo una vigilancia permanente y al aire libre en sus conductas individuales y colectivas por parte del aparato estatal aun cuando no representen una amenaza real o potencial para la seguridad de la sociedad.

2.1 Sociedad de Control y reconocimiento facial en China: algunos casos ejemplo

2.1.1 La policía china usa gafas con reconocimiento facial para identificar a sospechosos

Las fuerzas policiales de diferentes ciudades chinas, entre ellas Zhengzhou, capital de la superpoblada provincia de Henan, han sido equipadas con gafas oscuras, las cuales incorporan una cámara de video que permite captar la cara de los transeúntes y cruzar la información con las bases de datos policiales buscando coincidencias con la lista de sospechosos de haber cometido un crimen. El sistema no está limitado a identificar posibles criminales, sino que permite verificar toda la identidad de las personas escaneadas por las gafas.[13]

De acuerdo con las declaraciones de Zhang Xiaolei[14], portavoz del Departamento de Seguridad Pública de la provincia de Henan que realizó al periódico estatal Global Times, este nuevo sistema de vigilancia sólo necesita una imagen del rostro del individuo para identificarlo a diferencia de los sistemas de vigilancia anteriores que requerían múltiples fotografías tomadas desde diferentes ángulos para su identificación.

En los últimos años China ha dado un impulso significativo a las tecnologías de inteligencia artificial aplicadas a la vigilancia de la ciudadanía, un sector que el Partido Comunista gobernante considera de vital importancia estratégica. Sin embargo, estos avances puestos a disposición de las fuerzas de seguridad chinas son vistas con preocupación por parte de los críticos debido a sus implicaciones en términos de privacidad porque podrían ser usadas como medio para sofocar la disidencia en el país.

[13]Notas publicadas en https://elpais.com/internacional/2018/02/07/mundo_global/1518007737_209089.html https://elcomercio.pe/tecnologia/ciencias/china-reconocimiento-facial-vigilar-2-5-millones-habitantes-noticia-609576-noticia/

[14]Véase https://conlagentenoticias.com/la-policia-china-usa-gafas-con-reconocimiento-facial-para-identificar-a-sospechosos/

2.1.2 La etnia Uigur y la vigilancia

Durante la Conferencia Internacional sobre Internet, entre el 4 y 5 de diciembre del 2017[15], se realizó en China una exposición a cargo de Mei Jianming, experto en antiterrorismo del panel Intergubernamental Organización de Cooperación de Shanghái, que incluye a China y Rusia. Allí Jianming denunció como terroristas a los grupos que defienden los derechos humanos de la minoría islámica etnia Uigur en la región de Sinkiang, China, en la cual, según la denuncia de la organización[16] Human Rights Watch, el gobierno chino ha creado bases de datos biométricos (huellas dactilares y escaneo del iris) como forma de identificar y controlar a los disidentes y miembros de esta etnia.

Sinkiang, en el noroeste de China, es conocida oficialmente como la Región Autónoma Uigur de Sinkiang y su mayor grupo étnico está formado por los uigures con el islam como su religión mayoritaria. Este territorio ha servido como campo de pruebas para algunas de las técnicas de vigilancia y control más intrusivos y represivos que ha concretado el régimen chino.

El territorio se encuentra bajo intensa vigilancia policial desde hace varios años porque el gobierno lo considera necesario para enfrentar a grupos extremistas y separatistas. El sistema de vigilancia mediante coordenadas de GPS y reconocimiento facial establecido por las autoridades chinas implica un control masivo sobre aproximadamente 2.5 millones de personas, muchas pertenecientes a la minoría islámica de la etnia Uigur.

Según Fergus Ryan, analista y experto en China, perteneciente al Instituto Australiano de Política Estratégica (ASPI), estas tecnologías han sido implementadas como "parte de la represión contra uigures, kazajos y otras minorías étnicas realizadas por Pekín"[17]porque el territorio de Sinkiang fue *"un gran campo de pruebas para este tipo de tecnologías de vigilancia"*.

El gobierno chino ha sumado nuevas herramientas a su repertorio de sistema de vigilancia basados en el uso del mecanismo de "Big Data"[18]. Por ende, los procedimientos usados para encontrar patrones repetitivos dentro de esos datos son más sofisticados y requieren software especializado. Asimismo, sumó la inteligencia artificial que ha dado como resultado un software de reconocimiento de marcha que permite identificar a los ciudadanos chinos incluso

[15] Véase https://www.nytimes.com/es/2017/12/11/espanol/conferencia-internet-china-monitoreo-vigilancia.html

[16] Véase https://elpais.com/tecnologia/2017/12/14/actualidad/1513243284_855531.html y https://es.bitterwinter.org/el-estado-de-vigilancia-de-alta-tecnologia-de-china/

[17]Véase https://www.abc.net.au/news/2019-02-18/chinas-mass-surveillance-of-uyghur-muslims-revealed-in-data/10820634

[18] Término referido al conjunto de datos tan grandes y complejos como para que hagan falta aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente.

a 50 metros de distancia o cuando su rostro no es visible a la cámara de vigilancia (rostro cubierto o el sujeto esté de espaldas a la cámara) gracias a la forma característica de su cuerpo y su modo de andar, lo que implica un software de reconocimiento corporal.

Esta tecnología ya ha sido implementada en las dos mayores ciudades de China: Pekín y Shanghái por parte de las autoridades de seguridad chinas que pretenden utilizarla como un complemento a la tecnología de vigilancia basada en el reconocimiento facial.

Esta tecnología fue creada por Watrix, compañía de inteligencia artificial líder en China, enfocada al análisis de grandes cantidades de datos por video. Las tecnologías centrales de Watrix son las de reconocimiento de marcha más avanzada y las de visión industrial líder. La compañía ha proporcionado soluciones de inteligencia artificial para seguridad, transporte, fabricación y otras industrias.

El Ceo de la compañía es Huang Yongzh[19] y afirma que una de las ventajas que ofrece esta tecnología es que *"no precisa de la cooperación de la gente para que podamos conocer su identidad* "y avisa que *"el análisis de la marcha no es algo que se pueda engañar cojeando o encorvándose ya que analiza todas las características de un cuerpo entero".*

La empresa responsable de su desarrollo sostiene que la precisión es sólo del 94% por lo que es lo suficientemente bueno para su explotación comercial.

Organizaciones como Human Rights Watch han afirmado en numerosas ocasiones que mediante estos sistemas de vigilancia el régimen de Pekín viola en forma sistemática la privacidad de su ciudadanía y vigila a los disidentes. De acuerdo con las declaraciones de Sophie Richardson, directora de Human Rights Watch en China *"estas actividades deberían cesar hasta que el país adopte un marco de protección de la privacidad creíble".*[20]

3. Estados Unidos: Tierra de la libertad y ¿de la privacidad?

En Estados Unidos se observa una implementación masiva de tecnologías de control y vigilancia dentro de su sociedad. Estas tecnologías han sido implementadas con anterioridad a los atentados de las torres gemelas del World Trade Center experimentado por el país a comienzos del siglo XXI, aunque, luego del incidente, es notable el surgimiento de cambios dentro del paradigma de seguridad vigente hasta el momento.

[19] Véase https://www.infobae.com/america/tecno/2018/11/06/asi-funciona-el-gran-hermano-estatal-en-china-un-sistema-que-identifica-a-la-gente-segun-su-forma-de-caminar/

[20] Véase https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html

Según José María Blanco Navarro (2011), los ataques terroristas han despertado temor dentro de la población norteamericana, la cual ha resignado derechos y libertades inherentes al ser humano: el derecho a la intimidad y privacidad con la finalidad de permanecer "seguros" frente a los peligros de la sociedad contemporánea.

La autora Georgina Sánchez escribe el capítulo *"La política de defensa y seguridad de Estados Unidos a principios del siglo XXI" (2010)* y afirma que *"(...) El 11 de septiembre del 2001 fue la fecha que sacudió algunos de los supuestos básicos de la política de seguridad de Estados Unidos y dio lugar a una profunda transformación de implicancias mundiales"* (Sánchez, 2010, p.13).

Es importante observar a Estados Unidos y la implementación cada vez mayor de tecnologías de vigilancia y control sobre la población, ya que estas modalidades de control son indicadores de lo que luego suele ser trasladado al resto del mundo.

Así lo afirma Sánchez (2010) *"(...) La transformación de la política de defensa y seguridad de Estados Unidos a comienzos del siglo XXI no es sólo una reforma más sino un cambio profundo que impactará en el futuro de ese país y del resto del mundo*" (Sánchez, 2010, p.14).

Como se verá en los próximos capítulos esto también se aplica a la Argentina donde progresivamente comienzan a emplearse tecnologías de control y vigilancia cada vez más sofisticadas como el reconocimiento facial.

Cabe destacar que el uso de tecnología de reconocimiento facial no está exento de controversias y polémicas en los Estados Unidos. El instituto Nacional de Estándares y Tecnología (NIST) que depende del Departamento de Comercio de Estados Unidos, realizó un estudio sobre las tecnologías de reconocimiento facial y sostuvo que, el uso de esta tecnología puede conllevar prácticas raciales y sexistas en su funcionamiento. Según el informe emitido por la NIST, los algoritmos de reconocimiento facial fallan entre 10 y 100 veces más al momento de realizar la identificación de rostros de personas afroamericanas o asiáticas en relación con los rostros caucásicos. De esta manera, el informe asegura que los falsos positivos son más altos en las mujeres que en los hombres y esto es una constante en todos los algoritmos y conjuntos de datos analizados por los investigadores.

Para los autores del estudio de la NIST y en especial para Patrick Grother, estas fallas del sistema no son banales ya que los falsos positivos podrían dar como resultado acusaciones de delito erróneo e incluso detenciones. Como consecuencia de este informe, diversas publicaciones tecnológicas como "Technology Review", publicación del Instituto Tecnológico de Massachusetts, ponen en duda la conveniencia de la implementación masiva de estos sistemas de vigilancia y control como ocurre actualmente en Estados Unidos.

3.1 Algunos casos ejemplo

3.1.1 El FBI recopila sin permiso fotos del carnet de conducir para el reconocimiento facial

Estados Unidos ha implementado en forma masiva tecnologías de vigilancia y control sobre la población[21]. Diversas agencias del Estado, como el FBI y el Servicio de Inmigración y Control de Aduanas (ICE) están recurriendo a la utilización de datos privados de la ciudadanía, específicamente al uso sin consentimiento de las fotografías de los carnets de conducir para crear una base de datos de reconocimiento facial.

De acuerdo con Informes de la Oficina de Contabilidad del Gobierno Estadounidense (GAO), 21 Estados norteamericanos permiten que agencias federales de seguridad, como el FBI, escaneen fotos de las licencias de conducir de sus habitantes, aunque, supuestamente esto ocurre sólo si se amerita en una investigación. Una vez que el FBI recibe la información, se utiliza para comprobar si la fotografía es coincidente con alguna de las registradas en las bases de datos. Este sistema no se emplea únicamente para identificar sospechosos de delitos sino también para detectar posibles testigos de éste. De esta forma, el FBI tiene acceso a bases de datos locales, estatales y federales poseyendo 641 millones de fotografías para conformar su banco de datos que posibilitará el reconocimiento facial de la ciudadanía.

Este accionar es realizado sin el consentimiento ni conocimiento de los afectados. Así lo afirma el presidente del Comité de Supervisión de la Cámara de Representantes, Elijah E. Cummings *"los accesos a las bases de datos del Estado por parte de las fuerzas de seguridad suelen ser llevados a cabo con frecuencia en la sombra, sin consentimiento".*[22]

Esta información fue difundida por el reconocido diario Washington Post y generó alarma y preocupación por parte de los defensores de los derechos civiles y por las organizaciones de los Derechos Humanos. Los activistas temen que la administración de Donald Trump o futuros gobiernos empleen esa tecnología como un instrumento para atrapar y deportar inmigrantes indocumentados.

Al respecto, Shankar Narayan, integrante de la Unión de Libertades Civiles de Washington sostuvo que *"los organismos policiales ven una gran oportunidad de usar estas tecnologías para hacer cumplir estatus de inmigración de una manera que no es la pensada".*[23]

---

[21] Nota publicada el 9 de julio del 2019 en el medio Todo Noticias https://tn.com.ar/tecno/f5/el-fbi-recopila-sin-permiso-fotos-del-carnet-de-conducir-para-el-reconocimiento-facial_977144

[22] Véase: https://tn.com.ar/tecno/f5/el-fbi-recopila-sin-permiso-fotos-del-carnet-de-conducir-para-el-reconocimiento-facial_977144/

[23] Véase https://www.diariolasamericas.com/inmigracion-preocupa-uso-tecnologia-reconocimiento-facial-ice-n4180672

3.1.2 Reconocimiento facial en las fronteras de Estados Unidos

En agosto del 2019 se dio a conocer la intención de la Agencia de Aduanas y Protección Fronteriza de Estados Unidos que busca expandir el uso del reconocimiento facial en sus fronteras para evaluar a las personas que pretenden ingresar a su territorio[24].

La implementación de este sistema apunta a reemplazar los sistemas de seguridad y control existentes que dependen de métodos como la verificación de contraseñas por sistemas biométricos, y se reemplace por huellas digitales y escaneos faciales.

Durante la última década, la Agencia de Aduanas y Protección Fronteriza ha realizado importantes inversiones en software para el rastreo de personas y productos que han ingresado al país norteamericano. En 2013 estableció con Northroup Grumman Corp un contrato multimillonario para la realización de un software biométrico que ya se encuentra en uso en 15 aeropuertos del país. El objetivo de la agencia es expandir para el 2021 un programa para cubrir el 97% de los pasajeros de las aerolíneas con estos sistemas de identificación.

3.1.3 Reconocimiento facial en las escuelas norteamericanas

La implementación de tecnología de reconocimiento facial en Estados Unidos no sólo ha sido aplicada de manera generalizada en el ámbito público buscando enfrentar las amenazas de las sociedades contemporáneas, sino que se ha trasladado asimismo a entornos cerrados como son las instituciones educativas. En la ciudad de Lockport, en el estado de Nueva York, las escuelas comenzarán a implementar un sistema de reconocimiento facial denominado "*Aegis*" que será utilizado para la identificación de los asistentes a clase y también de objetos ocultos[25]

En la comunicación que el distrito escolar brindó a los padres de los alumnos, se afirma que el "Aegis" es un sistema de "alerta temprana" que puede notificar de potenciales amenazas a los funcionarios. Este tipo de amenazas pueden ser agresores sexuales de nivel 2 o 3 y/o personas vetadas a la entrada de los centros escolares. Los defensores del uso de esta tecnología en ámbitos educativos sostienen que constituye un importante instrumento para prevenir los tiroteos en las escuelas neoyorkinas ya que el software con el que cuenta el programa tiene la capacidad de identificar diferentes tipos de armas.

El distrito de Lockport instala el software y las cámaras necesarias para el funcionamiento del sistema con fondos provenientes de la "Ley de Bonos de Escuelas Inteligentes de Nueva York", la cual destina fondos para la adquisición de dispositivos tecnológicos para ser utilizados en

[24] Véase https://www.infobae.com/america/eeuu/2019/08/13/eeuu-ampliara-uso-de-reconocimiento-facial-en-fronteras/

[25] Véase https://www.iproup.com/innovacion/11424-biometria-los-colegios-y-la-polemica-por-el-reconocimiento-facial

educación como computadoras portátiles, pero, en esta ciudad de EE. UU., se ha decidido que esos fondos se usarán para la adquisición de tecnología de vigilancia.

La implementación de estas medidas no estuvo exenta de controversia y polémica debido a la violación de privacidad que conlleva y al riesgo de comercialización de datos privados de los individuos que son objeto de vigilancia del sistema.

Frente a estos riesgos, la Unión de Libertades Civiles de Nueva York le ha pedido al departamento de educación del Estado Neoyorquino que bloquee la implementación del proyecto. La entidad afirmó que la precisión de los sistemas de reconocimiento facial está en discusión y expresó inquietud por la privacidad de los estudiantes: *"Estos sistemas podrían potencialmente convertir los pasos de los estudiantes y miembros del personal en evidencia de una infracción o crimen y podrían criminalizar el mal comportamiento infantil y las interacciones personales".*[26]

3.1.4 San Francisco prohíbe el reconocimiento facial

La implementación de sistemas de vigilancia y control masivo por medio del reconocimiento facial se está extendiendo por todo el mundo, incluso en países periféricos como la Argentina. A pesar de ello, en ciudades norteamericanas como San Francisco, el 15 de mayo del 2019, la dirigencia política, luego de que la Junta de Supervisores votara 8 a 1 aprobando la medida, ha tomado la decisión de prohibirle a las fuerzas de seguridad y a las agencias públicas la utilización de estas tecnologías bajo el argumento de que *"la propensión de la tecnología de reconocimiento facial a poner en peligro los derechos y libertades civiles, supera sustancialmente sus beneficios".*[27]

Las autoridades de San Francisco afirman que el reconocimiento facial puede *"exacerbar la injusticia racial y amenazar nuestra capacidad de vivir sin la continua vigilancia del gobierno".*[28]

La normativa aprobada fue redactada por el supervisor Aarón Peskin quien apuntó que el reconocimiento facial implicaría un paso adelante hacia una mayor represión estatal. Durante el debate, Peskin nombró a China como ejemplo y el empleo de estas tecnologías para tener bajo control a la minoría musulmana en el país.

---

[26] Véase https://nakedsecurity.sophos.com/es/2018/06/26/school-facial-recognition-system-sparks-privacy-concerns/

[27] Nota publicada el 15 de mayo del 2019 en el medio La Vanguardia. https://www.lavanguardia.com/internacional/20190515/462256381193/san-francisco-reconocimiento-facial-prohibe.html

[28] Véase https://www.ambito.com/mundo/san-francisco/por-poner-peligro-derechos-y-libertades-prohibe-el-reconocimiento-facial-n5031664

La prohibición forma parte de una reglamentación más amplia que busca regular los sistemas de vigilancia y obligar a las agencias municipales que utilicen estas tecnologías a obtener autorización en forma previa. Para Peskin esta medida no es una política antitecnológica porque se trata de poder exigir responsabilidades en torno a la tecnología de vigilancia y garantizar que se hace un uso seguro de ella. Los partidarios de la prohibición temen posibles errores de identificación facial, así como la continua violación a la vida privada de la ciudadanía.

Tim Kingston, investigador de la Oficina de Defensa del Público de San Francisco aseguró al diario El País que *"es un disparate usar ese programa que ya se ha visto que se equivoca mucho al identificar a personas de pieles más oscuras*[29]*".*

Los defensores de esta tecnología de vigilancia y control como Stopcrime SF aseguran que el reconocimiento facial *"puede ayudar a localizar niños perdidos, personas con demencia y a luchar contra el tráfico sexual".*[30]

Por su parte, la Unión Estadounidense por las Libertades Civiles (ACLU) sostiene que esta tecnología puede *"ser usada de manera pasiva, que no requiere del consentimiento, conocimiento o participación del individuo".*[31]

Aarón Peskin, supervisor que impulsó la aprobación de esta medida también manifestó "*Esta no es una política anti tecnológica. Se trata de poder exigir responsabilidades en torno a la tecnología de vigilancia, de garantizar que se hace un uso seguro de ella"*[32]

A pesar de la medida que aprobó San Francisco, esta tecnología de vigilancia seguirá operando en lugares donde exista la jurisdicción federal como, por ejemplo, los aeropuertos. Para uno de los abogados de la ACLU, Matt Cagle, la tecnología de reconocimiento facial proporciona al gobierno un poder sin precedentes para rastrear a las personas que viven sus vidas cotidianas y eso es algo incompatible con una democracia. *"Las cámaras de la policía que escanean la cara no tienen lugar en nuestras calles, donde se pueden usar para vigilancia discriminatoria"*, afirmó Cagle[33] y sostuvo "*California ha actuado con valentía para detener la expansión de un*

[29] Véase https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html
[30] Véase https://www.ambito.com/mundo/san-francisco/por-poner-peligro-derechos-y-libertades-prohibe-el-reconocimiento-facial-n5031664
[31] Véase https://www.lanacion.com.ar/tecnologia/san-francisco-prohibe-policia-usar-tecnologia-reconocimiento-nid2247555
[32]Véase https://www.lavanguardia.com/internacional/20190515/462256381193/san-francisco-reconocimiento-facial-prohibe.html
[33]Véase https://www.efe.com/efe/america/ame-hispanos/aplauden-veto-a-reconocimiento-facial-en-camaras-de-la-policia-california/20000034-4083420

estado de vigilancia que presenta una amenaza sin precedentes para nuestros derechos y libertades".[34]

Conclusión

En este capítulo se retoman, desarrollan y ponen en juego dos conceptos mencionados en capítulos previos y que son fundamentales para comprender la temática de la tesina: la práctica de gubernamentalidad de la política del miedo y el cambio en el paradigma de seguridad del siglo XXl. Ambos temas son considerados como alternativas para establecer posibles vías de solución para contrarrestar problemáticas como las amenazas internas consideradas como "propias de las sociedades modernas," pero cuya implementación no hace más que exacerbar la lógica de control en las sociedades actuales.

El concepto de política del miedo puede ser visto como una práctica de gubernamentalidad que avala las propuestas establecidas en el nuevo paradigma de seguridad utilizado por la dirigencia política de diversas naciones, así como de otros actores económicos y políticos para lograr el reclamo y/o aceptación de la población hacia la incorporación de mayores medidas de seguridad y su consenso frente a la aplicación de nuevas modalidades y tecnologías de control y vigilancia. Está práctica de gubernamentalidad implica, en este sentido, la conducción de conductas, cuerpos y subjetividades característica de esta sociedad de control que se ejercita siempre en un marco de vigilancia y monitoreo.

Por otro lado, se retoma la idea de tecnologización de las fuerzas policiales a nivel global, (ya abordado en los capítulos previos), y se describe la puesta en práctica de tecnologías como el reconocimiento facial y el sistema de videovigilancia en dos de las principales potencias mundiales: China y Estados Unidos, que si bien poseen particularidades sociales e ideológicas diferentes, sirven para ilustrar la materialización de la puesta en práctica de la configuración de las sociedades de control no sólo en Argentina sino en todo el mundo.

Brindar un espacio a estas super potencias permite observar que las tecnologías de control y vigilancia implican un avance contra los derechos a la intimidad y privacidad de la población en general, pero también hacia grupos específicos puntuales como la etnia uigur en China o los grupos de migrantes en la frontera sur de Estados Unidos. En ambos países se observa no sólo la puesta en práctica de estos nuevos dispositivos de vigilancia masivos sobre las poblaciones sino también algunas discrepancias y similitudes entre ellas. Ambas naciones han firmado el Pacto Internacional de Derechos Civiles y Políticos que garantiza el respeto a la privacidad de

[34]Véase https://www.efe.com/efe/america/ame-hispanos/aplauden-veto-a-reconocimiento-facial-en-camaras-de-la-policia-california/20000034-4083420

sus habitantes. El tratado ha sido firmado y ratificado por Estados Unidos y sólo firmado por China. Sin embargo, cabe notar que, en mayor o menor medida, ambas potencias omiten lo establecido allí, incluso, violando sus disposiciones abiertamente como bien se contempla con las medidas adoptadas por el gobierno chino para perseguir y controlar a la etnia uigur o en el caso de Estados Unidos para vigilar y controlar el flujo migratorio en la frontera sur del país.

Por lo tanto, y a pesar de algunos intentos de los países occidentales denominados y que se autodenominan "tierra de la libertad" por remarcar la naturaleza "vigilante y controladora" establecida por el gobierno chino en su territorio también se ven inmersos en una compleja sociedad de control donde el desarrollo de tecnologías y modalidades de vigilancia se extienden hasta límites insospechados provocando avances contra los derechos a la privacidad e intimidad de la población, derechos avalados y establecidos no sólo por las leyes nacionales sino también por legislaciones internacionales.

Como se verá al abordar el caso de Argentina, y especialmente el de CABA, los ejemplos de China y Estados Unidos permiten observar que la lógica de la sociedad de control toma cada vez más fuerza en el mundo contemporáneo estableciendo fuerzas de seguridad en un nivel cada vez mayor de tecnologización, potenciando sus capacidades de control y vigilancia existan o no motivos válidos para ello. Sin embargo, al analizar y desarrollar estos casos tomados como ejemplo, se contempla una importante diferencia: el rechazo civil a su implementación. Este rechazo se observa perfectamente en el caso de la Ciudad de San Francisco, en Estados Unidos, donde las autoridades locales se percataron de los riesgos que conlleva la aplicación de dichas tecnologías en el espacio público afectando los derechos y las libertades civiles de la ciudadanía. El rechazo y prohibición a las fuerzas de seguridad de emplear estas tecnologías en la ciudad norteamericana ha tenido relevancia internacional y ha repercutido en diferentes metrópolis del país como la Ciudad de Boston.[35]

En agosto del 2020 en Reino Unido, la Corte de Apelaciones falló a favor de una demanda contra el uso del reconocimiento facial utilizado en vivo por la policía de Gales del Sur[36]. Según el fallo judicial, el reconocimiento facial es una tecnología de control y vigilancia más invasiva que la simple captura de fotografías o el uso de cámaras de videovigilancia ya que, actualmente,

[35] Véase https://www.telemundonuevainglaterra.com/noticias/local/boston-aprueba-prohibicion-de-tecnologia-de-reconocimiento-facial/2052621/

[36] Véase https://adc.org.ar/2020/09/18/avanza-la-regulacion-del-reconocimiento-facial-en-la-legislatura-porten

no existen los marcos jurídicos necesarios en el país para que las fuerzas policiales la empleen por lo cual, la corte consideró que la implementación del reconocimiento facial se realizó sin examinar correctamente las evaluaciones por parte del sistema.

Contrariamente a lo expuesto, este fenómeno no se ha podido identificar en China donde a pesar de la existencia del uso masivo de tecnologías de control y vigilancia, este trabajo de investigación no encontró voces opositoras a su utilización. Si bien no se descarta que en China existan ONGs que denuncien su uso masivo, éstas parecerían encontrarse bajo un monitoreo constante realizado por el propio gobierno. Principalmente son ONGs internacionales como Human Right Watch las que realizan estas denuncias. Aun así, cabe destacar que, progresivamente, diferentes voces provenientes desde organizaciones sin fines de lucro o del ámbito académico comienzan a levantar su voz y alertar sobre los riesgos que supone la aplicación de la tecnología de reconocimiento facial en muchos países, incluyendo a la Argentina, como se presentará y analizará en los próximos capítulos.

El alcance contra estos derechos inalienables bajo el argumento de proteger a la sociedad frente a las amenazas que predica el nuevo paradigma de seguridad se ha convertido en un factor constante en muchas naciones a nivel global, y la omisión, violaciones o tensiones respecto de las legislaciones nacionales e internacionales destinadas a protegerlos se desarrollará en los capítulos siguientes de manera que, es posible que algunos países, incluyendo Argentina, elaboren regulaciones específicas para realizar la práctica de videovigilancia, aunque es posible que otras naciones implementen el sistema de videovigilancia sin tomar en consideración normativas y legislaciones internacionales designadas a garantizar el derecho a la privacidad.

Capítulo 4: ¿Proteger la privacidad? Legislación argentina

Introducción

Este capítulo indaga y analiza las legislaciones nacionales específicamente, aquellas que se enfocan en regular el funcionamiento de las tecnologías de control y vigilancia social como son las cámaras de videovigilancia y reconocimiento facial. Para ello, se define el concepto de privacidad y se diferencian las diversas etapas y mutaciones que ha registrado a lo largo del tiempo, entendiéndolo como uno de los ejes claves del presente trabajo. A su vez, se identifican y describen las leyes y resoluciones que desde los poderes estatales han sido formuladas con la finalidad de controlar la aplicación y funcionalidad de los sistemas de vigilancia y control que operan en la sociedad argentina y que, al mismo tiempo, buscan garantizar el derecho a la privacidad e intimidad de la ciudadanía. Sin embargo, a través de su implementación en el espacio público, con el supuesto propósito de combatir la criminalidad pueden conllevar la violación de los llamados derechos esenciales del ser humano como lo es su privacidad.

1. Las cámaras están ¿y las leyes?

La privacidad, la ética y los derechos humanos, así como la expulsión social y la discriminación aparecen como ejes centrales para analizar los efectos que genera la aplicación de los sistemas de videovigilancia y reconocimiento facial.

Lío (2015) retoma el trabajo de Wood y Bali (2006) y afirma que

> *"(...) La vigilancia, la invasión y protección de la privacidad operan diferencialmente entre grupos, beneficiando a algunos y desfavoreciendo a otros. En este sentido, la vigilancia varía de acuerdo al lugar y en relación a la clase social, el grupo étnico y el género.* (Lío, 2015, p16).

La emergencia de los sistemas de videovigilancia y reconocimiento facial como una de sus aplicaciones, ha implicado la necesidad de construir diversos marcos normativos que definan, limiten y regulen su empleo en las sociedades. La gran extensión de estos sistemas de vigilancia, como una posible solución para enfrentar la criminalidad en el espacio público, ha generado cuestionamiento respecto a sus posibles efectos sobre la individualidad, privacidad y protección de los datos personales de los sujetos.

Para Lío (2015) no sólo es necesario el surgimiento de leyes específicas, sino que las prácticas de estos sistemas de vigilancia deben adecuarse a la normativa vigente en cada contexto. La autora remarca que la aplicación de estos sistemas de control sufre déficits en las legislaciones que deben regular su accionar

> *"(...) Desde una perspectiva amplia que contempla la difusión de las nuevas tecnologías podría decirse que la regulación emerge de forma gradual a medida que*

> *extiende su alcance y raramente se verifica una existencia de legislación formal y marcos regulatorios específicos previo a su utilización efectiva".* (Lio, 2015, p.17).

Lío retoma a Webster (2004) quien sostiene que el proceso de discusión juega un rol clave en el diseño de medidas y procesos regulatorios ya que los actores, agencias y aparatos gubernamentales involucrados en la difusión y aplicación de estos sistemas dan forma al emergente marco regulatorio. Para la autora, los mecanismos que se engloban bajo la idea de regulación incluyen la legislación formal (específica o no) así como los códigos de prácticas y estándares técnicos que surgen como resultado de una negociación generada entre *"(...) actores en la red de políticas públicas, involucrando gobiernos centrales y locales, la policía y numerosos grupos de interés"* (Lío, 2015, p.17).

También confronta las interacciones de los actores de las redes políticas, importantes en el diseño de las políticas públicas, incluyendo aquellas relacionadas con la seguridad, vigilancia y control del espacio público.

El texto mencionado expresa la necesidad de comprender los marcos regulatorios emergentes contemplando la existencia de una legislación formal combinada con las redes de coordinación y autorregulación, y al mismo tiempo, observa si la regulación de estos sistemas de vigilancia y control y su aplicación sobre la ciudadanía es satisfactoria y respetuosa con respecto a otros derechos como la protección de libertades individuales y civiles, la privacidad y la protección de los datos personales, los cuales son propensos a ser captados por el Estado a través de estas tecnologías de vigilancia y control que las mismas sociedades de control despliegan en su espacio público.

Dentro de las sociedades contemporáneas se generaría una negociación constante que vive la población en torno a qué derecho quiere "ganar o perder". Se experimenta una especie de "trueque" entre los derechos de los habitantes, como sostiene Lío (2015) al confirmar que *"(...) Las víctimas potenciales prefieren sacrificar su privacidad personal por un grado de protección personal"* (Lío, 2015, p.18).

Paulatinamente este escenario transcurre en un marco de secretismo y opacidad en el manejo de las tecnologías de vigilancia y control por parte de las fuerzas de seguridad del Estado mientras aumenta la transparencia en la vida de los ciudadanos comunes. En otras palabras, no sólo la población generalmente no tiene conocimiento sobre agencias gubernamentales que obtienen esa información o bajo qué reglas y circunstancias, sino que, incluso, los mismos dirigentes políticos de turno pueden no estar al corriente del funcionamiento de este entramado de información. Por lo tanto, este sistema de control se torna cada vez más opaco y con

mecanismos de funcionamiento que pueden escapar al control de la sociedad civil de los Estados.

2. Definiendo a la privacidad

Para analizar los nuevos riesgos hacia la privacidad de la población que pueden ocasionar los sistemas de vigilancia que operan en las sociedades contemporáneas es necesario definir con claridad el concepto de privacidad.

Según la Real Academia de la Lengua Española privacidad es el "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".* Esta definición se respalda por la Declaración Universal de los Derechos Humanos que establece en su artículo N°12 que el derecho a la vida privada es un derecho humano.

La privacidad implica todo lo que los sujetos tienen derecho a proteger para ellos mismos, todo lo que tenemos derecho a que los demás no sepan de nosotros. Es el ámbito de la esfera personal de la vida de un individuo que se desarrolla en un espacio reservado y debe mantenerse de manera confidencial.

De acuerdo con el trabajo "Pr*ivacidad y vigilancia en entorno digitales"* (2015) realizado por la Fundación Vía Libre, la privacidad puede ser definida como "*aquello que uno quiere mantener en privado, aquello que el hombre busca mantener en secreto: cierta información propia o sobre terceros*". (p.1)

La contundencia de estas definiciones es respaldada por el Artículo Nº19 de la Constitución Nacional Argentina que protege la privacidad de la ciudadanía y su conducta íntima al afirmar que" *las acciones privadas de los hombres que de ningún modo ofendan al orden o a la moral pública ni perjudiquen a terceros están sólo reservadas a Dios y exenta de la autoridad de los magistrados".*

Alcántara (2008) remarca la gran importancia que tiene la defensa de la privacidad de la ciudadanía en la sociedad contemporánea.

> *"(...) La lucha por la privacidad es también la lucha por decidir quién puede saber qué sobre nosotros, quién puede almacenarlo y en qué condiciones puede alguien acceder a ello. La lucha por la privacidad es la lucha por dilucidar la legitimidad de las enormes bases de datos con información personal que día a día se crean y van creciendo en nuestra sociedad para saberlo todo sobre nosotros. Aunque suene grandilocuente, la lucha por la privacidad es la lucha por volver a equilibrar las democracias. La democracia se basa en el respeto mutuo entre gobierno y pueblo y la sociedad digital y las posibilidades que ofrece hace que sea necesario un nuevo análisis con el objetivo de garantizar que la democracia siga siendo respetada."* (Alcántara, 2008, p.31).

Las sociedades democráticas contemporáneas se caracterizan por la existencia de un espacio en el cual el individuo es supuestamente soberano y donde el accionar del Estado u otros sujetos particulares no puede actuar sin violentar sus derechos. La falta de privacidad puede comprometer seriamente a la misma democracia.

El desarrollo y aplicación de estas tecnologías de control sobre las poblaciones se ha convertido en una realidad, aun cuando puede conllevar la pérdida de la privacidad de la ciudadanía como se refleja en los discursos de actores con fuerte participación en el desarrollo tecnológico.

Uno de ellos es Scott Mcnealy, CEO de Sun Micro System, quien en el 2000 afirmó "*la privacidad ha muerto, supérenlo"*[37] o como Larry Ellison, fundador de la tecnología Oracle, quien en 2001 sostuvo "*esta privacidad que les preocupa es en gran medida una ilusión"*[38].

Incluso Barack Obama, expresidente de Estados Unidos, el 7 de junio del 2013 aclaró "*es importante reconocer que uno no puede tener un 100% de seguridad y también un 100% de privacidad con cero inconveniencias. Vamos a tener que hacer algunas elecciones como sociedad".*[39]

El derecho a la privacidad es considerado como uno de los derechos fundamentales (también denominados de *primera generación*) del ser humano. Se trata de derechos inalienables, inviolables e irrenunciables y pertenecen a todas las personas por su dignidad y son incluidos dentro de la Constitución de una nación. Por otro lado, existen derechos denominados de *segunda generación* que incluyen derechos sociales, económicos y culturales mientras que los de *tercera generación* incorporan derechos heterogéneos como el derecho a la paz, a la calidad de vida o las garantías frente a la manipulación genética.

En los últimos años, autores como David Vallespin Pérez, Robert Gelman, Javier Bustamante Donas, entre otros, aúnan criterios y afirman que está surgiendo una *cuarta generación* de derechos humanos, los cuales están relacionados con las nuevas tecnologías digitales. Algunos de estos derechos se refieren al derecho a existir digitalmente o al de poseer una identidad digital.[40]

2.1 Las etapas de la privacidad

De acuerdo con el texto *"Desafíos de la biometría para la protección de los datos personales"* (2017) realizado por la Asociación por los Derechos Civiles (ADC), la distinción entre esfera privada y pública se halla presente desde la antigüedad, aunque en la Modernidad surge con mayor fuerza la idea de un ámbito de reserva del individuo cristalizada bajo la forma de un

[37] Véase http://www.sensebyte.com/es/principales-tendencias-de-la-industria/85-privacy-it-s-dead-get-over-it-it-s-about-trust-and-user-control-es

[38] Véase http://lobosuelto.com/felicidad-asegurada-i-carolina-di-palma/

[39] Véase https://www.elespanol.com/opinion/tribunas/20170908/245345464_12.html

[40] Véase: https://es.wikipedia.org/wiki/Tres_generaciones_de_derechos_humanos

derecho que puede ser esgrimido ante las autoridades judiciales en caso de que el sujeto se vea afectado.

Es posible distinguir tres etapas que la noción de privacidad ha ido atravesando desde el punto de vista jurídico a lo largo de la historia.

En la primera, el concepto de privacidad estaba centrado en su dimensión espacial. Se consideraba que el derecho a la privacidad tenía por objeto los espacios a los cuales las personas no podían acceder ni tener conocimiento sin autorización previa por parte del sujeto titular del derecho. En este enfoque, el domicilio particular de los ciudadanos constituye uno de los ejemplos más paradigmáticos, puesto que una determinada persona tiene la potestad de impedir intromisiones arbitrarias en él.

Este derecho es concedido y reconocido por la Constitución Nacional Argentina donde se piensa a los domicilios particulares como inviolables, así como también determinados objetos considerados dignos de protección como la correspondencia personal.

Así reza el Artículo Nº18 de la Constitución Nacional *"(...)El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación..."*.

En estos casos, la Constitución establece la posibilidad de interferencia por parte de las autoridades, pero estableciendo los casos y justificativos para la intervención por medio de leyes.

Una segunda etapa referida a la idea de privacidad implicó un desplazamiento desde un enfoque espacial hacia uno que evaluaba la naturaleza de la conducta del sujeto que debía ser regulada. Esta concepción entiende que la conducta privada de los individuos cuyas acciones no generen daños o perjuicios hacia terceros pertenece a la esfera íntima de los sujetos y, por lo tanto, no puede ser sancionada por el derecho como expresa el Artículo Nº19 de la Constitución Nacional mencionado anteriormente. Desde este punto de vista, el derecho a la privacidad protege la autonomía personal en la elección de planes de vida de los ciudadanos y evita la intromisión del Estado en los asuntos que sólo involucran a la moral de los sujetos.

Estos dos conceptos de privacidad han convivido por mucho tiempo, pero, con el desarrollo de tecnologías y el surgimiento de nuevos fenómenos fue necesaria una redefinición de las nociones tradicionales sobre el mismo.

El desarrollo tecnológico implicó una penetración de lo digital en la cotidianeidad de las sociedades contemporáneas. A esto se le suma el rol central que posee el conocimiento en las sociedades capitalistas del siglo XXI donde existe una fuerte avidez por la adquisición y difusión de la información.

Esto se refleja en el trabajo de Hidalgo (2004) donde el autor afirma que las fuerzas de seguridad del Estado pasan a estar caracterizadas como una institución que, a raíz de los cambios generados por la incorporación de tecnologías digitales, llevan a cabo una actividad de naturaleza eminentemente informacional, recolectando información de carácter privado de la ciudadanía con el argumento de realizar políticas que combatan la criminalidad.

La unión de estos fenómenos ha generado que el concepto de privacidad entre en una tercera etapa la cual está en estrecha vinculación con la *noción de información*.

En ella, la idea de privacidad pasa a ser vista como el derecho a que toda información sobre la vida privada de los sujetos en poder de terceros, como el Estado o los grandes conglomerados comerciales, no sea utilizada en perjuicio de los intereses del titular de esa información.

Por lo tanto, la Constitución Nacional Argentina garantiza el derecho a la privacidad de sus Artículos 18 y 19 los cuales buscan proteger la privacidad y conducta intima de su ciudadanía.

El alcance de estas deposiciones fue establecido por la Corte Suprema de Justicia en el fallo Ponzetti de Balbín c/ Editorial Atlántida en el año 1984 donde sostuvo que *"la protección material del ámbito de la privacidad resulta uno de los mayores valores del respeto a la dignidad de la persona y un rasgo diferencial entre el estado de derecho democrático y la forma política autoritaria y totalitaria".* [41]

[41] Véase https://www.psi.uba.ar/academica/carrerasdegrado/psicologia/sitios_catedras/obligatorias/723_etica2/material/casuistica/ponzetti_de_babin_derechos.pdf

Cuadro Nº1: Etapas de la privacidad

Primera etapa	*Segunda etapa*	*Tercera etapa*
▪ La privacidad estaba vinculada a la idea de espacio. ▪ Un ejemplo de esta etapa es la privacidad del domicilio particular y determinados objetos personales como la correspondencia. ▪ Las personas no podían ingresar ni tener conocimiento sin la autorización de la persona titular del derecho. ▪ Resguardado por el Artículo Nº18 de la Constitución Nacional.	▪ El concepto de la privacidad está vinculada a la conducta de la población que debe ser regulada. • Aquellos comportamientos del individuo que no generen perjuicios a terceros forman parte de la conducta íntima de la persona y se protege la privacidad de éste evitando la intromisión de los magistrados judiciales en acciones que sólo se refieran a la moralidad de la persona. ▪ Resguardado por el Artículo Nº19 de la Constitución Nacional.	▪ El concepto de privacidad está vinculado al concepto de información personal. ▪ Propia de los últimos años del siglo XXI ▪ Resultado de la penetración de las nuevas tecnologías digitales en la vida diaria de la población. ▪ La privacidad se entiende como el derecho a que toda la información privada de la vida de una persona que se encuentre en manos de terceros no sea utilizada con fines que pueda perjudicar los intereses particulares del titular de esa información. ▪ Protegido por la ley Nº25.326 (Ley de Protección de Datos Personales)

Fuente: Elaboración propia en base a ADC (2017)

Es importante destacar que a lo largo de las diferentes etapas que atravesó el concepto de privacidad han surgido diferentes tipos de tecnologías de vigilancia que se adecúan al contexto espaciotemporal y buscan llevar a cabo el control de población. Actualmente, el desarrollo técnico-tecnológico ha permitido que el surgimiento de mecanismos propios de la sociedad de control sea capaz de ejecutar una vigilancia más permanente, constante e invisible sobre la ciudadanía, pero cuyo uso puede implicar una violación del derecho a la privacidad, entendiéndola como vinculada al concepto de información personal.

La aplicación de tecnologías de control y vigilancia social, como el reconocimiento facial y el sistema de cámaras de videovigilancia como los que operan en CABA, responde a una lógica de funcionamiento de las fuerzas de seguridad del Estado, las cuales buscan la captación de datos de naturaleza privada de los sujetos con el argumento de combatir la criminalidad. Sin

embargo, este accionar genera una tensión con respecto a las legislaciones nacionales que intentan resguardar el derecho a la privacidad e intimidad de la población como se verá a continuación.

3. Ley de Protección de Datos Personales

Para garantizar la privacidad, desde octubre del 2000 Argentina cuenta con la ley Nº25.326 de Protección de Datos Personales.

> "*La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional".*

El entramado normativo de la Ley Nº25.326 se completó en el 2001 con la reglamentación de la ley a través del Decreto 1.558/01 que creó la Dirección Nacional de Protección de Datos Personales [42](DNPDP) siendo la autoridad de aplicación de esta ley.

Esta ley busca proteger de forma íntegra los datos personales de la ciudadanía, los cuales pueden ser captados, almacenados y utilizados sin consentimiento de su dueño por parte de los organismos que componen las fuerzas de seguridad del Estado. De esta forma se apunta a proteger integralmente los datos presentes en archivos, registros o base de datos. A su vez, la legislación busca regular la base de datos pública y privada. Esta ley establece una serie de principios a los cuales deben ajustarse las operaciones con el tratamiento de datos, de manera que se realice un tratamiento legítimo y respetuoso de esa información personal y de su dueño.

- La ley establece que las operaciones de tratamiento de datos se realicen únicamente sobre aquellos datos vistos como estrictamente necesarios para las finalidades establecidas.
- La recolección de esta información no puede recogerse por medios desleales o en forma contraria a la estipulada por la ley. Se busca prohibir el robo de información, el engaño o la estafa para acceder a la misma.
- Los datos personales no pueden ser empleados en funciones distintas o incompatibles con las que impulsaron originalmente la obtención de la información. Por lo tanto, se le debe informar al titular para qué se los empleará brindando éste su consentimiento.

[42] Ubicada en Julio Argentino Roca 710, 2° piso, Buenos Aires, Argentina.

- Los datos que figuren en las bases deben ser verdaderos, exactos y actualizados en caso de ser necesario. Los datos inexactos o incompletos deben ser suprimidos, sustituidos o contemplados ya que la base de datos debe ser exacta y completa.
- El almacenamiento de los datos debe realizarse de manera que el titular pueda ejercer el derecho de acceso ya que, uno de los elementos esenciales en la protección de ellos es la posibilidad que tiene su dueño de conocer cuáles figuran en las bases para controlar qué información existe sobre él y comprobar su veracidad y exactitud.
- La ley establece que existen ocasiones donde no es necesario el consentimiento del ciudadano a la hora de recabar información, por ejemplo, en el caso de que se trate de datos para ser utilizados en el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. La ley también establece que no se requiere consentimiento de la ciudadanía cuando se trata de datos que el Estado necesita recolectar para cumplir con actividades propias de su naturaleza como la seguridad.
- Hace referencia, a su vez, a los supuestos especiales dentro de los cuales se encuentran disposiciones sobre las bases de datos de fuerzas de seguridad, fuerzas armadas u organismos policiales o de inteligencia.
- Fundamentalmente menciona que las bases de datos deben cumplir los preceptos establecidos por la ley, sin embargo, el tratamiento de los datos con fines de defensa nacional o seguridad pública no requieren de consentimiento de los interesados siempre que dichos datos sean estrictamente necesarios para el cumplimiento de misiones de defensa nacional, seguridad pública o represión de delitos.

Por su parte, la Constitución Nacional Argentina establece en forma expresa el derecho a la protección de datos personales mediante la incorporación del *habeas data* donde el Artículo Nº43 sostiene que

> "*Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley (…) "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos".*

La herramienta de *habeas data* se ha convertido en una herramienta establecida por la Constitución Nacional para que los individuos puedan velar y proteger sus datos e

informaciones privadas de la tecnología de control y vigilancia empleados por las fuerzas de seguridad del Estado.

No solamente el derecho a la privacidad de la ciudadanía está contemplado por la Constitución Nacional. El Nuevo Código Civil y Comercial (2015) consagra mediante su Artículo Nº52 que uno de los aspectos más importantes de la intimidad de un sujeto, como lo es su imagen, merece una protección legislativa especial al establecer el consentimiento expreso de una persona para la captación de su voz e imagen. Esto no ocurre cuando la ciudadanía se encuentra vigilada de manera permanente y constante por el sistema de cámara de videovigilancia y reconocimiento facial como el que opera en CABA en 2019.

La Ley Nº25.326 establece que estos datos personales recolectados con fines personales deben ser *congelados*[43] cuando ya no sean necesarias las averiguaciones que motivaron su almacenamiento. La ciudadanía argentina tiene el derecho de poder controlar a los responsables de las bases de datos garantizado por el "*derecho a la información*" en el Artículo Nº13, el cual otorga a las personas la facultad de solicitar a la DNPDP informes sobre la base de datos existentes y sus finalidades, así como sus responsables.

El Artículo Nº13 de la ley se complementa con el Nº14 denominado *"Derecho de Acceso*" el cual le permite al titular de los datos solicitar y acceder a la información que existe sobre él en las bases de datos públicos y privados y en el caso de no obtener respuesta, iniciar la acción de habeas data.

Asimismo, el Artículo Nº16 establece el derecho a la rectificación, actualización o supresión de la información si los datos que conforman las bases de datos están desactualizados o son falsos. En estos casos el artículo mencionado establece que toda persona puede solicitar al responsable o usuario de la base de datos su corrección, actualización o supresión.

Por lo tanto, como se afirma en el texto *"Desafíos de la biometría para la protección de los datos personales"* (2017) generado por la Asociación por los Derechos Civiles, la protección de datos personales constituye un punto de apoyo necesario para la defensa de los derechos de la ciudadanía frente a los peligros que conllevan las tecnologías de vigilancia y su potencial violación a la privacidad de los sujetos.

El hecho que la información obtenida por las tecnologías de control y vigilancia sea catalogada como "datos sensibles" implica restricciones a su uso por parte de terceros. El Artículo Nº2 de la Ley Nº25.326 los considera como "*datos personales que revelan origen racial y étnico,*

[43]El concepto hace referencia a información personal que continúa estando almacenada en las bases de datos pero que no vuelven a ser empleados por el Estado siempre y cuando no existan motivos establecidos por ley que así lo requieran.

opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

Esto se apoya en lo que sostiene la ley en el Artículo Nº7 inciso 1º el cual afirma *"ninguna persona puede ser obligada a proporcionar datos sensibles"*. Mientras que en el inciso 3º se remarca que *"queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles".* Sin embargo, la legislación argentina contempla excepciones a la ley, las cuales son expuestas en el artículo Nº7 inciso 2º donde se sostiene que *"los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley*".

Concretamente, debe ser una norma jurídica de carácter general que emana de órganos legislativos constitucionalmente previstos y democráticamente elegidos y no por medio de decretos ejecutivos en los cuales el poder Legislativo no tenga la posibilidad de intervenir.

El sistema de protección de datos personales debe estar conformado y actuar en base a una serie de principios que deben respetarse al momento de llevar a cabo el tratamiento de datos. Estos principios deben ser: licitud, exactitud y calidad, entre otros, siendo aplicados con más rigurosidad cuando se trata de información que reviste el carácter de "datos sensibles" como lo son los datos biométricos.

Es importante destacar que la Ley Nº25.326 permite el tratamiento de los datos siempre y cuando sean vistos como necesarios para el cumplimiento estricto de las disposiciones legales referidas a la seguridad pública y represión de delitos. Esta doble restricción busca demostrar la intención legislativa de restringir al máximo el uso de los datos personales y sensibles de la ciudadanía limitando el accionar arbitrario del Estado Nacional en esta área.

Entonces, cabe decir que, la Ley de Protección de Datos Personales establece la protección integral de la información privada de la población inserta en las bases de datos conforme a lo establecido por el Articulo Nº43 de la Constitución Nacional.

La ley también busca garantizar un trato respetuoso de la información privada de cada ciudadano que se encuentre en bases de datos públicos y privados, al tiempo que busca evitar la captación y uso ilegal de los datos privados de la población por parte de las fuerzas de seguridad del Estado. Por lo tanto, se pretende garantizar que la captación y uso de dichos datos como su almacenaje cumpla con los requisitos legales.

Asimismo, se establece que la información personal de la ciudadanía debe ser exacta y real y los ciudadanos cuentan con el derecho a pedir la corrección o eliminación de la información en caso de ser incorrecta. Sostiene a su vez, que los datos personales de un sujeto podrán ser recolectados y utilizados por el Estado cuando existan razones de interés general autorizados

por ley. Por último, se establece en ella que las fuerzas de seguridad del Estado pueden utilizar los datos privados de la ciudadanía sin consentimiento o conocimiento de la población cuando las fuerzas de seguridad realicen misiones en relación con la defensa nacional, seguridad pública o represión de delitos.

3.1 Renovando lo viejo: Intento de modificación de la Ley Nº25.326

En junio del 2016 la Dirección Nacional de Protección de Datos Personales (DNPDP) planteó la necesidad de repensar la Ley Nº25.326 intentando impulsar un proceso de reflexión sobre su regulación en Argentina. La necesidad de modificar el marco normativo se basa en los avances tecnológicos dados desde la sanción de dicha ley en el 2000 y la experiencia adquirida por la DNPDP durante estos 16 años tomando en cuenta los cambios normativos ocurridos en el escenario internacional, sobre todo con el nuevo reglamento (UE) 2016/679 del Parlamento Europeo. Todos estos factores han llevado a la DNPDP a sostener la necesidad de una reforma total o parcial a la Ley Nº25.326 identificando líneas de discusión en su reforma. Entre ellas, la necesidad de implementar nuevos conceptos que no han sido incorporados al formularse la ley en el 2000 y que cobraron importancia frente al actual debate global.

Se destacaban dos aspectos importantes. Por un lado, la incorporación de normas que obligue a los responsables de las bases de datos a demostrar el efectivo cumplimiento de la Ley Nº25.326 sosteniendo la necesidad de incluir un "delegado de protección de datos" en organismos públicos y privados que se ocupe de resguardar.

Además, se sostenía la necesidad de reformular los principios generales establecidos en dicha Ley lo cual incluye la reformulación integral de la regulación de la transferencia internacional de datos personales y la incorporación de la notificación obligatoria a la autoridad de aplicación en caso de incidente de seguridad con la información. A su vez, se remarcaba la necesidad de revisar los derechos y obligaciones de los titulares de los datos, usuarios y responsables de bancos de datos o archivos.

Estas líneas de discusión desarrolladas por la entidad han sido publicadas en un anteproyecto de ley que, de ser aprobada por el Congreso de la Nación reemplazaría a la actual Ley Nº25.326. La nueva ley reemplazaría a la actual DNPDP por la Agencia Nacional de Protección de Datos Personales la cual tendría autonomía funcional y actuaría como órgano descentralizado dentro del Ministerio de Justicia y Derechos Humanos de la Nación buscando responder, de esta manera, a las objeciones de la Unión Europea al reconocer a Argentina como un país adecuado para la transferencia de datos.

Básicamente, se limitaba a ser titulares de datos personales a personas físicas en concordancia con lo que dispone la legislación de la Unión Europea y amplía el objeto de protección disponiendo que el objeto de la ley sea la protección integral de los datos personales sin que éstos estén limitados, como lo establece la actual ley, a los datos personales asentados en bases de datos públicos o privados destinados a dar informes.

El anteproyecto de ley estableció una revisión a la luz de la legislación europea de las nociones ya presentes en la Ley Nº25.326 como son: el concepto de base de dato, datos personales o datos sensibles, pero busca, asimismo, la incorporación de nuevos conceptos como datos genéticos o biométricos, estableciendo que el fundamento legal para el tratamiento de los datos personales sigue siendo el consentimiento del titular, asegurando que, bajo determinadas circunstancias, el consentimiento puede ser implícito y se agrega al interés legítimo de quien trata los datos en la medida en que prevalezcan los derechos del titular de dichos datos.

En cuanto a los derechos de los titulares de los datos, el anteproyecto sigue la línea de la Ley Nº25.326 y reconoce el de la ciudadanía al acceso, rectificación y oposición de su información personal. Incorpora el derecho a la supresión de información, también denominado como "derecho al olvido", aunque este derecho no procederá cuando el tratamiento de datos personales sea necesario para ejercer el derecho a la libertad de expresión e información.

Por último, introduce modificaciones en el régimen de la Ley en torno a la transferencia personal de datos y establece que para ser válida; dicha transferencia debe contar con el fundamento legal (lo que implica un consentimiento del titular de los datos o interés legítimo de quien los trata) y realizarse en países con un nivel adecuado de protección de datos, contemplando la incorporación de la obligación de notificar fuga de datos tanto a la autoridad de aplicación como al titular de los mismos.

En resumen, el avance tecnológico que experimentó el mundo en los 16 años desde que se sancionó la Ley de Protección de Datos Personales tornó necesario actualizar la legislación vigente. Por lo cual, por iniciativa de la DNPDP, en el 2016 se impulsó modificar la Ley Nº25.326 buscando incorporar nuevas normas que obligara a los responsables de las bases de datos a demostrar el correcto y efectivo cumplimiento de las disposiciones establecidas en la misma. Esta iniciativa nace en la gestión de Mauricio Macri. En 2016 mediante la Ley Nº27.275 fue creada la Agencia de Acceso a la Información Pública, sin embargo, en el 2017, a través del Decreto 746/2017, tanto la Agencia como la Ley Nº25.326 pasaron a depender de la Jefatura de Gabinete de Ministros que funcionó como organismo de control. Con cada modificación de la ley vigente, la autoridad de aplicación fue siendo más asumida por la figura del presidente hasta quedar directamente controlada por el Jefe de Gabinete. Por lo tanto, el

proyecto de ley que buscaba modificar la Ley de Protección de Datos Personales continúa subordinando la autoridad de aplicación al poder ejecutivo, algo que las regulaciones de datos personales de la Unión Europea y Estados Unidos intentan evitar para garantizar la transparencia y la acción estatal.

A casi dos décadas de haberse sancionado la Ley de Protección de Datos Personales en Argentina, la necesidad de modificarla y adecuarla a las nuevas tecnologías y prácticas digitales como el Big Data, Data Mining (minería de datos) o Cloud Computing (computación en la nube) ponían en escena la necesidad de actualizar la legislación para proteger los datos de la ciudadanía frente a las nuevas amenazas y vulneraciones que podrían ocurrir en las sociedades contemporáneas.

Si bien el intento de modificar la Ley Nº25.326 en el país tomaba como modelo el reglamento general de protección de datos (GDPD) de la Unión Europea establecido en el 2016, la legislación argentina no buscaba ser una copia idéntica de lo pautado en la legislación europea como afirmó Eduardo Bertoni, director de la Agencia de Acceso a la Información Pública (AAIP) *"La clave es tratar de alcanzar cambios regulatorios que permitan ser considerados un país de legislación adecuada para facilitar los intercambios de información. Ahora, legislación adecuada es respetar los principios generales, no un cortar y pegar del nuevo reglamento europeo".*

Dentro de las principales modificaciones planteadas para actualizar la Ley Nº25.326 se encontraban:

- Incorporar el deber de notificación de incidentes en materia de seguridad y comunicación de los datos personales.
- Igual a lo establecido por el GDPD, incorporar un delegado en materia de protección de datos que lleve a cabo estudios en torno al impacto del procesamiento de datos.
- El anteproyecto establece que el sistema de consentimiento por parte de los titulares de los datos iba a ser de carácter "mixto" admitiendo tanto el consentimiento expreso como tácito de los usuarios.
- La renovación de la ley no iba a incluir la incorporación del derecho al olvido, impidiendo que los usuarios solicitaran la desindexación de sus datos personales. De acuerdo con la ley, este eje estaría cubierto por el Artículo Nº16 de la ley de Protección de Datos Personales que establece el derecho a la rectificación, actualización y supresión de la información personal.

- La actualización de la ley suponía la inclusión de nueva terminología y definiciones en base al desarrollo de nuevas tecnologías y prácticas, como datos biométricos y genéticos.
- El proyecto de ley buscaba modificar la transparencia de datos personales entre países, estableciendo que esta transparencia será lícita cuando el país poseyera un nivel adecuado de protección de datos (como la Unión Europea) y siempre que exista consentimiento previo de parte del titular de la información.

Cabe destacar que, a pesar de ser uno de los proyectos de ley impulsados por el oficialismo, a lo largo del gobierno de Mauricio Macri la iniciativa para debatir la actualización de la Ley Nº25.326 se vio frenada y no hubo avances en su trámite administrativo. Más allá de este hecho, cabe señalar que esta propuesta era necesaria dado que significó la posibilidad de iniciar el debate necesario para adecuar una legislación que ya posee más de dos décadas en su elaboración.

4. Legislaciones Nacionales respecto de la videovigilancia

4.1 Normativas Generales

En 1994 se llevó a cabo en Argentina la reforma constitucional que incorporó grandes cambios en materia de legislación porque se incluyeron Tratados Internacionales de Derechos Humanos entre los cuales cabe mencionar la Convención Americana sobre Derecho Humano (CIDH).

Ésta, en su Artículo Nº11 establece que "*Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".*

Esta disposición es muy similar a la establecida por el Artículo Nº17 del Pacto Internacional sobre Derecho Civil y Político que afirma "*Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".* Este pacto fue incorporado en la reforma constitucional mencionada.

El principio rector de la protección de los datos de los usuarios debe tener su base en el principio de que los mismos pueden ser tratados y transformados en información únicamente para los fines que han sido autorizados por parte de los dueños y por medio de personas autorizadas.

4.2 Normativas Específicas

En el ámbito nacional existen otras normativas específicas referidas a videovigilancia. Por un lado, la Resolución Nº238/2012 del Ministerio de Seguridad de la Presidencia de la Nación que

regula el sistema de videovigilancia "*en el ámbito de la Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval Argentina y/o Policía de Seguridad Aeroportuaria".*

El trabajo de Eileen Berenice Cejas y Carlos César González "*Estado de la normativa sobre videovigilancia en Argentina y su relación con la protección de datos personales"* (2015) aborda los principios de funcionamiento del sistema de videovigilancia los cuales deberían ser legalidad respeto a la privacidad de las personas y transparencia. El trabajo también hace referencia a la ley Nº25.326 donde se afirma que el sistema

> *(...)" debe cumplimentar las exigencias previstas en materia de procedimiento, tratamiento de datos, deber de reserva y confidencialidad, protección y resguardo de la información, cumplimiento exclusivo de la finalidad específica de su creación, funcionamiento e inscripción de banco de datos exigido por la misma ley*" (Cejas y González 2015, p.4)

A su vez, la Disposición 10/2015 de la (DNPDP) contiene una serie de principios aplicados a los sistemas de videovigilancia dentro del territorio argentino donde se enfoca en dictar normas reglamentarias que deben ser controladas en el desarrollo de las actividades comprendidas por la Ley Nº25.326. La disposición enfatiza en los requisitos de la licitud para la recolección de estas imágenes e informaciones personales de la ciudadanía, así como al respeto hacia la finalidad con que ha sido recolectada esta información.

La normativa busca asegurar la calidad de los datos captados por las cámaras de videovigilancia, garantizando la seguridad y confidencialidad de dicha información a fin de preservar el derecho a la privacidad de la ciudadanía, y, al mismo tiempo, garantizar el ejercicio de los derechos a la supresión y rectificación de la información equivocada por parte de los titulares de la información. En sus puntos más relevantes, la Resolución N°238/2012 del Ministerio de Seguridad de la Presidencia de la Nación establece los lineamientos generales y premisas esenciales respecto del funcionamiento de videocámaras en espacios públicos, desarrollando criterios de localización y utilización, tratamiento y confidencialidad de las imágenes registradas, procedimientos aplicables, funcionamiento de los centros de monitoreo y casos específicos de comunicación y remisión a las autoridades judiciales y del Ministerio Público Fiscal competentes. Sus lineamientos buscan estar equiparados en términos legales a los recaudos y precisiones establecidos por la Ley Nº25.326 surgida en el espíritu de un marco de coordinación de las fuerzas de seguridad e instituciones policiales federales buscando establecer un *"protocolo general de utilización de videocámaras en espacios públicos".*

En el siguiente cuadro se resumen las principales normativas nacionales específicas vigentes respecto de la videovigilancia.

Cuadro Nº2: Normativas Nacionales específicas respecto de videovigilancia

Resolución N°238/2012 Ministerio de Seguridad Presidencia de la Nación	• El ministerio de seguridad establece la supervisión de los centros de monitoreo urbano y la normativa para la instalación y uso de la tecnología de videovigilancia. • El uso de las imágenes captadas debe estar destinado sólo a la prevención y punición de ilícitos generando pruebas para la investigación judicial considerando a la seguridad como un valor esencial en el estado de derecho. • El uso de esta tecnología de videovigilancia sólo puede ser operada por las autoridades competentes que maniobren estos sistemas basados en principios de legalidad y privacidad de la ciudadanía. • La instalación y ubicación de videocámaras debe estar publicado para fortalecer el acceso a la información por parte de la ciudadanía y transparentar el manejo de las fuerzas de seguridad. • Se prohíbe el uso de los dispositivos de videovigilancia para la práctica de actividades con fines discriminatorios. • Los agentes públicos destinados a la cooperación de las tecnologías de videovigilancia deben respetar los principios de confidencialidad y legalidad en el tratamiento de la información captada buscando respetar la privacidad de la población.
La Disposición 10/2015 de la (DNPDP)	• En el artículo primero se exige el consentimiento previo del titular del dato debiendo informar que la captación de la imagen puede realizarse a través de un cartel que indique la presencia de cámaras de videovigilancia en la zona, pero sin necesidad de que se indique su ubicación específica. Se establece que no se requerirá el consentimiento en 3 excepciones: 1. Cuando la recolección del dato la realice el organizador de un evento privado en un espacio público o privado. 2. Cuando quien recolecte el dato sea el Estado en ejercicio de sus funciones (respetando el Artículo N°6 de la Ley Nº25.326). 3. Cuando la recolección del dato se realice en un espacio de uso propio. • Las imágenes captadas no pueden tener un destino diferente a lo que motivó su captación. • Garantía en la calidad de los datos: estos deben tener relación con la finalidad con los que han sido captados. • Los datos captados por el sistema de videovigilancia deben ser resguardados de forma segura y confidencial para evitar pérdidas o usos no autorizados de los mismos. • El titular de los datos tiene derecho a suprimir o rectificar la información errónea. • Todas las bases de datos que recolectan información a través de cámaras de videovigilancia deben estar registradas en el registro nacional de bases de datos.

Fuente: Elaboración propia en base a las letras de las leyes

4.3 Recomendaciones de las ONGs

Es importante incluir en la discusión a las figuras de las ONGs y a la ciudadanía preocupada en cuestiones de la privacidad cuyas posturas ayudarán a enriquecer y brindar nuevos enfoques a la polémica en torno a la aplicación de estos sistemas en el espacio público para garantizar la

correcta aplicación de las tecnologías de videovigilancia y reconocimiento facial en los mismos. El trabajo de Cejas y González (2015) realiza una serie de recomendaciones:

- Las leyes existentes deben adecuarse a la totalidad de principios de la Disposición 10/2015/DNPDP.
- Buscar la forma de brindar participación a la ciudadanía, ONGs y organizaciones civiles al momento de decidir y planificar la instalación de cámaras de videovigilancia en el ámbito público.
- Establecer en forma clara bajo qué circunstancias y con qué cuidados las imágenes captadas por el sistema de videovigilancia pueden ser cedidas a los medios de comunicación bajo regímenes de responsabilidad unificados.
- Instalar medios técnicos y tecnológicos más seguros para el almacenamiento de imágenes y videos captados por el sistema de videovigilancia y la posterior supresión de ese contenido.
- Disponer un plazo unificado de almacenamiento de imágenes y videos a nivel nacional que responda a los principios de proporcionalidad y razonabilidad.
- Modificar la Ley N°25.326 de protección de datos personales o sancionar una ley a partir de la cual se creen organismos autónomos y autárquicos capaces de auditar el uso de los datos personales de la ciudadanía por parte de distintos organismos del Estado.

Conclusión

Este capítulo ha profundizado sobre conceptos fundamentales para una mejor comprensión de la temática planteada. Uno de ellos es la noción de privacidad y la transformación experimentada a lo largo del tiempo como resultado de los cambios sociales y tecnológicos ocurridos en el interior de las sociedades.

Existe un tema al que se debe tener en cuenta: las modificaciones que la legislación argentina debió realizar y continuar ejecutando para acompañar los cambios y transformaciones que sufre el concepto de privacidad en las sociedades contemporáneas, enfatizando, sobre todo, en la tercera etapa la cual se encuentra fuertemente relacionada con la idea de información personal de la ciudadanía, resultado de la penetración de las nuevas tecnologías digitales y, en especial de aquellas de vigilancia diaria sobre la población.

Este capítulo contempla además del concepto de privacidad propiamente dicho y las transformaciones que ha ido sufriendo en Argentina, las normativas nacionales generales y específicas que lo avalan. El andamiaje de la legislación nacional respecto a la privacidad de

los individuos muestra la intención de adecuarse a la tercera etapa de la privacidad. Sin embargo, se observa que los intentos por acomodar y actualizar normas específicas para la protección de los datos personales de la población, como la Ley Nº25.326 mencionada en el marco del capitalismo informacional no se concretan por falta de consenso político entre el oficialismo y la oposición como ocurrió en el caso argentino.

Por ello, uno de los ejes centrales de este capítulo se enfoca en el análisis de esta ley que busca garantizar la protección integral de los datos personales frente al accionar de las nuevas tecnologías y modalidades de vigilancia implementadas por las fuerzas de seguridad Comprender las disposiciones establecidas por esta legislación resulta crucial a la hora de analizar las tensiones provocadas entre privacidad y vigilancia en la sociedad porteña actual.

El capítulo recorre los intentos por renovar las disposiciones establecidas en la Ley Nº25.236 para adecuarla al nuevo escenario de sociedad de control que experimenta Argentina remarcando los obstáculos que han impedido llevar a cabo esta renovación. Eventualmente se analizan las legislaciones específicas que a nivel nacional tienen el objetivo de regular el funcionamiento del sistema de videovigilancia para garantizar el derecho constitucional del derecho a la privacidad e intimidad de cada sujeto.

El análisis de la Resolución 238/2012 del Ministerio de Seguridad de la Presidencia de la Nación, la Ley Nº25.326 y/o la Disposición 10/2015 de la Dirección Nacional de Datos Personales resulta fundamental para comprender el marco regulatorio de las nuevas tecnologías de vigilancia y control que operan en el país. Conocerlas será de utilidad para encuadrar el abordaje de los casos de análisis seleccionados para esta tesis.

Finalmente, las ONGs, preocupadas frente a los potenciales riesgos que supone la implementación de las cámaras de videovigilancia con reconocimiento facial, hacen hincapié tanto en las legislaciones como en el funcionamiento de las nuevas modalidades y tecnologías de vigilancia. La actualidad atraviesa la tercera etapa de la privacidad la cual se relaciona directamente con el de información personal, producto del avance de las nuevas tecnologías digitales en la vida diaria donde también se incorpora la tecnología empleada por las fuerzas policiales para el control y la vigilancia. En los próximos capítulos, que, pese a la normativa desplegada para contemplar y codificar una tercera etapa, de todos modos, en ocasiones las prácticas de saber-poder ejercidas desde los gobiernos y fuerzas de seguridad tienden frecuentemente a tensionar los derechos y obligaciones establecidas en dichas regulaciones.

Capítulo 5: Reconocimiento facial en CABA y leyes

Introducción

En este capítulo se hace referencia a la implementación del sistema de reconocimiento facial en CABA, a las fuerzas de seguridad que operan estas tecnologías de vigilancia y control y a las características técnicas propias de estas herramientas con sus falencias y errores.

Asimismo, se profundiza en la forma de aplicación del reconocimiento facial en el espacio público de CABA en 2019, los objetivos que se pretenden alcanzar desde el Gobierno de la Ciudad y las voces detractoras provenientes de las organizaciones de la sociedad civil, entre ellas, la Asociación por los Derechos Civiles (ADC) y la Fundación "Vía Libre", cuyos integrantes cuestionan la implementación de las mismas y alertan sobre los riesgos que su aplicación conlleva para la privacidad e intimidad de la población.

Por último, se realiza un recorrido en torno a las legislaciones de CABA que regulan el sistema de videovigilancia y reconocimiento facial en la Ciudad, mientras buscan preservar y garantizar el derecho a la privacidad de la ciudadanía frente a la aplicación masiva de tecnologías de vigilancia.

Como ya se ha visto, el siglo XXI trajo aparejado profundos cambios dentro del paradigma de seguridad de las naciones las cuales han implementado una política de "guerra preventiva" (Alcántara 2008), buscando controlar exhaustivamente a su propia ciudadanía para evitar la aparición de amenazas internas que pusiesen en peligro las sociedades (el terrorismo o criminalidad). Estos cambios, indudablemente contribuyen a consolidar la aplicación de las sociedades de control en el mundo contemporáneo. La sociedad de control implica la adopción de formas de control "ultrarápidas" en el espacio público, las cuales se tornan omnipresentes e invisibilizadas y reemplazan a las antiguas formas de control propias de la sociedad disciplinaria que operaban dentro de los espacios cerrados como remarca Rodríguez (2008).

La sociedad de control está más relacionada con los adelantos técnicos/tecnológicos de vigilancia y control que con las instituciones. Esto permite que la vigilancia ejercida por los Estados pueda ser desempeñada de manera más discreta y flexible e incluso, promocionar estas tecnologías como instrumentos para el combate de la inseguridad y contar así con el apoyo de la población.

Una de las características más notorias de la sociedad de control es, como sostiene Gendler (2017), el hecho de que la población ya no se encuentra sometida a una vigilancia permanente dentro de un espacio confinado, sino que existe la tendencia a la libre circulación de los individuos en el espacio público.

Ello provoca que en sociedades como en CABA, donde opera el reconocimiento facial, toda la ciudadanía sea susceptible de ser identificada y catalogada como "sospechosa" por parte de los nuevos instrumentos de vigilancia y control de las fuerzas de seguridad.

La idea de panóptico es propia de las sociedades disciplinarias donde se produce una construcción de "celdas y espacios" y donde los sujetos son individualizados y visibles constantemente por parte de quien los observa.

Lío (2015) sostiene que el concepto de panóptico debe ser revisado a la luz de las nuevas modalidades de vigilancia que operan en las sociedades a partir del desarrollo y expansión de la infra cultura digital. De acuerdo con su trabajo, el desarrollo y aplicación de tecnologías como el sistema de reconocimiento facial y videovigilancia puede ser considerado como una nueva expresión del poder disciplinario del panóptico en las sociedades contemporáneas, estableciendo una vigilancia permanente e invisibilizada (similar a un ojo que "todo lo ve") sobre la población y regulando su accionar en el marco de las sociedades de control.

Aquí se empieza a delinear la configuración que posibilita el despliegue de estas prácticas de control y vigilancia.

1.Situación en CABA

El uso de las tecnologías de vigilancia y control no son utilizadas exclusivamente en países centrales como Estados Unidos o China. Paulatinamente también comienzan a implementarse en países periféricos como en el caso de Argentina.

Durante su primer mandato (2015-2019) el Jefe de Gobierno porteño, Horacio Rodríguez Larreta levantó dos grandes banderas que caracterizaron su gestión: seguridad y modernización. Estas consignas lo acompañaron a lo largo del 2019 durante la campaña política para ser reelecto en su cargo. El 24 de abril de 2019 el viceministro del gobierno porteño y quien también está a cargo del Ministerio de Justicia y Seguridad de CABA, Diego Santilli, anunciaba la implementación de un software ruso de reconocimiento facial para la detección de delincuentes con "pedido de captura" que surgen del sistema de Consulta Nacional de Rebeldías y Capturas (CONARC) del Registro Nacional de Reincidencia.

En la inauguración de la técnica, el 25 de abril de 2019, Santilli sostuvo que existen más de 40.000 prófugos: 15.000 por robo y hurto, 1.500 por delitos sexuales, 2.300 por narcotráfico y 1.300 por homicidios.[44]

Horacio Rodríguez Larreta presentó el sistema de vigilancia y control afirmando "*es un paso más que estamos dando de incorporar tecnología para cuidar a la gente de la Ciudad, nuestro único objetivo en esto es que los vecinos de la Ciudad estén más seguros y no estén en la calle caminando alrededor de delincuentes*"[45]

La ministra de Seguridad, Patricia Bullrich, quien acompañó a Larreta en la presentación del sistema de vigilancia también sostuvo "*ahora con estas cámaras inteligentes que buscan*

[44] Véase https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

[45] Véase https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

específicamente a estos prófugos creo que vamos a tener una capacidad de darle una enorme tranquilidad a la sociedad de que no esté caminando al lado de un asesino, al lado de un pederasta o de un pedófilo. Esto es una manera real de cuidar a la gente"[46].

El sistema de reconocimiento facial de prófugos es una extensión del sistema público integral de videovigilancia. La red integral de monitoreo de CABA cuenta con 12.906 dispositivos repartidos en la Ciudad entre las que se incluye 871 en las estaciones de subte, 327 en AUSA, 130 en tránsito y 4.000 en colectivos sumados a las que existen en la vía pública.

Esta red está supervisada desde dos centros de monitoreo urbano: uno situado en el barrio de Chacarita y otro en la intersección de Diagonal Norte y Avenida 9 de Julio.

Si bien en su primera etapa de despliegue y aplicación el sistema fue utilizado en entornos cerrados y controlados (estaciones de subte), en esta nueva etapa de la gestión, el gobierno porteño buscará ampliar y expandir la red de cámaras de reconocimiento facial incorporándolas en zonas con menor densidad de población incrementando el apoyo de este sistema en los "senderos escolares". Asimismo, se sumarán cámaras y equipos de monitoreo en puntos de acceso a la Ciudad donde tienden a producirse situaciones delictivas.

El sistema de identificación facial opera de manera rotativa a través de 300 de las casi 13 mil cámaras callejeras con las que cuenta la Ciudad requiriendo que el ciudadano a detener se encuentre por ende en la vía pública (puntos neurálgicos de la Ciudad como estaciones de trenes y subtes). Son en estos puntos claves de la metrópoli donde se ha efectuado un reconocimiento facial y posterior detención de un importante porcentaje de prófugos de la justicia.

Una de las detenciones que tuvo mayor repercusión en los medios de comunicación fue la identificación y detención, por medio del software, de un abusador sexual denunciado 18 veces por delito de abuso sexual agravado en diferentes distritos. El abusador fue detenido en la estación Congreso de la línea A del subte, en el barrio porteño de Balvanera y puesto a disposición del Juzgado Criminal de Instrucción Nº35.

De acuerdo con declaraciones del Ministerio de Seguridad de la Ciudad de Buenos Aires, durante los primeros 88 días de la implementación del sistema, el cual, según el ministerio opera sólo con un margen de 4% de error, se emitieron 1.227 alertas de personas de las cuales, 226 quedaron detenidas por delitos graves, 13 fueron acusados de abuso, 10 por homicidio, 11 por narcotráfico y 57 por delito de robo a mano armada, es decir, un 18.41% del total de los casos, mientras el resto de alertas, que fueron 1.001 representando un 81.59% de los casos

[46]Véase https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

fueron liberadas, pero no debido a fallas del sistema de reconocimiento facial sino a errores en el manejo de las bases de datos.

La operatoria puede resumirse en la siguiente secuencia:

1) El poder Judicial establece las órdenes de captura para individuos requeridos por la justicia penal.
2) El sistema de reconocimiento facial desplegado en las 300 cámaras de CABA identifica el rostro de ciudadanos que transitan por puntos neurálgicos de la Ciudad.
3) Cuando el sistema de reconocimiento facial identifica a una persona incluida en la base de datos del CONARC, los Centro de Monitoreo Urbano avisan al personal policial más cercano. Estas órdenes de captura pueden provenir del Poder Judicial Federal, Nacional, Provinciales y de la Ciudad Autónoma de Buenos Aires.
4) La alerta llega al personal policial a través de una aplicación específica instalada en los teléfonos institucionales de la policía cercanos a la cámara que emitió la alerta. El personal policial recibe el nombre, apellido, tipología de la causa y las imágenes de la persona buscada, además de un mapa que indica la cámara que emitió dicha alerta.
5) Una vez que la policía ha capturado al presunto prófugo, éste es demorado por la fuerza de seguridad hasta que desde los juzgados se aclare su situación, proceso que puede tomar varias horas. A veces, el retraso se debe a la falta de respuesta por parte del juzgado o al sistema que no relaciona nombre y apellido con el número de documento del demorado. Como se mencionó, la mayoría de los ciudadanos identificados por el sistema en CABA fueron puestos en libertad por orden de los juzgados.

A comienzos del 2019, la ministra de Seguridad de la Nación, Patricia Bullrich afirmaba que, si de ella dependiese, el registro de ADN debería ser obligatorio para los habitantes de la Nación y no sólo para aquellos que hayan incurrido en algún delito.[47]

El desarrollo de estas tecnologías de vigilancia, control y entrecruzamiento de datos puede llevar a que, paulatinamente, Argentina se transforme en una sociedad con un sistema de vigilancia generalizada bajo el argumento de que éstas son empleadas como instrumentos para producir una sociedad más segura y combatir la criminalidad. La instrumentalización de las medidas de control se origina en las nuevas modalidades de control social y en el temor de la población de verse afectada por conductas que generen una acción disruptiva tanto en su integridad personal como en sus bienes materiales y la percepción de que en la sociedad

[47] Véase https://www.infobae.com/opinion/2019/02/27/adios-a-la-privacidad-un-registro-nacional-de-adn-como-gran-hermano-de-la-nueva-era/

contemporánea existe una situación de violencia generalizada donde la delincuencia tiene repercusiones inmediatas en la calidad de vida.

La incorporación de tecnologías de vigilancia y control como las que se están implementando en el país son modalidades propias de la sociedad de control, ya que tienen por objetivo el monitoreo permanente bajo la argumentación de la prevención de situaciones de riesgo y criminalidad, lo que caracteriza su instrumentalidad.

2. Las Cámaras son los juguetes. El jugador, la policía de la Ciudad. El juego, la vigilancia

Para el abordaje de la tesina es necesario caracterizar a las fuerzas de seguridad que operan las tecnologías de vigilancia y control en la Ciudad Autónoma de Buenos Aires en el año 2019. En la Capital Federal, tanto el sistema de videovigilancia como el software de reconocimiento facial incorporado al sistema son manejados por la fuerza de seguridad denominada "Policía de la Ciudad de Buenos Aires". Creada por la Ley Nº5.688/16 del Sistema Integral de Seguridad Pública, fue sancionada el 17 de noviembre del 2016 y puesta en operación el 1 de enero del 2017 durante el mandato presidencial de Mauricio Macri y Horacio Rodríguez Larreta como Jefe de Gobierno, ambos funcionarios políticos pertenecientes a la alianza política "Cambiemos".

La fuerza de Seguridad fue creada por iniciativa de Rodríguez Larreta[48] e ideada como una fuerza única de seguridad policial de la Ciudad de Buenos Aires como resultado de la unión de la Policía Metropolitana con la Superintendencia de Seguridad Metropolitana de la Policía Federal, la cual había sido traspasada al gobierno de la Ciudad por iniciativa de Mauricio Macri cuando era mandatario de la Nación.

De acuerdo con la resolución N°312/MJYSGC/18 se establecen las áreas y responsabilidades primarias de la Policía de la Ciudad, donde se incluyen tres Superintendencias fuertemente relacionadas con la aplicación de tecnologías de control y vigilancia dentro del espacio público de la Ciudad. [49]

En primer lugar, la policía de la Ciudad cuenta con la Superintendencia de Operaciones y Orden Urbano cuyo objetivo, según la página oficial de la fuerza, es planificar y disponer de los servicios de seguridad urbana necesarios para la prevención general del delito y la preservación del orden público. En segundo lugar, la fuerza de seguridad cuenta con la Dirección Autónoma

[48] Véase https://es.wikipedia.org/wiki/Polic%C3%ADa_de_la_Ciudad_de_Buenos_Aires

[49] Véase https://documentosboletinoficial.buenosaires.gob.ar/publico/PE-RES-MJYSGC-MJYSGC-312-18-ANX.pdf

de Análisis e Información Delictual que se encarga de diseñar, proyectar y coordinar sistemas de información de soporte de toda la información vinculada a la actividad criminal, y también de planificar y ejecutar las actividades de obtención y análisis de la información en materia criminal. Por último, es importante destacar que la Policía de la Ciudad cuenta con la Dirección Autónoma de Tecnologías Aplicadas a la Seguridad cuya responsabilidad primaria apunta a intervenir en el transporte, administración y monitoreo de imágenes móviles y fijas de video vigilancia policial y mediar en las actividades operativas ligadas a la generación de imágenes de video relacionadas con los objetivos fijados por la institución policial para el desenvolvimiento de su función. Asimismo, esta Dirección tiene la función de coordinar las necesidades tácticas y operativas para brindar una respuesta eficiente y dinámica a los requerimientos de la Superioridad o de la Justicia para la obtención de las imágenes. También debe responder a los requerimientos Judiciales con las imágenes del sistema de videovigilancia y brindar asistencia técnica y asesoramiento a la Superioridad y al Gobierno de la CABA cuando sea debidamente solicitado en materia de monitoreo de imágenes ejerciendo las facultades que disponen las normas regulatorias en la materia.

Como se ha mencionado en anteriores capítulos, el objetivo de la policía es abordar y administrar todo lo que sucede en las sociedades por pequeño e insignificante que pueda parecer (Foucault, 1975) por lo que, las fuerzas de seguridad son equipadas con instrumentos y tecnologías de control que permitan realizar una vigilancia omnipresente y capilar sobre la población.

De acuerdo con Hidalgo (2004) tanto la metodología de trabajo como las fuerzas de seguridad han ido mutando y cambiando, generando modificaciones en la forma de controlar los espacios públicos mediante la incorporación de tecnologías digitales que le ha otorgado a las fuerzas de seguridad realizar una actividad de naturaleza informacional. En el marco de las sociedades de control, los individuos tienen una mayor libertad de circulación en el espacio público, pero se encuentran sometidos a sospecha y vigilancia permanente. Por lo tanto, las fuerzas de seguridad debieron modularse con tecnologías y modalidades de vigilancia propias de las nuevas sociedades de manera que puedan ejercer sobre los sujetos una vigilancia constante y al aire libre casi sin que los sujetos se percaten de ello.

En el capítulo 3 de esta tesina se observó que la política del miedo exacerba los temores de la población para obtener mayores concesiones en torno a la aplicación de tecnologías de control y vigilancia más intrusivas sobre su privacidad con el argumento de estar combatiendo la criminalidad y generar sociedades más seguras. Esto no es una característica propia de la Argentina, sino que se trata de un fenómeno global por lo cual Lechner (2016) sostiene *"(...)*

Los Estados se han tecnificado con métodos y diseños tanto de prevención como de punición contra los delitos". (Lechner, 2016, p.4).

Entonces, la implementación de tecnologías de control y vigilancia sobre las sociedades contemporáneas no responde a un fenómeno aislado, ya que es posible identificar nuevas formas de control y monitoreo de la población realizadas por las fuerzas de seguridad del Estado en regiones tan distantes y diversas como lo es la República Popular de China, los Estados Unidos e incluso la Argentina.

2.1 El gran oculista de la Ciudad: Los Centros de Monitoreo Urbano.

CABA ha sido una de las ciudades pioneras en el país en incorporar el sistema de video vigilancia. La regulación de este sistema se ha generado tomando como base la Ley Nº9.380 sancionada en el 2007 en la provincia de Córdoba. En 2008 la Ciudad Autónoma de Buenos Aires sancionó la Ley Nº2.602 tomando en cuenta aspectos presentes en la Ley Nº9.380 como el plazo para el almacenamiento de las imágenes, el carácter confidencial de las mismas, etc. Un año más tarde, en 2009 se inauguró el sistema de monitoreo urbano de la Ciudad con el apoyo y críticas de diferentes sectores de la sociedad como las organizaciones gubernamentales y no gubernamentales y los habitantes de la Ciudad, todos preocupados por el riesgo que el sistema podía presentar para sus datos personales.

Los Centros de Monitoreo Urbano (CMU) son dependientes de la Dirección de Tecnología y de la Superintendencia de Comunicaciones y Servicio Técnicos. El centro más reciente fue fundado en junio del 2019 por la Policía de la Ciudad en el barrio de Chacarita.

De acuerdo con la página oficial del Gobierno de la Ciudad Autónoma de Buenos Aires, el (CMU) es uno de los centros más grandes y modernos de América Latina. Su función principal es la prevención de delitos e intervención alertando a los oficiales presentes por la zona. Las tecnologías con las que cuenta este centro son empleadas como apoyo en investigaciones judiciales y policiales. El CMU cuenta con capacidad de monitorear 7.300 cámaras de videovigilancia, algunas de las cuales poseen reconocimiento facial, y se encarga de supervisar 4.000 cámaras instaladas en unidades de transporte público que circulan diariamente por CABA.

En el lugar trabajan 542 personas entre personal civil y policial de las cuales, 422 son operadores que monitorean las imágenes captadas por el sistema de videovigilancia. Los operadores se distribuyen en tres turnos de ocho horas diarias bajo la responsabilidad de un coordinador operativo y un coordinador general las 24hs del día los 365 días del año.

Las computadoras utilizadas para el monitoreo de las cámaras de videovigilancia son de alto rendimiento, con capacidad de procesar imágenes captadas en 4K a alta velocidad. El material captado por el sistema de cámaras de la Ciudad es grabado en una sala de control y almacenamiento de "última generación" donde el material se aloja de modo restringido y el sistema de archivo digital de imágenes se protege mediante una doble encriptación.

Según la página oficial del GCBA el funcionamiento del CMU cuenta con un protocolo de actuación mediante el cual se prohíbe la difusión de imágenes captadas por el sistema de cámaras, las cuales pueden ser solicitadas por un juez como una medida de prueba en una investigación judicial. El gobierno afirma que el software utilizado en este sistema de vigilancia impide tomar imágenes de ámbitos privados y se encuentra limitado únicamente al espacio público.

El trabajo de Eileen Cejas *"Centro de Monitoreo Urbano en la Ciudad Autónoma de Buenos Aires: la importancia de la participación ciudadana en el control del sistema"* (2016) plantea una serie de falencias en la operación de los CMU como por ejemplo "*no existe la inscripción a la base de datos de la defensoría del pueblo (según la Ley Nº25.326)"* (Cejas, 2016, p.7).

La instalación de cámaras de videovigilancia en el espacio público está condicionada por la energía que proviene del alumbrado público, por lo que no es posible la instalación de cámaras si no existen columnas que posean cédula fotoeléctrica.

3.Tolkien lo soñó, la tecnología lo creó. Hay un ojo que todo lo ve: Aspectos técnicos del reconocimiento facial en CABA

La implementación de los sistemas de reconocimiento facial que se acoplan a la infraestructura de cámaras de videovigilancia y operan en CABA ha generado fuertes preocupaciones en cuanto al riesgo que supone para la privacidad de la ciudadanía. Diversas organizaciones no gubernamentales como la Asociación por los Derechos Civiles, (ADC) ha solicitado informes al Gobierno de la Ciudad Autónoma de Buenos Aires para conocer con mayor profundidad el funcionamiento legal y técnico de estos dispositivos de control y vigilancia, sobre todo, si se toma en cuenta que el software de reconocimiento facial puede llegar a tener altos porcentajes de falsos positivos como se reflejó en las pruebas que la Metropolitan Police de Londres realizó entre 2016 y 2018[50] con un resultado del 96% de personas mal identificadas como criminales. En este sentido, estos softwares pueden ser susceptibles a generar discriminaciones en su funcionamiento (que puede ser intencional o no) en cuanto al género, sexo o raza.

[50] Publicado en la página https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

De acuerdo con el informe que recibió la ADC por parte del Gobierno porteño previo a la implantación del sistema, la mayor preocupación de las autoridades ministeriales se centró en maximizar sus potencialidades y beneficios para la seguridad pública y, minimizar sus aspectos negativos en términos de derechos humanos.

Según las declaraciones del Gobierno de la Ciudad, el sistema de reconocimiento facial escanea y contrasta exclusivamente los datos biométricos de las personas incorporadas a la base de datos de Consulta Nacional de Rebeldías y Capturas (CONARC)[51] "*con la única finalidad de identificar a un posible prófugo y cooperar con el poder judicial en su detención"*[52], luego de lo cual se destruye el registro de la base.

Sin embargo, al consultar el boletín oficial y el sistema de compras públicos de la Ciudad es posible encontrar publicado el pliego de bases y condiciones para la contratación directa de un servicio integral de video. Entre los requisitos técnicos que el Gobierno de la Ciudad estableció en el pliego de compra aparece:

1) El software debe permitir la detección facial contando con una base de datos fotográfica de individuos los cuales serán buscados por las imágenes en vivo capturadas por las cámaras de videovigilancia de la Ciudad pertenecientes a la Policía de la Ciudad. La base de datos de búsqueda será provista por el Ministerio de Justicia y Seguridad.
2) Debe contar con una base de datos fotográfica de hasta 100.000 rostros para su posterior identificación conformando una "lista negra de personas" buscadas.
3) Debe contar con alertas de identificaciones positivas sobre las reglas aplicadas y sobre la identificación de rostros.
4) Debe resguardar estas alertas de manera encriptada.[53]

[51] El CONARC fue creado en el año 2009 por medio del decreto 346/2009 y responde a la necesidad de brindar un servicio ágil y eficiente en el intercambio de información con los Poderes Judiciales y Ministerios Públicos de toda la Argentina, la Policía Federal y las policías provinciales conforme a las bases de datos que posee el Registro Nacional de Reincidencia, el cual incluye recursos humanos e informáticos que operando en forma conjunta ofrecen una herramienta que posibilita el intercambio de información fluida entre los organismos.
El CONARC implica el desarrollo de un software por parte del Estado Nacional para combatir una criminalidad que se torna cada vez más compleja. Esta herramienta permite que las autoridades policiales y judiciales puedan obtener una respuesta inmediata y logren resolver cuestiones procesales de manera expeditiva, ya que la implementación del CONARC refleja la totalidad de los casos de rebeldía, captura, averiguación de paradero y comparendo que posee el Registro Nacional de Reincidencia.
Véase:http://www.saij.gob.ar/346-nacional-creacion-sistema-consulta-nacional-rebeldias-capturas-conarc-dn20090000346-2009-04-21/123456789-0abc-643-0000-9002soterced

[52] Véase https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

[53]Publicado en la página https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

La utilización tradicional de reconocimiento facial recurre al uso de algoritmos para identificar las características faciales de los sujetos, analizando el tamaño, la posición y forma de ojos, nariz, pómulos, etc., al tiempo que se emplean técnicas de coincidencia en las plantillas que resulta en la representación del rostro comprimido. En general, el reconocimiento facial puede tener dos enfoques: el geométrico, centrado en las características distintivas del sujeto a identificar y el fotométrico que recurre al enfoque estadístico donde la imagen se divide en valores y éstos se comparan con las plantillas existentes para eliminar las diferencias.

Concretamente, el software de reconocimiento facial es un software biométrico capaz de identificar a un individuo a partir de una imagen digital mediante el uso de algoritmos matemáticos y el mapeo de la misma manera en la que se almacenaría la información de una huella digital. Por tanto, genera la detección de un rostro para luego escanearlo, crear los objetivos y analizar las coincidencias y verificación de los individuos.

El software de reconocimiento facial que opera en CABA se denomina "ULTRAIP®" y fue desarrollado por la empresa Danaide S.A. Cuenta con técnicas de reconocimiento facial tridimensional que emplea sensores 3D para captar información sobre las formas de un rostro. Esta información se emplea para identificar características distintivas en la superficie facial de las personas como el contorno de la nariz, ojos y mentón.[54] Este software no se ve afectado por las cámaras de iluminación y logra la identificación también desde diferentes ángulos de visión.

De acuerdo con la página Web del Gobierno de la Ciudad de Buenos Aires, el software de reconocimiento facial permite detectar el género del sujeto en una foto con una precisión del 99% y la edad con una precisión del 95% en un umbral de 5 años.[55]

El software de reconocimiento facial "ULTRAIP®" comenzó a operar el 24 de abril de 2019 en CABA con Resolución Nº398/19 sobre la infraestructura de cámaras de seguridad (CCTV) y centros de monitoreo de la ciudad.

Esta tecnología permite la búsqueda en la base de datos en menos de medio segundo e implementa el reconocimiento facial en diversas condiciones de iluminación y ángulos de escena permitiendo el reconocimiento aun si el prófugo ha modificado su apariencia física (por ejemplo, barba o diferentes peinados).

Para lograr esta efectividad, las cámaras de videovigilancia tienen una resolución de 4K y permiten la visualización de escenas con muy poca luz y en condiciones climatológicas contrarias. Los dispositivos tienen autofoco y su configuración permite un registro de vigilancia

[54] Véase https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/
[55] Véase https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

en 360 grados. Están instalados en domos con un zoom óptico de 30X con alta velocidad de movimiento que los posibilita con capacidad de visualización y seguimiento de personas u objetos.

Este sistema de reconocimiento facial funciona en simultáneo en 300 cámaras de video vigilancia las cuales van rotando sobre la totalidad de las cámaras que se encuentran en operación en puntos neurálgicos de la Ciudad.

4.Intereses diferentes, opiniones diferentes: Voces a favor y en contra del reconocimiento facial

La implementación del sistema de videovigilancia y reconocimiento facial en Argentina trajo aparejado la presencia de voces a favor y en contra alrededor de estos sistemas de vigilancia y control social. El trabajo de Eileen Berenice Cejas y Carlos César González "*Estado de la normativa sobre videovigilancia en Argentina y su relación con la protección de datos personales"* (2015) apunta que en el país existen dos grandes posturas en cuanto al uso del reconocimiento facial en CABA: la gubernamental y la de las empresas licitadoras de los sistemas propiamente dichos que se encuentran a favor de estos mecanismos de control y vigilancia.

Eduardo Capelo, titular de la Cámara Argentina de Seguridad Electrónica (CASEL) es un referente a favor y opina que las cámaras "(…) *no sólo sirven contra la inseguridad*, aclara, *sino también para prestar otros servicios a la comunidad, como operar rápidamente en situaciones de accidentes o bloqueos de tránsito en caso de emergencias".* (Cejas y González, 2015, p.3)

En sintonía, la postura del GCBA continúa sosteniendo que la implementación de estas tecnologías actúa como una herramienta para prevenir y combatir los delitos ocurridos en el espacio público y garantiza la protección de la ciudadanía ante amenazas tales como la criminalidad y el terrorismo asegurando la convivencia de la población.

Desde los diferentes estratos gubernamentales, el poder político de turno pondera la utilidad de los sistemas de videovigilancia y reconocimiento facial que operan en CABA destacando su uso en la prevención del delito e incremento de la seguridad de los vecinos, justificando su implementación masiva mediante el discurso de la "política del miedo" conforme al cambio de paradigma de seguridad luego del atentado del 11 de setiembre del 2001 producido en las torres gemelas en Estados Unidos.[56]

[56] Cabe destacar al respecto que el despliegue de la política del miedo a nivel internacional también tuvo diversos correlatos en Argentina, como por ejemplo en el año 2007 cuando durante el gobierno de Cristina Fernández de Kirchner se aprobó la Ley Nº26.734 denominada Ley Antiterrorista, la cual buscaba evitar el lavado de dinero como fuente de financiamiento del terrorismo internacional y establecía penas de prisión para quienes formaran parte de una asociación ilícita con fines terroristas. Véase: https://www.argentina.gob.ar/noticias/ley-antiterrorista-otra-de-las-normas-especiales

Cabe remarcar que en Argentina también existen voces contrarias y se hacen oír. Por lo general, son las ONGs, las asociaciones civiles y los ciudadanos independientes los que cuestionan el sistema de videovigilancia que opera en CABA.

Una de las principales organizaciones que polemiza sobre la implementación masiva de esta tecnología es la Fundación "Vía libre". Esta organización, sin fines de lucro, fundada en el año 2000 promueve los ideales del software libre y lo aplica a la libre difusión del conocimiento y de la cultura. Uno de los ejes principales de su trabajo es el derecho a la intimidad de la ciudadanía, por lo que su presidenta Beatriz Busaniche afirma:

> "(…) *si contamos con que las cámaras están mayormente ubicadas en plazas y lugares de alta circulación pronto tendremos una base de datos enorme de las actividades de la gente que circula por allí, incluyendo rostros y expresiones de activistas sociales, militantes, mujeres y niños que pasan regularmente por esos lugares. Pero no tenemos muy claro qué pasa con toda la información que se recopila, cuánto tiempo se mantiene, cómo se procesa, cómo se guarda, quién tiene acceso, con qué fines se realiza*" (Cejas y González, 2015, p.3).

También, en una nota publicada el 11 de abril de 2019 por el medio Iprofesional, Busaniche critica fuertemente la instalación de los sistemas de vigilancia y control en CABA al sostener

> *"Montar un sistema de este tipo implica que hay que procesar a todas las personas. No hay forma de limitar a los malos. Los sistemas de reconocimiento facial en los espacios públicos son propios de los estados autoritarios. El más avanzado es China. Parte del supuesto de que todos somos sospechosos y representa una filosofía contraria a los derechos humanos comenzando por la intimidad de las personas."*[56]

Por otro lado, en una entrevista realizada el 26 de abril de 2019 con el medio LN, Enrique Chaparro, miembro de la Fundación "Vía Libre", afirmaba que *"el interrogante que queda abierto es ver qué piensa hacer el Gobierno de la Ciudad con las imágenes que capta y analiza de personas que no son los delincuentes que están prófugos".*[57]

Busaniche también denuncia el avance en materia de vigilancia en la sociedad argentina cuando remarca que

> *"En nombre de la seguridad pública, Argentina ha impulsado políticas de vigilancia masiva incluyendo un monitoreo generalizado del espacio público. La privacidad es particularmente esencial en un país que a lo largo de su historia ha tenido importantes movimientos sociales y políticos que han ganado las calles para hacer oír su voz. Es de enorme importancia que los activistas puedan permanecer anónimos en las manifestaciones públicas, en particular cuando están en desacuerdo con el gobierno. De esta manera, SIBIOS no sólo amenaza la privacidad de los ciudadanos y el derecho a la protección de sus datos personales, sino que también involucra una seria amenaza a los derechos civiles y políticos".*[58]

[57] Véase https://www.youtube.com/watch?v=mrlrqxbrbY8

[58] Véase https://www.vialibre.org.ar/2012/01/10/biometria-en-argentina-la-vigilancia-masiva-como-politica-de-estado/

La falta de transparencia en torno al manejo del sistema SIBIOS favorece que el Estado fácilmente pueda violar los principios establecidos por ley para garantizar una mínima recolección de datos porque permite una masiva e innecesaria recolección de datos personales y sensibles por parte del Estado, lo cual le brinda un gran poder concentrado.

Según declaraciones de la Electronic Frontier Foundation (EFF), una de las principales ONG que actúa a nivel mundial en defensa de la privacidad digital sostiene que el desarrollo de tecnologías de vigilancia y control que realicen un seguimiento perfecto de los habitantes es dañino y perjudicial para una sociedad libre y democrática. Al respecto, Katitza Rodríguez, su Directora Internacional de Derechos Civiles, señala que la vigilancia puede justificarse cuando ha sido prescripta por una ley públicamente disponible que cumpla con un nivel de precisión y claridades suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. La vigilancia debe ser limitada a lo que es estrictamente necesario para alcanzar un objetivo legítimo, como un último recurso disponible o habiendo varios medios, sea el menos propenso a vulnerar los derechos humanos.[59] Por ende, los ciudadanos deben tener expectativas razonables en torno a mantener su privacidad y anonimato, en particular, frente a la construcción de perfiles por parte del Estado.

A pesar de las advertencias realizadas por académicos y expertos sobre los riesgos que conlleva la aplicación de estas tecnologías de control y vigilancia sobre la población, a pocos días de la implementación del sistema de reconocimiento facial en CABA los medios de comunicación masivos han comenzado a informar sobre fallas en él.

Si bien no fue esta la situación presentada en los casos de Rachel Holway y de Federico Ibarrola analizados en el capítulo 6, los falsos positivos son uno de los errores más comunes cuestionados por el sistema de reconocimiento facial y representan un grave riesgo para el derecho a la privacidad de la ciudanía. Y así lo expresa Enrique Chaparro *"Todos los sistemas de reconocimiento facial tienen un porcentaje significativo de lo que se llama falsos positivos, un ejemplo de esto fue hace unos años en un partido de la Champions League donde la policía de Gales desplegó el sistema para identificar a las personas que tenían prohibido ingresar a los estadios. El resultado fue que de los 2.900 identificados, un 92% fue de falsos positivos".*[60]

Este sistema de vigilancia y control no está exento de polémicas debido a los falsos positivos ocurridos en CABA donde el Ministerio de Justicia y Seguridad de la Nación asegura que el

[59] Véase https://www.lanacion.com.ar/tecnologia/en-busca-de-las-armas-de-vigilancia-masiva-nid1636661
[60] Véase https://www.youtube.com/watch?v=mrlrqxbrbY8

margen de error del sistema es muy bajo y que los falsos positivos rondan el 4% de las identificaciones totales realizadas por el sistema.

Por su parte, Leandro Ucciferri, abogado e investigador de ADC, Asociación de los Derechos Civiles, sostiene que con la implementación de estas tecnologías de control y vigilancia *"se coarta la libertad",* y acota "a *la vigilancia estatal se le suma el control sobre el comportamiento. Es simplista decir que los malos van a ser arrestados con esta herramienta",* afirmó en una entrevista brindada al medio Iprofesional el 11 de abril de 2019. Ucciferri también advirtió que *"cuando se usan grandes bases de datos, se viola el principio de inocencia y debido proceso contemplados en los artículos Nº18 y Nº19 de la Constitución Nacional. Por estar presente en una base de datos hay reversión en la carga de la prueba porque no se presume inocencia."*[61]

Estos sistemas de vigilancia avanzan sobre la privacidad y presunción de inocencia de la ciudadanía, como afirmó Beatriz Busaniche en una entrevista con el medio ANCCOM *"Todos estamos siendo monitoreados permanentemente en búsqueda de criminales, pero somos inocentes. Si nos pidieran permanentemente el DNI en la calle lo veríamos con malos ojos, como un Estado autoritario"*[62]

5. Legislación de la Ciudad Autónoma de Buenos Aires

El reconocimiento facial ha comenzado a operar en CABA con la Resolución 398/19 del Ministerio de Justicia y Seguridad y su anexo. En ella se establece que, si bien la Constitución de la Ciudad Autónoma de Buenos Aires en su Artículo N°12 reconoce como garantía "*el derecho a la privacidad, intimidad y confidencialidad como parte inviolable de la dignidad humana"* también afirma en el Artículo N°34 que "*la seguridad pública es un deber propio e irrenunciable del Estado y es ofrecido con equidad a todos los habitantes".*

Esta resolución, que inició el funcionamiento de reconocimiento facial en la Ciudad afirma que a través la Ley Nº5.688 del sistema integral de seguridad pública, CABA adhirió al funcionamiento de la Ley Nacional Nº24.059 de Seguridad Interior donde se establece como definición de seguridad pública a la situación basada en el derecho en el cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional y la Constitución de la Ciudad Autónoma de Buenos Aires.

[61] Véase https://www.iprofesional.com/tecnologia/289744-delitos-informaticos-ley-procesal-Cuestionan-el-sistema-de-videovigilancia-porteno-por-vulnerar-derechos-humanos

[62] Véase https://www.vialibre.org.ar/2019/05/13/el-gran-hermano-porteno/

El gobierno de la Ciudad se ampara en el Artículo N°75 como uno de los principios rectores de la resolución ya que en su punto 7 afirma

> "(…) *innovación tecnológica, incorporación y desarrollo de nuevas tecnologías para mejorar la gestión institucional y la transparencia, incrementar la protección del personal policial en el ejercicio de las funciones, disuadir la comisión de delitos y contravenciones, mejorar la previsión de conductas delictivas y la investigación de nuevas formas de criminalidad*".

Al mismo tiempo, el Artículo N°474 de esta ley crea el "*sistema público integral de video vigilancia de la Ciudad Autónoma de Buenos Aires*" cuya autoridad de aplicación es el Ministerio de Justicia.

Es interesante notar, que la Resolución 398/19 establece que la regulación del sistema público integral de videovigilancia de CABA incluye el posterior tratamiento de las imágenes captadas por el sistema de vigilancia respetando el régimen de garantías de los derechos fundamentales y de las libertades públicas de la ciudadanía, las cuales deben ser respetadas de forma ineludible en la grabación y uso de las imágenes. La Resolución también afirma que la utilización integral del sistema de videovigilancia debe basarse en los principios de proporcionalidad y razonabilidad[63] y con intervención mínima sobre la privacidad de la población. Por lo tanto, el uso de estas tecnologías de control y vigilancia para la prevención y combate de la criminalidad en el espacio púbico debe ser controlado y proporcionado a fin de evitar abusos sobre la privacidad de la población.

De acuerdo con la Resolución, la procedencia señala que sólo podría emplearse cuando resulte adecuado en una determinada situación concreta para garantizar y asegurar la convivencia ciudadana y para la prevención de faltas, contravenciones, delitos e infracciones relacionadas con la seguridad pública.

En la práctica, como se aborda más adelante en este trabajo, se observa que la implementación de este sistema de vigilancia y control dentro de CABA ha puesto en contradicción los dos

[63] El principio de proporcionalidad establece el procedimiento correcto tanto a nivel conceptual como normativo que un tribunal debe utilizar para aplicar e interpretar la normativa sobre los derechos fundamentales establecidos en la Constitución.
El principio de razonabilidad se contempla en el artículo Nº28 de la Constitución argentina al sostener que *"los principios, garantías y derechos reconocidos en los anteriores artículos no podrán ser alterados por las leyes que reglamentan su ejercicio".* Sin embargo, en la jurisprudencia argentina este principio nunca fue definido de manera precisa y se lo ha considerado como *"un principio flexible".*
Por lo tanto, en Argentina el principio de razonabilidad es entendido como un control que va más allá de la simple verificación de la presencia de la norma al sistema judicial.
Véase: http://www.derecho.uba.ar/revistas-digitales/index.php/revista-electronica-gioja/article/download/65/47 y http://revistaargumentos.justiciacordoba.gob.ar/index.php/primera/article/download/13/8/#:~:text=El%20art%C3%ADculo%2028%20de%20la,leyes%20que%20reglamenten%20su%20ejercicio%E2%80%9D.

principios de la Resolución 398/19 mencionados, ya que, como se ha visto, la aplicación del reconocimiento facial no está sujeta a una disposición legal o judicial específica, sino que toda la ciudadanía puede ser una posible víctima de este sistema de vigilancia y control, el cual se aplica permanente e indiscriminadamente sobre la población exista o no argumentos para su empleo. Esta Resolución establece también que la utilización del sistema de reconocimiento facial estará sujeta a la utilización de las bases de datos del CONARC la cual fue creada mediante el decreto penal Nº346/09. Al respecto, el Ministerio de Justicia y Derechos Humanos de la Nación publica diariamente por Internet y con formato abierto el listado de personas buscadas con órdenes de detención emitidas por autoridades judiciales del ámbito federal, nacional y provincial y de CABA[63]. Sin embargo, a lo largo de esta tesina se demuestra que esta disposición no siempre es llevada a la práctica y que las bases de datos en las que se sustenta el funcionamiento del reconocimiento facial se encuentran desactualizadas como se puede corroborar en los casos analizados.

De acuerdo con el Ministerio de Justicia y Derechos Humanos de la Ciudad, el uso indebido, irregular e ilícito del sistema de reconocimiento facial por parte del personal policial o civil de la fuerza se encuentra sujeto al régimen disciplinario ordinario previsto en la Ley Nº5688 y su reglamentación (Decreto 53/17) y en la Ley Nº471 de relaciones laborales en el ámbito del gobierno de la Ciudad de Buenos Aires y sus normas reglamentarias. En pocas palabras esto significa que, de acuerdo con la Ley Nº471, Artículo 52, los trabajadores de la CABA, entre los que se encuentran los integrantes de la policía de la Ciudad, pueden ser sometidos a diferentes tipos de sanciones disciplinarias como apercibimiento, suspensión por 30 días, cesantía o exoneración, las cuales serán aplicadas sin perjuicio de las responsabilidades administrativas, civiles y penales establecidas por las leyes.

5.1 Legislaciones que complementan y componen el sistema de videovigilancia en CABA

Además de la Resolución mencionada en el subapartado anterior, cabe destacar que el sistema de videovigilancia en CABA se complementa por la Ley Nº2602 la cual, sancionada en el año 2008 y reglamentada por el Decreto parcial 46/2008, establece principios generales para la utilización del sistema de videocámaras. En su artículo Nº2 se prevé que el sistema de videovigilancia de la Ciudad opere según

> *"La utilización de videocámaras está regida por el principio de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas e*

infracciones relacionadas con la seguridad pública. La intervención mínima exige la ponderación en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de conformidad con los principios consagrados en nuestra Constitución Nacional y de la Ciudad Autónoma de Buenos Aires".

La ley establece en su artículo N°14 garantías para el correcto funcionamiento del sistema de videovigilancia en el espacio público de CABA:

a. La existencia de videocámaras, así como la autoridad responsable de su aplicación, debe informarse mediante un cartel indicativo de manera clara y permanente, excepto orden contraria por parte de autoridad judicial.
b. Toda persona interesada podrá ejercer, ante autoridad judicial competente, los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura, acreditando los extremos alegados.
c. La autoridad de aplicación deberá publicar en la página web del Gobierno de la Ciudad de Buenos Aires los puntos en los cuales se instalen videocámaras.

Cabe destacar que esta ley también se encuentra complementada por su Decreto Reglamentario 716/2009, el cual fue asimismo modificado posteriormente por el Decreto 119/09 GCABA.
Por otro lado, el sistema de videovigilancia de CABA cuenta a su vez con la Ley N°3130 y una serie de Resoluciones: 410/MJYSGC, 10/MJYSGC/11, 156/PMCABA/12 y 157/pmcaba/12 generadas por el Ministerio de Seguridad y Justicia de CABA, autoridad de aplicación de estos sistemas de vigilancia y control social.
En el siguiente cuadro se resumen las regulaciones complementarias.

Cuadro Nº3: Legislación complementaria sobre el sistema de videovigilancia en CABA

Decreto Reglamentario716/2009 dirigido a la ley N°2602 en su considerando 6 establece en el Artículo Nº4	*"El poder ejecutivo no podrá utilizar las videocámaras instaladas en lugares públicos para captar imágenes del interior de las propiedades privadas excepto cuando se cuente con autorización judicial expresa. Es evidente que la norma tiende a preservar la privacidad e intimidad de las personas, por ello, a efectos de preservar sus postulados, resulta conveniente establecer que para dar cumplimiento a una demanda judicial sólo podrán utilizarse las videocámaras que se encuentren instaladas con anterioridad a la notificación de la medida judicial en el espacio público adyacente".*

Ley Nº3130 formulada debido a la constitución de un centro único de comando y control (CUCC) encargado de recibir en tiempo real los avisos de emergencia que permitiesen la detección de delitos e ilícitos en la vía pública de CABA.	***El Artículo N°2*** decreta que *"la reglamentación establece un protocolo de intervención ante la emergencia que deberá respetar los límites que establece la ley Nº2602 para la prevención de cualquier afectación a la intimidad de las personas".* ***El Artículo N°6*** afirma que *"el funcionario público o agente responsable que en cualquier forma vulnere los principios y procedimientos en materia de protección a la intimidad de las personas establecidos en la presente norma y su reglamentación, así como en la ley Nº2602 es considerado falta grave, sin perjuicio de las responsabilidades civiles y penales que pudieran corresponderle".*
Resolución 410/MJYSBC/10 remite a los considerandos de la ley N°3130.	Se refiere a la responsabilidad de los operadores de cámaras de videovigilancia y establece que el acceso a la ley de información derivada de las grabaciones realizadas por el sistema de monitoreo es restrictivo a los funcionarios determinados para acceder a ella.
Resolución 10/MJYSGC/11	Aprueba el manual de procedimiento del centro de monitoreo urbano de la ya desaparecida Policía Metropolitana, sin embargo, el público no logró acceder al contenido del manual La defensoría del pueblo de la CABA solicitó un informe sobre las características de las cámaras de videovigilancia, los sitios instalados y una copia del manual de procedimiento que utilizaba la fuerza para el manejo de los dispositivos de vigilancia. La respuesta a la petición por parte de la policía fue escasa e insuficiente afirmando que las cámaras se encontraban señalizadas, lo que contribuye a aumentar el marco de opacidad y secretismo en el que opera el sistema de vigilancia y control en la Ciudad.
Resolución Nº314 /MJYSGC/11	***Considerando Nº4****: "La Constitución de la CABA refiere en varias de sus disposiciones al derecho de acceso a la información y a la libertad de expresión y de prensa"* lo que se refleja en el Artículo 12 inciso 2, 42, 43, 47 y 105. ***Considerando N°5***: Sostiene que el Artículo Nº2 de la Ley de Servicios de Comunicación Audiovisual Nº26.522 establece que *"la actividad realizada por los servicios de comunicación audiovisual se considera de interés público y de carácter fundamental para el desarrollo sociocultural de la población por el que se exterioriza el derecho humano inalienable de expresar, recibir difusión e investigar informaciones, ideas y opiniones".* ***Considerando N°10***: Establece "*la posibilidad de que los medios de difusión cuenten con el material obtenido a través de cámaras del centro de monitoreo urbano, satisfaciendo las*

	demandas contenidas en las citadas normas de la Constitución de la CABA y de la Ley Nº26.522 y N°104".
Resolución N°157/PMCABA/12	Establece "*la creación de un registro de cámaras de video vigilancia privadas y de una base de datos de cámaras de vigilancia privadas, cuya finalidad es la unidad de información recibida con las cámaras públicas. Complementa a la resolución 156 al crear un registro de cámaras del poder ejecutivo".*
Ley Nº2602	Regula el funcionamiento del sistema de videovigilancia en CABA y establece que el uso de nuevas tecnologías deberá *"buscar una intervención mínima sobre la privacidad de la población moderada por los principios de razonabilidad y proporcionalidad".* Señala la prevención de las afectaciones sobre la privacidad de la ciudadanía y acota a lo indispensable de la discrecionalidad de los funcionarios encargados de esta tecnología.

Fuente: Elaboración propia en base al texto de las leyes

Es posible apreciar cómo este conjunto de reglamentaciones, leyes y decretos mencionados cumple el objetivo de asegurar que el funcionamiento del sistema de videovigilancia y reconocimiento facial que opera en CABA sea utilizado como prevención y combate frente a los riesgos que suceden en las sociedades. Decretos complementarios al funcionamiento del sistema de videovigilancia como el 716/2009 o la Ley Nº3130 establecen que las tecnologías de control y vigilancia deben operar sin causar perjuicio a la privacidad e intimidad de la ciudadanía.

El artículo N°6 de la Ley Nº3130, así como la Resolución 410/ MJYSBC/ 10 señalan la responsabilidad y el castigo para el personal de las fuerzas de seguridad que opere el sistema de videovigilancia y cuyo accionar resulte en una violación a la privacidad e intimidad de la población. Por otro lado, cabe mencionar el Artículo N°14 de la Ley Nº2602 que acuerda que las cámaras de videovigilancia deben estar claramente identificadas en el espacio público y en las páginas webs oficiales del gobierno de la Ciudad.

Se considera, entonces, que la sanción y aplicación de estas leyes, decretos y resoluciones han sido formuladas con el objetivo de que exista un control y una regulación sobre el funcionamiento de las nuevas tecnologías, las cuales, como se afirma en la Ley Nº2.602, debe operar con una naturaleza de intervención mínima como sostiene la Resolución 398/19, conforme a los principios de proporcionalidad y razonabilidad a fin de garantizar el derecho a la ciudadanía.

Indudablemente, estas regulaciones buscan darle un "marco de transparencia" al accionar de las fuerzas de seguridad buscando asegurar que la implementación de las tecnologías de control

se establezca “por el propio bien” como se explica en el capítulo 3 al exponer acerca de la política del miedo.

Ahora, como se presentará en el siguiente capítulo, la puesta en práctica del sistema de videovigilancia y reconocimiento facial en CABA no está exento de falencias, errores y puntos oscuros en su funcionamiento, tal como se demuestra en el análisis de los casos elegidos de Rachel Holway y Guillermo Federico Ibarrola. La opacidad en el funcionamiento de las fuerzas de seguridad se refleja también en la Resolución 10/MJYSGC/11 que aprueba el procedimiento del Centro del Monitoreo Urbano.

Sin embargo, las respuestas a las solicitudes[64] por parte de la Defensoría del Pueblo de la Ciudad de Buenos Aires para acceder al conocimiento de las características técnicas de las cámaras, su ubicación, así como al manual de procedimiento de su manejo han sido insuficientes por parte de las fuerzas de seguridad.

6. La policía nos vigila y nosotros, ¿vigilamos a la policía? Participación ciudadana en el control de las fuerzas de seguridad

Es importante remarcar que la instalación de los sistemas de videovigilancia implementados en la sociedad argentina para control y vigilancia de la población debe priorizar la importancia del acceso a la información ciudadana.

Para Merino (1996), la participación de la ciudadanía significa la intervención de los miembros de la sociedad en los centros de gobierno para lograr la toma de decisiones de la vida colectiva y la administración de los recursos, con el propósito de que la población poco a poco forme parte de las decisiones tomadas por los gobernantes y pueda influir en las políticas y decisiones públicas. Para alcanzar esta meta es necesario institucionalizar estos mecanismos de participación, procesos y organismos mediante una normativa legal.

Guillen, Sáenz, Badii y Castillo (2009) plantean que la participación ciudadana implica una búsqueda de la ciudadanía para alcanzar una mejor calidad de vida. Esta participación puede ser considerada como un “despertar” de una sociedad que se encontraba dormida y ahora busca involucrarse en el accionar y en las políticas gubernamentales controlando la intervención estatal e intentando proteger sus derechos e intereses. El rol de la ciudadanía de involucrarse en el control ejercido por parte Estado es fundamental para mejorar la calidad democrática de la sociedad.

[64] Véase http://www.defensoria.org.ar/noticias/irregularidades-en-el-sistema-de-reconocimiento-facial-la-defensoria-presento-un-informe/
https://www.lavozdetandil.com.ar/2019/07/29/defensoria-del-pueblo-insiste-en-pedido-de-informes-sobre-camaras-de-seguridad

Al hablar de posibles formas de participación ciudadana para ejercer un control civil sobre la acción de las fuerzas de seguridad a nivel nacional y puntualmente en CABA, se debe nuevamente mencionar el rol que desempeñan las organizaciones no gubernamentales (ONGs) cuya tarea es indagar e investigar sobre las políticas y tecnologías que aplican dichas fuerzas en cuanto a la vigilancia en el ámbito público, colaborar en alertar al conjunto de la población y denunciar, cuando es necesario, al observar la incorporación de tecnologías, como el reconocimiento facial que trae aparejado riesgos para la privacidad de la ciudadanía.

Como hemos visto en este capítulo, existen varias ONGs que han demostrado un rol importante a la hora de clarificar a la sociedad el funcionamiento de las nuevas políticas y tecnologías aplicadas por las fuerzas de seguridad en CABA.

Por lo tanto, se puede considerar fundamental el rol de las ONGs que investigan y denuncian, cuando así lo amerita, el ejercicio de las fuerzas de seguridad haciendo pública la denuncia y arrojando "un poco de luz" al funcionamiento de las fuerzas de seguridad cuyo accionar a menudo se da en un marco de secretismo y opacidad.

Por ello, se puede concluir que las ONGs también operan a favor al intentar contribuir con preservar la democracia y la libertad dentro de las sociedades contemporáneas. Es por ello por lo que no se debe omitir que el rol desempeñado por las organizaciones sin fines de lucro puede verse afectado debido a la opacidad en los manejos que los Estados realizan tanto de sus tecnologías de control y vigilancia como de las modalidades de vigilancia desplegadas por las fuerzas de seguridad, lo que implica que su rol en defensa de los derechos de la ciudadanía pueda verse seriamente dificultado.

Conclusión

Este capítulo se dirigió a puntualizar el funcionamiento del sistema de videovigilancia y reconocimiento facial instalado en CABA en 2019 focalizando el proceso de despliegue e instrumentación en su espacio público. Para ello, se enfatizó sobre el rol desempeñado por la policía de la Ciudad como fuerza de seguridad del Estado encargada de operar el sistema de reconocimiento facial en la Ciudad Autónoma de Buenos Aires.

Esto se vincula con el capítulo dos de esta tesina, el cual aborda el protagonismo que las fuerzas de seguridad cumplen en el marco de las sociedades de control y el consecuente proceso de tecnologización que experimentan, con especial énfasis sobre el rol de la Policía de la Ciudad, la principal fuerza de seguridad que interviene en este territorio.

Asimismo, se analizó el fenómeno de los Centros de Monitoreo Urbano (CMU), los cuales operan, por un lado, el funcionamiento de las cámaras de videovigilancia y reconocimiento

facial desplegado en el espacio público de la Ciudad, y por otro, regulan las disposiciones técnicas y tecnológicas con las que cuentan los Centros de Monitoreo Urbano y sus características que, de acuerdo al discurso del gobierno porteño, garantizan el correcto funcionamiento del sistema de videovigilancia y reconocimiento facial, aunque, conforme a la investigación llevada a cabo estas afirmaciones pueden ser puestas en discusión.

Para una mejor comprensión de las amenazas que implica para la privacidad e intimidad de la población el despliegue de estas tecnologías de control y vigilancia, también ha sido necesario describir las características técnicas del software de reconocimiento facial implementado por el gobierno de la Ciudad Autónoma de Buenos Aires. Si bien en el capítulo dos se trataron las características técnicas/tecnológicas de las nuevas herramientas utilizadas por las fuerzas de seguridad en el marco de las sociedades de control en general, el presente capítulo se centró en el apartado técnico puntual del software de reconocimiento facial ULTRAIP, adquirido y puesto en operación por el gobierno porteño de Horacio Rodríguez Larreta en el 2019. Este capítulo retoma, a su vez, el debate en torno a la conveniencia o no de su implementación en el espacio público.

Existen discursos a favor y en contra. Los discursos a favor del reconocimiento facial son realizados principalmente por actores pertenecientes a la esfera gubernamental como son los medios de comunicación y empresas licitadoras de esta tecnología, los cuales pueden responder a una amplia gama de intereses, mientras que, las voces opositoras provienen del sector académico y de las ONGs, cuyo estudio está centrado en la problemática de vigilancia y privacidad.

Al enfocarse en la realidad de CABA, este capítulo se complementa con el capítulo cuatro donde se analizan minuciosamente las legislaciones nacionales sobre la vigilancia y, puntualmente, las establecidas en 2019 en CABA, con el objetivo de proteger el derecho a la privacidad e intimidad de la ciudadanía.

El análisis de las legislaciones presentadas en ambos capítulos será de vital utilidad al momento de emplearlo en el abordaje de los casos tomados en este trabajo de Rachel Holway y Guillermo Federico Ibarrola ya que se podrá observar, analizar y verificar si la presente legislación es respetada por las nuevas herramientas y modalidades de vigilancia o dejada de lado.

Finalmente, y a modo de cierre, el capítulo retoma la problemática de la policía como fuerza de seguridad del Estado y operadora de las tecnologías de control y vigilancia masiva, la cual, en múltiples ocasiones acciona inmersa en un marco de opacidad y secretismo alejada del control civil. Por lo tanto, es posible empezar a vislumbrar algunas alternativas para subsanar esta situación. Una de ellas podría ser la intervención de las Juntas Comunales o de las ONGs

ejerciendo la función de monitoreo sobre la implementación de las tecnologías de vigilancia y su avance contra los derechos de la población como lo vienen realizando distintas ONGs, como es el caso de las ya nombradas “ADC” o Fundación “Vía Libre”.

Capítulo 6: Análisis de casos

Introducción

En el presente capítulo se analizan dos casos puntuales donde el sistema de reconocimiento facial instalado en CABA durante el año 2019 ha mostrado falencias.

Estos casos involucraron a dos ciudadanos argentinos: Rachel Holway y Guillermo Federico Ibarrola, quienes fueron identificados y detenidos por las fuerzas de seguridad a través del software de reconocimiento facial que opera en el ámbito público de la Ciudad.

Sin embargo, en ambas detenciones se demostró que el error habría sido desencadenado por la desactualización en la base de datos del Poder Judicial y de las fuerzas de seguridad. Estos casos puntuales tuvieron una importante cobertura mediática en medios nacionales e internacionales, los cuales colocaron en el centro del debate público los riesgos que conlleva la privacidad con la implementación de las tecnologías de control y vigilancia.

Ambos casos se estudian a la luz de las leyes nacionales y de la Ciudad Autónoma de Buenos Aires que regulan el sistema de videovigilancia y reconocimiento facial demostrando la tensión que se genera entre vigilancia y privacidad en el espacio público**.** De esta manera, se aborda cómo la aplicación de las modalidades de vigilancia ha puesto en tirantez o incluso vulnerado la normativa legal nacional como la de CABA que ampara y protege los derechos inalienables de la ciudadanía como es el derecho a la privacidad. Asimismo, se realiza un análisis en torno a la cobertura periodística que han recibido los casos seleccionados, así como el rol que desempeñan los medios de comunicación en transmitir la información acerca de la aplicación de las tecnologías de vigilancia y control en el espacio público.

Como se ha plasmado en capítulos anteriores, la implementación de tecnologías de control y vigilancia sobre las sociedades contemporáneas no responde a un fenómeno aislado dado que; es posible identificar nuevas formas de control realizadas por las fuerzas de seguridad del Estado en regiones diversas y distantes como la República Popular de China, los Estados Unidos y ahora también Argentina.

En este sentido, el siglo XXI ha generado fuertes cambios dentro del paradigma de seguridad a nivel global impulsando a que las naciones concreten una política que Alcántara (2008) ha denominado “guerra preventiva” mediante la cual se realiza la implementación de una vigilancia generalizada sobre las poblaciones tratando de evitar la aparición de amenazas que

surgen desde el interior de las propias sociedades como el terrorismo y la criminalidad. Como se ha visto, bajo la premisa de proteger a la población de estos riesgos, el nuevo paradigma de seguridad conlleva la adopción de nuevas formas de control ultrarrápidas en el espacio público (Deleuze, 1990), las cuales han sido producidas por los avances técnico/tecnológicos que permiten realizar una vigilancia permanente e invisibilizada sobre la población, que, en su conjunto, se convierte en objeto de sospecha y, por consiguiente sometida a un control permanente aun cuando no existan causas atribuibles para implementar estas medidas. Este escenario conduce a que se produzca lo que afirma Gendler (2017) que todos los integrantes de la ciudadanía pasan a convertirse en potenciales sospechosos de ser criminales para las fuerzas de seguridad. La aplicación masiva de tecnologías de vigilancia y control en el espacio público contribuye a consolidar la aplicación de la sociedad de control como modelo dominante en el mundo contemporáneo.

1.Ponerle nombre y apellido al error: El caso de análisis de Rachel Holway en la Ciudad Autónoma de Buenos Aires

1.1 Descripción del caso

Rachel Holway fue detenida el 11 de julio de 2019 en la estación Retiro de la línea C de subtes luego de que el sistema de reconocimiento facial la identificara como prófuga porque su rostro y número de documento aparecía en la base de datos de Consulta Nacional de Rebeldía y Capturas (CONARC). Este caso presentó una amplia cobertura por los medios de comunicación potenciada, por supuesto, por el hecho de que la ciudadana era conocida mediáticamente por ser la fundadora de la ONG "Alerta Vida" que impulsa investigaciones contra la pedofilia y las redes de trata en Argentina.

Cuando se conoció su detención, posibilitada por el software de reconocimiento facial, algunos medios de comunicación, como País 24, barajaron la posibilidad de que la causa de su detención pudiese estar vinculada a una denuncia realizada en el 2018 donde se implicaba al entonces presidente Mauricio Macri en causas de explotación sexual[65]

[65] *"La gente votó a un presidente con causas de explotación sexual, da vergüenza ajena. La gente no sabe quién es*" afirmó Holway al medio País 24.

Véase http://www.pais24.com/index.php?go=n349691

Frente a este contexto, Holway considera estar siendo perseguida por las fuerzas de seguridad del Estado como consecuencia de su denuncia al exmandatario *"dicen que el Ministerio de Seguridad manda mi foto para que me detengan"* remarcó en una entrevista para País 24.[66]

Cabe aclarar que ella poseía una causa judicial iniciada por su expareja por el delito de falsificación de documentos, pero sobreseída en el 2004 por el Juez Eduardo Moumdjian, a cargo del Juzgado de Instrucción Nº7, siendo el fallo confirmado por la cámara en 2005. Sin embargo, 14 años después del cierre de la causa seguía figurando en el sistema como prófuga de la justicia ya que su información y datos personales aún se encontraban en las bases de datos del CONARC.

En este caso, desde el Ministerio de Seguridad de CABA se responsabilizó por el error al Juzgado Nº7, afirmando que el sistema de reconocimiento facial sólo tiene un margen de error del 4% y se provoca cuando el Poder Judicial no actualiza la información de las bases de datos en relación con los juicios.

Al observar el incorrecto arresto policial de la ciudadana se puede percibir una violación a su privacidad e intimidad al ser identificada y detenida por el sistema de vigilancia en uno de los puntos más neurálgicos del espacio público de la ciudad.[67]

El caso de Holway pone de manifiesto una de las grandes falencias sobre el funcionamiento del sistema de reconocimiento facial que detalla la Asociación por los Derechos Civiles: la desactualización y renovación de la información de las grandes bases de datos como el CONARC sobre el cual opera el sistema de reconocimiento facial dentro de CABA. A pesar de que el Ministerio de Seguridad de la Ciudad remarcó que su detención se produjo por una desactualización de la base de datos, ella recela de esta afirmación y sostiene que "*Esto no me cierra: durante todos estos años salí y entré al país, hice Migraciones, presenté mi documento y nunca tuve problemas"*[68] reiterando su postura de que ha sido víctima de una persecución por parte de las fuerzas de seguridad.

Este caso nos remite a la tensión generada respecto de la tercera etapa de la privacidad analizada en capítulos anteriores, donde se sostiene que la idea de privacidad pasa a ser vista como el derecho a que toda información sobre la vida privada de los sujetos en poder del Estado o de

[66] Véase http://www.pais24.com/index.php?go=n349691

[67] Véase: https://www.pagina12.com.ar/223372-camaras-de-reconocimiento-facial-larreta-prometio-10-000-mas

[68] Véase: http://www.pais24.com/index.php?go=n349691

grandes conglomerados comerciales no sea empleada en perjuicio de los titulares de dicha información.

1.2 Tensión con la normativa vigente

1.2.1 Tensión con la regulación nacional

Al analizar este caso, salta a la vista que el sistema de videovigilancia y reconocimiento facial de CABA está violando la Ley Nº25.326 de Protección de Datos Personales. Si bien esta ley establece múltiples criterios para el manejo de los datos privados de la ciudadanía, en este caso particular se observa la violación de varios de sus artículos.

En primer lugar, el Nº4 Inciso 1 que establece *"los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que lo hubieran obtenido".* En segundo lugar, su Inciso 4 que establece *"los datos deben ser exactos y actualizarse en el caso de que ello fuera necesario".* Y finalmente, el Inciso 5 afirma que *"los datos total o parcialmente inexactos o que sean incompletos deben ser suprimidos o sustituidos o en su caso completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate".*

Como se ha visto en el capítulo cuatro de esta tesina, esta ley establece que los datos personales de la población recolectados por las fuerzas de seguridad deben ser *congelados*[69] en el momento en que los motivos que originaron su almacenamiento ya no existan como tales.

Al analizar este caso también se observa la vulneración del Artículo N°16 que afirma que la ciudadanía tiene derecho a que su información personal almacenada en la base de datos sea actualizada y ratificada o incluso eliminada si así corresponde, pero no fue así con Holway.

Asimismo, se observa la tensión producida con respecto a lo establecido por el Artículo Nº52 del Nuevo Código Civil y Comercial, que estipula que las personas humanas *"lesionadas en su intimidad personal o familiar, honra o reputación, imagen o identidad pueden establecer el reclamo o prevención de los daños sufridos".*

La ciudadana no sólo fue detenida por las fuerzas policiales de la Ciudad equivocadamente en el espacio público y ante la vista de otros ciudadanos, sino que su caso recibió cobertura periodística por parte de medios locales y nacionales. Esta detención errónea y su consecuente exposición, sin duda, constituye un ataque que conlleva una lesión para su imagen.

En el caso Holway también se ha producido una tensión respecto a lo que está establecido en el Artículo Nº19 de la Constitución Nacional. Si bien la ciudadana había tenido una causa judicial, ésta había sido cerrada desde hacía más de una década, por lo que, toda acción que

[69] Véase nota al pie N°43.

realizara en el espacio público y no entrara en conflicto con lo estipulado por el artículo mencionado correspondería a su índole privada. Sin embargo, la desactualización de las bases de datos provoca que los sistemas de vigilancia y control generen una identificación de la persona y les permita a las fuerzas de seguridad conocer dónde está, con quién o qué está haciendo sin que exista una causa válida para aplicar esta vigilancia provocando una intrusión sobre su vida íntima y personal.

El caso también muestra una tensión entre privacidad y vigilancia ya que el Artículo Nº3 de la Disposición 10/2015 de la DNPDP establece *"la información que se recabe debe ser adecuada, pertinente y no excesiva en relación a la finalidad para la que se hubiera obtenido".*

Este artículo establece que se buscará evitar especialmente cualquier afectación del derecho a la privacidad de la ciudadanía. A pesar de ello se observa que las fuerzas policiales no respetaron lo establecido por la legislación dado el gran despliegue de medios técnicos y humanos utilizados para combatir un supuesto delito, que no sólo no representaba una amenaza inmediata para la sociedad, sino que, al mismo tiempo, su causa judicial ya había concluido.

En este punto, se debe reflexionar sobre lo dispuesto por la Resolución 238/2012 del Ministerio de Seguridad. Por un lado, el Artículo Nº3 establece que las imágenes captadas por el sistema de videovigilancia *"tendrán como finalidad exclusiva contribuir a la prevención y conjuración de ilícitos brindando un aporte probatorio relevante para la investigación judicial*".

Cabe preguntar entonces, ¿qué prueba relevante constituía la identificación de Holway a través del reconocimiento facial para la supuesta investigación de una causa judicial ya cerrada y el delito por el cual se la imputaba no suponía una amenaza grave para la sociedad?

Es necesario aclarar que el Artículo Nº2 establece claramente que todo el funcionamiento del sistema de videovigilancia debe operar *"debiendo garantizar un funcionamiento sustentado en principios de legalidad y respeto de la privacidad de las personas"*, lo cual no fue cumplido.

1.2.2 Tensión con la regulación de la Ciudad

Se puede considerar que la detención de Holway incumple con lo dispuesto por el artículo Nº2 de la Ley Nº2.602 y la Resolución 398/MJYSGC/19 donde se establece que el funcionamiento integral del sistema de videovigilancia que opera en CABA debe actuar respetando los principios de proporcionalidad y razonabilidad de acuerdo con el ilícito que busca prevenir/combatir. Ambas regulaciones sostienen que la operación de estas tecnologías de vigilancia y control se dará con la mínima intervención posible sobre la privacidad de la población y siempre que exista una situación concreta de delito, ya que el sistema tiene el objetivo de asegurar la convivencia ciudadana.

El caso permite observar que el accionar de las fuerzas de seguridad ha violado el Artículo Nº1 de la Ley Nº2.602 donde se dicta *"la utilización por parte del poder ejecutivo de videocámaras para grabar imágenes en lugares públicos y su posterior tratamiento estableciendo específicamente el régimen de garantías de los derechos fundamentales públicas de los ciudadanos*" afirmando que estos derechos deben ser respetados en forma ineludible tanto en el proceso de grabación como en el uso de las imágenes obtenidas por el sistema.

El accionar de las fuerzas de seguridad, en este caso específico, entra en rigidez con lo establecido por diversos artículos de la Ley Nº5.688. Por ejemplo, el Artículo Nº75 en su inciso 7 determina que la innovación e incorporación de nuevas tecnologías busca mejorar la gestión institucional, la transparencia, la previsión de conductas delictivas y la investigación de nuevas formas de criminalidad. Sin embargo, en este caso puntual, se ve claramente que la ciudadana no estaba en proceso de cometer ningún delito que pusiera en riesgo a terceros o a sus bienes.

El hecho de que el inciso establezca el objetivo de transparentar y mejorar la gestión institucional de las fuerzas policiales en realidad no se cumple con Holway ya que refleja lo contrario. Si bien en el pasado la ciudadana había incurrido en una causa judicial, cerrada al momento de su detención, la base de datos de las fuerzas policiales y judiciales no poseían una actualización de ello. Este hecho remite a una falta de transparencia del Poder Judicial como de las fuerzas policiales lo que impone un riesgo para la privacidad e intimidad de la población.

Por otra parte, el Artículo Nº475 remarca que tanto la captación como el uso de las imágenes obtenidas por el sistema de videovigilancia deben llevarse a cabo respetando los derechos fundamentales y libertades públicas de la ciudadanía. Asimismo, el Artículo Nº476 de la Ley Nº5.688 sostiene al igual que la Ley Nº2.602 que el accionar del sistema de videovigilancia debe operar guiado bajo los principios de proporcionalidad y razonabilidad en su procedencia e intervención sobre el hecho.

El caso analizado amerita observar también la tirantez que se produce entre la aplicación de las nuevas tecnologías de control y vigilancia y el derecho a la privacidad de la ciudadana. Así, en el Artículo Nº2 de la Ley Nº3.130 se dicta que el funcionamiento del sistema de videovigilancia y su reglamentación impone *"respetar los límites que establece la Ley Nº2.602 para la prevención de cualquier afectación para la intimidad de las personas, y que acotará a lo indispensable la discrecionalidad del operador".*

Cabe destacar también el Decreto Reglamentario 716/2009 en su Artículo Nº1 el cual aprueba la reglamentación de la Ley Nº2.602 que establece y regula el funcionamiento del sistema de videovigilancia en CABA y cuyo texto establece respetar el régimen de garantías de derechos fundamentales y libertades públicas de los ciudadanos. Este Decreto se sanciona buscando

reglamentar lo establecido por esta ley que a nivel teórico parece priorizar el respeto a la ciudadanía y a sus derechos pero que, en la práctica, como se evidenció en este caso, produce una fuerte violación hacia estas disposiciones por parte del accionar de las nuevas modalidades y tecnologías de vigilancia.

Se observa así, que a nivel nacional como en la normativa de CABA existen legislaciones que pretenden garantizar el funcionamiento del sistema de videovigilancia y reconocimiento facial respetando los principios de razonabilidad y proporcionalidad priorizando el respeto hacia los derechos esenciales de la población incluyendo el derecho a la privacidad. Pero, lo ocurrido con Holway demuestra que, en la práctica, dichas disposiciones y regulaciones no son priorizadas frente al despliegue de las nuevas tecnologías de control y vigilancia en el espacio público de la Ciudad.

1.2.3 Resumen de las tensiones

Las disposiciones de las regulaciones antes mencionadas invitan a plantear que la detención de Holway se produce en un contexto que no constituía una situación de riesgo ni para terceros ni para sí misma. La ciudadana tampoco había cometido una falta o infracción relacionada con la seguridad pública (como estipula el artículo) para la utilización del sistema de videovigilancia. Sería interesante debatir si el uso del reconocimiento facial para su identificación constituye una medida proporcional a su caso, ya que en el 2004 no había sido acusada de un delito violento sino de *"falsificación de documentación"*.

Sin embargo, no parece existir una clasificación en torno a los tipos de delitos que ameritan ser combatidos mediante el sistema de reconocimiento facial, sino que todos los ciudadanos son susceptibles de ser identificados por el sistema, aun cuando la información presente en las bases de datos de las fuerzas de seguridad se encuentre desactualizada o sea errónea.

Cuadro Nº4: Tensiones de la legislación con el caso Holway

Regulaciones	**Tensiones**
Regulaciones Nacionales	
Constitución Nacional	Tensión con el articulo 19
Constitución Nacional	Artículo 43° No entra en tensión
Ley de Protección de Datos Personales Nº25326	Tensión respecto del objetivo, del Artículo 4 incisos 4° y 5°.

	Artículo 16° inciso 1°
Nuevo Código Civil y Comercial	Tensión con el Artículo 52
Resolución 238/2012 Ministerio de Seguridad	Tensión con el Artículo 2° y 3°
Disposición 10/2015 DNPDP	Tensión con el Artículo 3° .
Regulaciones Ciudad Autónoma de Buenos Aires.	
Resolución 398/19 MJYSGC	Tensión con el hecho y lo dispuesto por la resolución.
Ley N°2602	Tensión con el Artículo 1° y 2°
Ley N°5688	Tensión con el Artículo 75° inciso 7 Tensión con el Artículo 475° y 476°
Decreto Reglamentario 716/2009	No entra en tensión
Ley N°3130	Tensión con el Artículo Nº2°
Resolución 10/MJYSGC/11	Opacidad al aprobar el procedimiento del CMU
Resolución 314/MJYSGC/10	No entra en tensión
Decreto 716/2009	Entra en tensión al reglamentar la Ley 2602

Fuente: Elaboración propia en base a las leyes.

El análisis realizado del caso de Rachel Holway demostró que la puesta en funcionamiento de las nuevas tecnologías de vigilancia masiva como la operación de nuevas modalidades de vigilancia suponen la existencia de una tensión respecto a las legislaciones nacionales y de CABA destinadas no sólo a regular la operación de estos sistemas en el espacio público sino también a resguardar el derecho a la privacidad e intimidad de la ciudadanía.

En este caso puntual se evidencia que algunas normativas nacionales como la Ley de Protección de Datos Personales Nº25.326, la Resolución 238/2012 del Ministerio de Seguridad de la Nación junto a otras específicas de CABA como la Ley Nº2.602 y la Ley Nº5.688 han entrado en tensión de manera más comprometida con la incorporación del reconocimiento

facial en el ámbito público respecto a su función de preservar la privacidad de la población. Otras legislaciones, como la Disposición 10/2015 DNDDP, la Ley Nº3.130 y la Resolución 398/19 del MJYSGC de CABA también han entrado en tensión con respecto a la privacidad, pero de forma menos severa que las normativas mencionadas anteriormente.

Por último, el Artículo Nº43 de la Constitución Nacional, el Decreto Reglamentario 716/2009 y la Resolución 314/10 de MJYSGC de la CABA no entran en tensión con respecto a la privacidad de la ciudadanía en el caso contemplado.

1.3 Análisis Cobertura Mediática

El caso de Rachel Holway recibió una amplia cobertura mediática en medios nacionales[70] e internacionales. Al respecto, el relevamiento de la cobertura periodística ha arrojado un total de nueve medios de comunicación: ocho nacionales y uno internacional: el canal ruso RT.

RT ha sido el único medio internacional que ha brindado cobertura periodística al caso realizando una fuerte crítica a la implementación del reconocimiento facial en CABA al afirmar que, desde su implementación se han detenido 1227 personas de las cuales sólo 256 corresponden a criminales buscados por las fuerzas de seguridad lo que en la práctica daría una efectividad de tan solo el 20%. Destaca, a su vez, el gran nivel de fallas del sistema de vigilancia. El canal ruso despliega un posicionamiento generalmente contrario a las políticas aplicadas por el gobierno de "Cambiemos" y retoma las declaraciones de María del Carmen Verdu, abogada y titular, Coordinadora contra la Represión Policial e Institucional (CORREPI), quien, además, aborda el caso de Holway sosteniendo que el reconocimiento facial *"no es una herramienta para frenar el delito o encontrar prófugos porque, si para detener un criminal necesitas privar de la libertad a 1000 personas que no hicieron nada, estás cometiendo un daño mucho más grave".*[71]

Cabe destacar que el caso también ha recibido cobertura periodística de uno de los medios de comunicación más importantes de Argentina: el diario Clarín, afín al gobierno nacional del expresidente Mauricio Macri y al jefe de gobierno porteño Horacio Rodríguez Larreta. El caso, además, fue cubierto mediáticamente por Página 12, uno de los principales medios de la oposición del entonces gobierno de "Juntos por el Cambio".

[70] Véase https://www.youtube.com/watch?v=mi91K8SDGbk
http://www.pais24.com/index.php?go=n349691
https://argentinatoday.org/2019/08/03/argentina-victimas-del-reconocimiento-facial-estatal/

[71] Véase https://actualidad.rt.com/actualidad/322341-fallas-sistema-seguridad-reconocimiento-facial-argentina

Sin embargo, llama la atención la cobertura recibida de medios de comunicación más pequeños del interior de la provincia de Buenos Aires como "Tu Mercedes" o "De la Bahía" a pesar de estar alejados de CABA, mientras otros importantes medios del país más cercanos al oficialismo (Infobae, La Nación) u opositores (La Izquierda diario) no brindaron ninguna cobertura.

La forma de tratamiento que los casos han recibido por los medios depende en gran medida del posicionamiento editorial que posean en torno a la política de seguridad adoptadas por "Cambiemos" en CABA y el apoyo o rechazo que manifiesten hacia el accionar del Estado.

En este caso específico se observa que tanto los medios nacionales (opositores y oficialistas) como el internacional tuvieron una actitud crítica y de repudio hacia la detención de la ciudadana.

En algunos medios opositores, como Página 12, la crítica al sistema de videovigilancia de Larreta fue mucho más severa al catalogarlo como "*gran hermano porteño*", sistema de vigilancia *"orwelliano",* o incluso como "*panóptico Larretista".*[72]

La cobertura enfatizó que el error que provocó su detención estuvo originado en una falta de actualización de las bases de datos del Poder Judicial y en algunos casos se buscó eliminar la responsabilidad del Ministro de Seguridad de CABA, Diego Santilli como lo demuestra la cobertura del medio "Vía País" donde, en la nota publicada sobre el caso sostiene *"sabemos que la base de datos está sucia porque los magistrados no actualizan la información, pero desde que lanzamos el programa tenemos más cosas a favor que en contra".*[73]

Medios más afines al gobierno porteño, como Clarín[74] también ha mostrado un discurso crítico frente a las detenciones erróneas reconstruyendo el momento de la detención en primera persona y colocando al lector en el lugar del acusado para que se identifique con la situación. No debe omitirse que Clarín, en la misma cobertura periodística, menciona los "éxitos" que ha obtenido el sistema de reconocimiento facial al detener a los prófugos de la justicia algunos de ellos acusados de delitos graves como violaciones u homicidios.

Por otro lado, en la cobertura del medio Todo Noticias (TN) se observa que el caso de la incorrecta detención de Holway generó una fuerte crítica por parte del medio a pesar de responder a una línea editorial favorable al gobierno porteño de Horacio Rodríguez Larreta.

[72] Véase https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien
[73] Véase https://viapais.com.ar/buenos-aires/1136492-por-un-error-en-el-sistema-de-reconocimiento-facial-detuvieron-a-una-referente-de-la-lucha-contra-la-pedofilia/
[74] Véase https://www.clarin.com/policiales/identificaron-14-personas-dia-reconocimiento-facial-81-quedo-libre_0_O_WhA1FAf.html

Todo Noticias enfatiza el error en la detención de la ciudadana al incluir frases en formato "negrita" que destacan del resto del texto como *"el magistrado la sobreseyó en 2004" o "más de 14 años después la orden de captura seguía vigente",* enfatizando que, efectivamente, el error por una detención equivocada fue cometido por las fuerzas policiales.

El medio también reproduce la postura del Ministerio de Seguridad de CABA responsabilizando al Juzgado por no comunicar la resolución del caso a su debido tiempo *"ellos no comunicaron el sobreseimiento, estamos trabajando para que estas cosas no pasen más, tenemos un margen de error del 4%.*[75].

Como se mencionó anteriormente, medios de comunicación más pequeños y alejados de la Ciudad como el diario digital Tu Mercedes cubrió la noticia caracterizada por su brevedad señalando al sistema de reconocimiento facial operante como *"novedoso*", aunque, no necesariamente se mostró a favor de la implementación de esta tecnología considerándola como positiva, ya que destaca la presencia de falencias y así lo afirma en sus líneas *"lo cierto es que ni bien implementado ya comenzaron a sentirse los errores"*[76]

Por su parte, la cobertura del caso por parte del diario De la Bahía es más bien escasa y enfocada primordialmente en informar acerca de las características técnicas/tecnológicas del sistema de reconocimiento facial instalado en la Ciudad Autónoma de Buenos Aires.

Si bien el medio se pronuncia con críticas al sistema de vigilancia, la realiza con menos dureza que otros medios de comunicación , enfatizando en que los ciudadanos demorados deben *"permanecer junto a los efectivos hasta que se aclare su situación, lo que puede demorar varias horas ante la falta de respuestas por parte del juzgado"*[77] por lo que reconoce que gran parte de las falencias del sistema de reconocimiento facial está en el Poder Judicial y depende del manejo que éste realice de los datos personales de la población.

Cuadro Nº5: Cobertura mediática caso Rachel Holway

[75] Véase https://tn.com.ar/sociedad/sistema-de-reconocimiento-facial-retuvieron-por-error-una-referente-de-la-lucha-contra-la_977335

[76] Véase https://www.tumercedes.com/noticia/220989

[77]Véase https://www.delabahia.com.ar/aciertos-y-errores-del-nuevo-sistema-de-reconocimiento-facial-en-las-calles-de-buenos-aires/

Medio/ fecha	*Título de la nota*	*Resumen noticia*	*Principal problema enunciado*	*Tensión respecto a la privacidad*	*Referencia política del miedo*
Todo Noticias (TN) 10/7/2019	*"Sistema de reconocimiento facial: retuvieron por error a una referente de la lucha contra la explotación de menores".*	Reconstruye antecedente judicial y retomado su voz y la postura del Ministerio de Seguridad de CABA que responsabiliza de la detención a la desactualización de la base de datos del poder judicial.	Enfatiza la desactualización de las bases de datos del CONARC	Tensión indirecta con la privacidad por haber sido sobreseída de su causa judicial, pero seguía figurando en el CONARC.	Se retoman declaraciones del Ministerio de Seguridad de CABA *"Desde que se lanzó el programa de reconocimiento facial tenemos más cosas a favor que en contra"* y remarca que desde el 25/4al 2/7/19 el sistema detuvo a 1043 personas, 174 por delitos de homicidio o abuso sexual.
Vía País 11/7/2019	*"Por un error en el sistema de reconocimiento facial detuvieron a una referente de la lucha contra la pedofilia"*	Transmite sólo la postura de la ciudadana de forma breve.	Enfatiza la desactualización de las bases de datos del CONARC.	Remarca el cierre de la causa judicial de Holway en 2014 aunque en apariencia seguía vigente.	No se menciona
Tu Mercedes 12/7/2019	*"El nuevo reconocimiento facial de prófugos ya mostró los primeros errores"*	Breve abordaje del caso recuperando muy escasamente la voz de la ciudadana y sin dar lugar a la postura del Gobierno de la Ciudad. Analiza el funcionamiento del reconocimiento facial y sus características técnicas.	El medio presenta el problema como un sistema de vigilancia masivo.	No se menciona	No se menciona
País 24 13/7/2019	*"Detuvieron a una activista que acusó a Macri de explotación sexual".*	Fuerte énfasis en la posibilidad de que su detención se debiera a las denuncias hacia Mauricio Macri.	Se enfatiza la desactualización de las bases de datos del CONARC.	Referencia indirecta a la problemática de la invasión a la privacidad e intimidad de la ciudadanía.	No se menciona.

Clarín 22/7/2019	*"Identificaron a 14 personas por día con el reconocimiento facial, pero el 81% quedó libre"*	Aborda el caso recurriendo a otros similares. Critica el funcionamiento del sistema del reconocimiento facial y el manejo de las bases de datos.	Enfatiza la desactualización de las bases de datos del CONARC.	No hace referencia.	Menciona la utilización del reconocimiento facial para la identificación de los prófugos de la justicia, pero remarca que sólo el 18% queda detenido.
RT 27/7/2019	"Sólo *detiene a inocentes: Las polémicas fallas en el sistema de seguridad con reconocimiento facial de Buenos Aires"*	La cobertura del medio recupera las voces de Larreta, de Holway y de integrantes del CORREPI. Analiza el funcionamiento del sistema de reconocimiento facial, pero con una postura muy crítica.	Desactualización de las bases de datos del CONARC. Aborda la implementación del reconocimiento facial como instrumento de control social.	Retoma la afirmación de María del Carmen Verdù, titular del CORREPI *"si para detener a un criminal necesitas privar de la libertad a 1000 personas que no hicieron nada, estás cometiendo un daño mucho más grave".*	Retoma los dichos de Patricia Bullrich, *"vamos a tener la capacidad de darle enorme tranquilidad a la sociedad de que no está caminando al lado de un asesino, al lado de un pederasta".*
De la Bahía 29/7/201	*"Aciertos y errores del nuevo sistema de reconocimiento facial en las calles de Buenos Aires*".	Busca mostrar los aspectos positivos de esta tecnología al detallar el número de prófugos detenidos e ilustra los riesgos al reconstruir el caso de Holway.	Presenta el problema como un sistema de vigilancia masivo y enfatiza la desactualización de las bases de datos del CONARC.	No se menciona	Mantiene una postura "neutra" al sostener que el sistema *"arrojó buenos y malos resultados"*. Sostiene la detención de 226 sujetos por delitos graves pero que el 81.59% del total de los 1227 identificados quedaron libres.
Argentina Today 3/8/2019	*" Argentina: Víctimas del reconocimiento facial estatal"*	Se recurre a otros medios para reconstruir múltiples casos de detenciones erróneas provocadas por el sistema de reconocimiento facial en CABA.	Se enfatiza la desactualización de las bases de datos del CONARC.	No se menciona	No se menciona

Página 12 4/10/2019	*"Cámaras de reconocimiento facial: Larreta prometió 10.000 más".*	Fuerte crítica al sistema de videovigilancia porteño.	El medio presenta el problema y se remite a un sistema de vigilancia total de manera no explícita.	Referencia directa a la problemática de la intimidad.	Se retoma la declaración de la campaña electoral de Larreta de instalar *"10000 cámaras con reconocimiento facial*". en todos los barrios para que "*cada día vivamos más tranquilos."*

Fuente: Elaboración propia en base a coberturas periodísticas.

Conclusiones Análisis cobertura mediática.

En la cobertura mediática del caso de Holway, la amplia mayoría de los medios enuncia como factor desencadenante de su errónea detención a la desactualización de las bases de datos del CONARC. Ello implica que el error no fue provocado por el funcionamiento del propio sistema de reconocimiento facial habilitado en la Ciudad Autónoma de Buenos Aires sino en los incorrectos manejos de los funcionarios encargados de la base de datos.

Si bien este parece ser el enfoque más común que los medios de comunicación le otorgaron al caso, cabe destacar que, aquellos medios con una línea editorial contraria al gobierno porteño como" Página 12" o el canal ruso "RT" han considerado la implementación del reconocimiento facial como "un sistema de vigilancia total" y como instrumento de control social, a la vez que alertan acerca de la problemática respecto a la privacidad que supone su implementación, siendo RT el medio que toma mayores cantidades de declaraciones de voces opositoras con respecto a la implementación del sistema.

Medios con la línea editorial más cercana al gobierno de "Juntos por el Cambio" en CABA como "Clarín" o "Todo Noticias" también sostienen que el principal problema que derivó en la errónea detención de la ciudadana fue la desactualización de la base de datos por parte del Poder Judicial, y, a diferencia de los medios opositores al gobierno porteño, ni "Clarín" ni "TN" hacen referencia a la implementación de un sistema de vigilancia total ni propio de la sociedad de control. Por el contrario, ambas coberturas mediáticas recuperan discursos propios del oficialismo en los cuales se justifica la implementación del reconocimiento facial como herramienta para combatir la criminalidad en CABA.

Es justamente a través de reflexiones similares a los de estos medios que la alianza entre la dirigencia política de turno y algunos conglomerados mediáticos transmiten construcciones periodísticas que incorporan discursos propios de la "política del miedo". Sin embargo, como se ha visto a lo largo de este capítulo, esto no evita que, incluso, desde los medios de

comunicación afines al gobierno se eleven críticas en torno al incorrecto funcionamiento de las nuevas tecnologías de control y vigilancia en el espacio público.

El caso observado también ha recibido cobertura periodística de medios de comunicación más pequeños correspondientes a localidades del interior del país como la Ciudad de Mercedes (diario "u Mercedes") y la Ciudad de Bahía Blanca (diario De La Bahía). "Tu Mercedes" presenta al sistema de reconocimiento facial como "un sistema de vigilancia masivo" mientras que, "De La Bahía", si bien sostiene qué puede implicar la instalación de un sistema de vigilancia masivo, enfatiza que el error que derivó en la detención de Holway se debió a la desactualización del CONARC. Este medio muestra una postura "neutra" afirmando que la implementación de las nuevas tecnologías de vigilancia y control buscan arrojar resultados positivos y negativos, aunque no especifica ninguna postura ni a favor ni en contra de las políticas de seguridad implementadas por el gobierno porteño.

Finalmente, el diario "País 24" considera que la detención de la ciudadana se debió a la desactualización de las bases de datos del CONARC, aunque, la cobertura periodística del medio parece afirmar, implícitamente, que fue "perseguida" por el sistema de reconocimiento facial debido a denuncias que realizó sobre el expresidente de la Nación, Mauricio Macri. Se deduce, entonces, que para "País 24" el gobierno porteño utiliza el reconocimiento facial como un instrumento de persecución y control masivo de la ciudadanía lo que supone una violación a su privacidad.

Si bien muchas de las coberturas periodísticas mencionan que Rachel Holway es fundadora de la ONG "Alerta Vida", en ninguno de los medios se hace hincapié que su detención pudo haber estado vinculada a las denuncias que llevó a cabo. Así como en capítulos anteriores se ha abordado el hecho de que el sistema de reconocimiento facial es utilizado en otros países para controlar grupos sociales específicos, el medio "País 24" desliza la idea que esta tecnología puede ser utilizada en Argentina hacia personas específicas según la voluntad del gobierno de turno.

2.Errores que cuestan caro: El caso de análisis de Guillermo Federico Ibarrola en la Ciudad Autónoma de Buenos Aires.

2.1 Descripción del caso

Otro caso de un supuesto error en el funcionamiento del sistema de reconocimiento facial se tornó visible con Guillermo Federico Ibarrola, identificado por el software en la estación de trenes de Retiro el sábado 27 de julio de 2019 y acusado de un robo en Bahía Blanca acontecido en mayo del 2016. La familia del detenido denuncia una captura por error porque asegura que

el ciudadano desconoce esa ciudad. Los allegados del supuesto prófugo aluden que en el 2014 fue víctima de un robo donde le sustrajeron el DNI y en este marco creen que podría haberse gestado una presunta confusión. Ibarrola fue liberado luego de estar detenido 6 días pese a declarar su inocencia desde el momento de su detención.

El acusado fue detenido también en uno de los puntos neurálgicos de la Ciudad de Buenos Aires. Después de ser identificado y trasladado a la Ciudad de Bahía Blanca se confirmó su inocencia y su incorrecta detención se atribuyó a un error del Documento Nacional de Identidad (DNI) de los sospechosos del ilícito en las bases de datos del CONARC, lo que provocó que el propio Ibarrola fuese considerado como prófugo de la Justicia. Su situación procesal fue aclarada y las autoridades reconocieron su error afirmando que "*se mandaron una macana muy grande"*[78] y dispusieron su liberación.

Tomando como referencia su caso es posible identificar dos grandes falencias en el sistema de reconocimiento facial que fueron denunciadas en el informe realizado por la ADC.

Por un lado, se contemplan falencias en las bases de datos del CONARC debido a la carga errónea de los DNI de los ciudadanos reclamados por la justicia, lo que deriva en la identificación y detención equivocada (como en este ejemplo) de los sujetos que transitan en el espacio público. Cabe enfatizar que ambas detenciones se debieron a errores humanos en el manejo de las bases de datos que opera el reconocimiento facial en CABA. La operación de estas bases de datos recae en miembros del Poder Judicial y de las fuerzas de seguridad y, como sostiene la ADC, esto representa una de las grandes falencias de estos sistemas que se encuentran en operación en el espacio público de la Ciudad.

El manejo incorrecto y descuidado de las bases de datos como el CONARC implica serias consecuencias para la ciudadanía. No sólo se afecta el derecho a la privacidad e intimidad de la población y al hecho de recibir ataques a la reputación y honra de los afectados, sino que las consecuencias de las incorrectas detenciones pueden ser mucho más severas y extensas en el tiempo.

Para ilustrar esta afirmación, se puede añadir que el delito del cual se lo acusaba estaba caratulado como *"Robo agravado"* que contempla una pena de entre cinco y quince años de prisión de acuerdo con el artículo Nº166 del Código Penal Argentino. Ibarrola tuvo la fortuna de que el Poder Judicial se percatase a tiempo de su error y lo ratificara, caso contrario, el

[78] Véase https://tn.com.ar/policiales/paso-seis-dias-detenido-por-un-dato-mal-cargado-en-el-sistema-de-reconocimiento-facial_984084/

ciudadano hubiera enfrentado un proceso judicial muy dificultoso, por lo que declaró al recuperar su libertad *"Me podrían haber arruinado la vida*".[79]

Este caso denota otra falencia que posee el sistema de reconocimiento facial ya que, según el informe publicado por la ADC, el único personal con acceso al funcionamiento del sistema son los integrantes de la Policía de la Ciudad, excluyendo a otras fuerzas de seguridad y a funcionarios de otros ministerios, pese a que el delito atribuido a Ibarrola no ocurrió en CABA.

A esta altura es necesario preguntarse acerca del grado de capacitación y experiencia que poseen los operadores de las cámaras de videovigilancia y reconocimiento facial de la Ciudad ya que, al investigar sobre el tema, no fue posible acceder a una copia del manual del procedimiento de los Centros de Monitoreo Urbano (CMU) de la Policía de la Ciudad, lo que contribuye a aumentar el marco de opacidad y secretismo mediante el cual operan las tecnologías de vigilancia y control.

2.2 Tensión con la normativa vigente

2.2.1 Tensión con la regulación nacional

Estudiando este caso en detalle, se observa una violación a la Ley de Protección de Datos Personales Nº25.326. Se evidencia que los datos biométricos del sujeto en cuestión estaban precargados en el sistema de reconocimiento facial aun cuando el ciudadano no tenía una orden de captura por un delito cometido.

Asimismo, se puede considerar que el error cometido por las fuerzas de seguridad viola el artículo Nº4 de la Ley Nº25326. La identificación errónea del ciudadano Ibarrola no sólo dañó su intimidad y privacidad al ser identificado por las tecnologías de control y vigilancia de las fuerzas de seguridad en el espacio público, también constituyó una violación a su honra y reputación. Cabe mencionar aquí la lentitud de la justicia en rectificar el error y otorgarle la libertad. Este ataque a su honra y reputación es contemplado por el nuevo Código Civil y Comercial (2015) que en su Artículo Nº52 establece la imagen como uno de los aspectos más importantes para preservar la intimidad y privacidad de la población argentina cuando sostiene *"la persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad o que de cualquier modo resulte menoscabada en su dignidad personal puede reclamar la prevención y reparación de daños sufridos*".

79 Véase https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial/

En este caso se detecta una tensión entre el derecho a la privacidad y la vigilancia al mirar el Artículo Nº4 inciso 5 de la Ley Nº25.326 que apunta a la necesidad de que en caso de existir datos total o parcialmente inexactos o incompletos éstos deberán ser suprimidos o sustituidos por los responsables de los archivos de las bases de datos. Sin embargo, en este caso hubo un manejo descuidado en torno a los datos de información personal del ciudadano por parte de los integrantes del Poder Judicial como de las fuerzas policiales lo que ocasionó un grave perjuicio para su privacidad.

En el Artículo Nº16 inciso 1 y 2, la Ley Nº25.326 establece el derecho de la ciudadanía a que su información personal sea rectificada, actualizada o suprimida cuando corresponda por parte de los responsables de los bancos de datos en el plazo máximo de cinco días luego de que se hubiese detectado el error o la falsedad en la información. Aquí, el manejo incorrecto de las bases de datos no sólo fue responsabilidad de los integrantes de las fuerzas policiales y del Poder Judicial, sino que cabe aclarar que el sujeto permaneció detenido por las autoridades una semana superando el tiempo máximo establecido por la ley para subsanar el error.

Analizar el caso Ibarrola nos invita observar el Artículo Nº3 de la Disposición 10/2015 DNPDP que establece que "*deberá evitarse especialmente cualquier afectación del derecho a la privacidad".* Por otro lado, y para resguardar el carácter privado de la información de la ciudadanía, el Artículo Nº4 reza *"los responsables de las bases de datos deberán adaptar medidas técnicas y organizativas que resulten necesarias para evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones intencionales o no de información ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado".*

De este modo, se observa que estas legislaciones no fueron tenidas en cuenta por el despliegue de las tecnologías y de las nuevas modalidades de vigilancia en el espacio público de la Ciudad.

De la misma forma que en el caso de Holway, en el de Ibarrola se produce una tensión respecto a lo estipulado por el Artículo Nº19 de la Constitución, el cual establece que las acciones privadas de los hombres que no afecten la moral o el orden público o a otros ciudadanos no son competencia de la autoridad de los magistrados. Por lo cual, en este caso como el anterior, los errores humanos en el manejo de las bases de datos y en el sistema de reconocimiento facial provocan la detención del ciudadano al volver de un encuentro familiar, actividad que escapa a la competencia del Poder Judicial. Si bien el delito por el que fue requerido por la justicia argentina parece justificar el despliegue del reconocimiento facial, los errores en la carga de la información personal del sujeto es lo que provoca que las nuevas modalidades de vigilancia terminen generando una seria intrusión en su vida personal poniendo en tensión su privacidad.

Al analizar la Resolución 238/2012 del Ministerio de Seguridad se evidencia una tensión con respecto a tres artículos entre el derecho a la privacidad y la vigilancia. En primer lugar, el Artículo Nº2 declara que el sistema de videovigilancia debe operar sustentado en los principios de legalidad y respeto de la privacidad de las personas, mientras que el uso de imágenes captadas tiene el objetivo de prevenir y conjugar ilícitos resguardando los derechos, libertades y garantías de las personas. El manejo inadecuado de las bases de datos no sólo no contribuyó a generar una sociedad más segura, principal argumento esgrimido para la implementación del reconocimiento facial y nuevas tecnologías de control y vigilancia, sino que también afectó el derecho a la privacidad e intimidad de un ciudadano inocente.

En segundo lugar, se muestra una clara tensión entre vigilancia y privacidad al recuperar el punto 13 de la Resolución 238/2012 que establece que el personal asignado al sistema de videovigilancia y bases de datos debe contar con la capacitación e idoneidad técnica y legal acorde a las responsabilidades y funciones que deberá ejercer. Sin embargo, la cobertura del caso dejó al descubierto errores humanos del personal policial y de funcionarios judiciales encargados del manejo de la información de carácter sensible de la población, lo que se ve agravado debido a la opacidad característica en el funcionamiento del sistema tanto de videovigilancia como de reconocimiento facial y el secretismo con que operan estas nuevas tecnologías propias de las sociedades de control.

En tercer lugar, existe una tirantez entre vigilancia y el punto 14 de la Resolución 238/2012 en la que se establece que todo registro de videovigilancia debe cumplimentar en materia de procedimiento, tratamiento, protección y resguardo de los datos captados por el sistema establecido por la Ley de Protección de Datos Personales Nº25.326, así como por las normas locales y provinciales aplicadas a estas tecnologías de vigilancia y control.

2.2.2 Tensión con la regulación de la Ciudad

Al estudiar este caso se puede afirmar que la actuación del sistema de videovigilancia ha vulnerado la Ley Nº3.130 de la reglamentación para el sistema de monitoreo de CABA, que, específicamente, en su artículo N°2 afirma que el protocolo de intervención del sistema de cámaras debe actuar respetando siempre lo dispuesto por la Ley Nº2.602, la cual establece que el uso de las tecnologías de vigilancia y control como las cámaras de videovigilancia y reconocimiento facial siempre deberán buscar una intervención mínima sobre la privacidad e intimidad de la ciudadanía y moderada por los principios de proporcionalidad y razonabilidad, de manera que las respuestas de las fuerzas de seguridad no sean desproporcionadas.

El caso Ibarrola muestra las tensiones generadas entre el derecho a la privacidad y la vigilancia al observar lo establecido en la Resolución 398/17 del Ministerio de Justicia y Seguridad del gobierno de la Ciudad ya que el cuerpo del texto remite al Artículo Nº12 de la Constitución de la Ciudad Autónoma de Buenos Aires donde se reconoce como una garantía *"el derecho a la privacidad, intimidad y confidencialidad como parte inviolable de la dignidad humana".*

Del mismo modo que en el análisis del caso de Rachel Holway, la Ley Nº5.688 en el Artículo Nº75 inciso 7, remarca que el proceso de innovación tecnológica es propio de las fuerzas de seguridad en el marco de las sociedades de control y tiene el objetivo de mejorar la gestión institucional y la transparencia y debe ser utilizada para el combate y la prevención de delitos. Sin embargo, la incorporación de las nuevas tecnologías aplicadas a las fuerzas de seguridad como a la justicia no contribuyeron a transparentar el accionar de estas instituciones. Por el contrario, la cobertura periodística del caso por parte de algunos medios detectó mutuos reproches entre el Poder Judicial y las fuerzas policiales sobre el desprolijo manejo de las bases de datos lo que provocó la errónea detención del ciudadano.

Asimismo, genera una rigidez con el Artículo Nº475 de la ley que establece el respeto al régimen de garantías de los derechos fundamentales de la ciudadanía como de sus libertades públicas en el proceso de captación de los materiales y su posterior uso y almacenamiento.

Cabe mencionar también una tensión con el Artículo Nº476 que en sintonía con lo dispuesto por el Articulo 2 de la Ley Nº2.602 sostiene que el uso del sistema integral de videovigilancia se deberá regir respetando los principios de razonabilidad y proporcionalidad para combatir los hechos delictivos.

Tampoco se debe omitir lo establecido por el Artículo Nº6 de la Ley Nº3.130 que enfatiza sobre los funcionarios públicos y/o los agentes de las fuerzas de seguridad que vulneren los principios y procedimientos referidos a la protección de la intimidad de la ciudadanía establecidos tanto por esta ley como por la Nº2.602. En este sentido, en algunos medios de comunicación se sostuvo que se aplicarían sanciones administrativas ya que la ley califica la falta como grave y atribuye responsabilidades civiles y penales hacia los responsables del error que derivó en la errónea detención del sujeto. Sin embargo, no se brindó más información sobre este aspecto, lo que se entiende que contribuye a aumentar la opacidad y secretismo sobre los manejos internos dentro de las fuerzas de seguridad y del Poder Judicial en Argentina.

Por último, entonces, es posible sostener que al igual que en el anterior caso, aquí existe una tensión respecto al Decreto 716/2009 el cual reglamenta la aplicación de la Ley Nº2.602 en CABA que en su Artículo Nº1 deja establecido que el uso del sistema de videovigilancia en espacios públicos deberá respetar, en todas sus fases, los derechos fundamentales y las

libertades públicas de la ciudadanía de forma ineludible aunque, el análisis y descripción de los casos abordados en esta tesina contradicen esta legislación.

Cuadro Nº6: Tensiones de la legislación con el caso Ibarrola

Regulaciones	***Tensiones***
Regulaciones Nacionales	
Constitución Nacional	Entra en tensión con el Articulo 19
Constitución Nacional	No entra en tensión con el Artículo 43
Ley de Protección de Datos Personales N°25326	Tensión con el Artículo 4° inciso 4 y 5 Tensión con el Artículo 16° inciso 1 y 1
Nuevo Código Civil y Comercial	Tensión Artículo 52°
Disposición 10/2015 DNPDP	Tensión con el Artículo 3° y 4°
Resolución 238/2012 Ministerio de Seguridad.	Tensión con el Artículo 2°,3°,13° y 14°
Regulaciones Ciudad Autónoma de Buenos Aires	
Resolución 398/19 MJYSGC	Tensión con el Artículo 12
Ley N°5688	Tensión con el Artículo 75° Inciso 7 Tensión con el Artículo 475° y 476°
Ley N°2602	Tensión con el Artículo 1° y 2°
Decreto 716/2009	Entra en tensión al reglamentar la Ley Nº2602
Ley N°3130	Tensión con el Artículo 2° y 6°
Resolución 10/MJYSGC/10	No entra en tensión
Resolución 314/,JYSGC/10	No entra en tensión
Resolución 157/GCABA/12	No entra en tensión.

Fuente: Elaboración propia en base a las leyes

Luego de analizar el caso de Guillermo Ibarrola se observa que la implementación masiva de nuevas tecnologías y modalidades de vigilancia, como el reconocimiento facial, implica que se genere una rigidez y en algunos casos, una violación de las legislaciones nacionales y de CABA destinadas a regular el funcionamiento del sistema de videovigilancia y a proteger los derechos a la privacidad e intimidad de la población.

Con Ibarrola se evidencia que en el caso de algunas normativas nacionales como la Ley Nº25.326, la Resolución 238/2012 del Ministerio de Seguridad, la Ley Nº5.688 y la Ley Nº2.602 de CABA implican una tensión grave respecto a la privacidad de la población frente a la implementación de estas tecnologías.

Respecto a legislaciones nacionales como el Artículo Nº52 del Nuevo Código Civil y Comercial y la Disposición 10/2015 DNPDD y legislaciones de CABA como la Ley Nº2.602, el Decreto 716/2009 y la Ley Nº3.130, si bien presentan una tensión con respecto al derecho a la privacidad, se puede considerar que no revisten la misma gravedad que las legislaciones mencionadas anteriormente.

Finalmente, respecto de legislaciones nacionales como el Artículo Nº23 de la Constitución Nacional, así como la Resolución 314 JYSGC/10 y la Resolución 1577GCABA/12 de CABA en este caso analizado, no se evidencia una tensión con la privacidad de la ciudadanía.

2.3 Análisis cobertura mediática

La cobertura periodística del caso de Guillermo Ibarrola también recibió atención de los medios nacionales (opositores y oficialistas) condicionado por la línea editorial a la cual corresponden y su apoyo o no a las medidas y políticas de seguridad tomadas por la gestión de" Cambiemos" en CABA.

El caso recibió una fuerte cobertura mediática de los medios tradicionales y digitales. Se ha registrado que, al menos 12 medios[80] (11 nacionales y el internacional canal ruso RT) han cubierto mediáticamente el caso cuya detención errónea ocurrió en CABA donde actualmente se encuentra operando el sistema de reconocimiento facial. La cobertura mediática de medios procedentes del interior del país como el diario "El Patagónico" de la provincia de Chubut y algunos de los medios más grandes de Argentina como el grupo "Clarín" o el portal de noticias Infobae, ambos poseedores de un gran alcance y recepción a lo largo y ancho del país también se hicieron presente. El impacto del caso generó un repudio generalizado en los medios de comunicación no sólo por el extenso tiempo que fue detenido siendo inocente, sino también por la gravedad de la causa (robo agravado) imputada.

[80] Véase https://www.youtube.com/watch?v=oXM3dQpN9k4www.youtube.com/watch?v=iMCPRxjOUws https://www.youtube.com/watch?v=gCmwcbz78kc https://www.a24.com/actualidad/hombre-estuvo-detenido-seis-dias-error-recupero-libertad-haber-arruinado-vida-08022019_SJSieA-XB https://telefenoticias.com.ar/actualidad/lo-detuvieron-en-retiro-por-el-sistema-de-reconocimiento-facial-su-familia-sostiene-que-es-un-error/

Cabe destacar que una de las coberturas periodísticas que se pronunció por el caso de Ibarrola fue la agencia Télam, que funciona como una sociedad de estado y se conforma como la segunda mayor agencia de noticias argentinas de Latinoamérica[81].

Uno de los medios que ha cubierto el caso con mayor cantidad de notas periodísticas es el diario "La Brújula 24". Este medio de comunicación hizo un seguimiento bastante profundo del caso Ibarrola al realizar, al menos cuatro notas periodísticas que informan a la ciudadanía sobre lo ocurrido con la detención y posterior proceso judicial que atravesó.

"La Brújula 24" es un medio de comunicación que pertenece a la Ciudad de Bahía Blanca, localidad donde se cometió el crimen por el cual se acusaba al detenido. El tratamiento mediático brindado por este medio no incluye calificaciones positivas ni negativas hacia el sistema de videovigilancia o el accionar de las fuerzas de seguridad. Sólo hace hincapié en la reconstrucción del hecho desde el punto de vista del detenido y busca diferenciarse de la cobertura periodística de otros medios al incluir la voz del secretario general de la fiscalía de Bahía Blanca, quien responsabiliza a las fuerzas policiales en el error en la carga de la información y afirma *"es lamentable, inadmisible, fueron seis días detenido de forma injusta, todo por un error desde la policía de Bahía a la hora de consignar los datos de la persona que se estaba buscando"*. [82]

El canal ruso RT también presentó una cobertura periodística del caso siendo uno de los pocos medios internacionales (si no el único) que se ha podido detectar para la realización de este análisis. El tratamiento mediático del caso por parte del medio se reduce únicamente a una noticia donde se intenta reconstruir brevemente la detención del sujeto calificando al sistema de reconocimiento facial como *"controvertido"*, y, al igual que la cobertura de otros medios de comunicación de la Argentina, adjetivando la experiencia del ciudadano como una *"pesadilla"*.

Por otro lado, si bien RT busca reflejar la postura de la Policía de la Ciudad frente al sistema de reconocimiento facial, se observa una clara posición del medio en contra de este sistema, ya que su cobertura periodística hace eco de lo afirmado por otros medios de la oposición

[81] Es relevante que Télam haya cubierto mediáticamente este caso debido no sólo al gran alcance mediático que posee sino al hecho de que múltiples medios de comunicación dentro y fuera del país recurren a la información publicada por esta agencia para la construcción de las noticias que publican, por lo que se ha visto aumentado el alcance y difusión de lo ocurrido.

[82] Véase https://www.labrujula24.com/2019/08/01/lo-detuvieron-por-un-robo-en-bahia-pero-no-conoce-la-ciudad-n7319

argentina como "Página 12" *"hay un error de interpretación y todos apuntan al sistema cuando en verdad lo que hubo fue un error de carga de los datos en el CONARC".*[83]

El tratamiento del caso por parte de RT busca recabar voces con un fuerte grado de crítica hacia el sistema como la voz de la abogada María Julia Giorelli, del Centro de Protección de los Datos de la Defensoría quien sostuvo "*en todos estos problemas con los datos del CONARC que están muy desactualizados o mal cargados, tenemos que decir que el sistema no está funcionando".*

Al igual que el caso de Rachel Holway, la errónea detención de Ibarrola recibió cobertura mediática en medios de comunicación como Clarín, el portal de noticias de Infobae o el canal de Todo Noticias[84], cuya línea editorial se muestra más afín a las políticas del gobierno de la Ciudad. Estos mostraron un fuerte nivel de crítica hacia la errónea detención de Ibarrola, pero defendieron el funcionamiento del sistema de reconocimiento facial: *"El reconocimiento facial funcionó bien, estaba mal cargada la búsqueda"*, publicó la cobertura de Infobae, mientras que el diario "Clarín" afirmó que los funcionarios judiciales desligaron de cualquier responsabilidad al sistema de reconocimiento facial porteño *"utiliza como base de datos la del RNP y funcionó bien. Por eso identificó a Ibarrola con el número de DNI que había colocado la policía, pero el error venía de antes"*[85]. Clarín también enfatizó que el oficial encargado de subir las informaciones a las bases de datos en forma errónea provocando la detención equivocada sería sancionado con penas administrativas.

En medios opositores como "Página 12" se hizo énfasis en la crítica al sistema de videovigilancia de CABA al considerarlo como un sistema de vigilancia *"Orwelliano"*[86]mismo calificativo que fue empleado por el medio en la cobertura periodística del caso Holway, mientras que la cobertura de "La Izquierda Diario", también opositor realiza una crítica dura pero que no roza lo burlesco. Se pronuncia hacia el sistema de videovigilancia y reconocimiento facial como un "*chiche vigilante"* que *"amarga y perjudica la vida de varias personas"*[87] y de la entonces ministra de seguridad de la Nación, Patricia Bullrich a quien considera como *"la gran hermana"* que se desvela pensando en cómo vigilar a grandes sectores de la población.

---

[83] Véase https://actualidad.rt.com/actualidad/323123-argentino-semana-rejas-reconocimiento-facial

[84] Véase https://tn.com.ar/policiales/paso-seis-dias-detenido-por-un-dato-mal-cargado-en-el-sistema-de-reconocimiento-facial_984084

[85] Véase https://www.clarin.com/policiales/paso-semana-preso-error-policial-sistema-reconocimiento-facial_0_6KiuCu0fy.htmç

[86] Véase: https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien

[87] Véase: http://www.laizquierdadiario.com/El-Gran-Hermano-macrista-mantuvo-6-dias-preso-a-un-hombre-pero-fue-un-error

El diario "Tiempo Argentino", con una línea editorial opositora a las políticas establecidas por el gobierno porteño, cubrió el caso de Ibarrola estableciendo un fuerte nivel de crítica hacia el despliegue de las nuevas tecnologías de control y vigilancia en el espacio público de la Ciudad. El medio realizó una reconstrucción del caso desde el punto de vista de la víctima empleando una adjetivación fuerte y contundente para describir la experiencia que atravesó al considerarla como una "pesadilla".[88] quien afirmó *"me tocó como le puede tocar a cualquier otra persona por un error en una máquina".*[89]

"El Grito del Sur" es otro diario con una línea editorial opositora a la gestión de "Juntos por el Cambio" en CABA. Este medio también generó una fuerte crítica al funcionamiento del sistema, pero, su crítica raya lo burlesco al utilizar la calificación de "insólito"[90] para describir la detención del sujeto.

Se puede considerar que el término "insólito" utilizado por el medio para describir el accionar llevado a cabo por las fuerzas de seguridad de la Ciudad encargadas de la operación de estas tecnologías remite a lo ineficaz e incompetente a la hora de utilizarlas.

Al analizar la cobertura de los distintos medios se observa que el tratamiento informativo busca que los receptores empaticen con el caso del ciudadano, se coloque en su lugar y llegue a entender que nadie está exento de que le ocurra lo mismo.

Cuadro Nº7: Cobertura mediática caso Guillermo Ibarrola

Medio/ fecha	Título	Resumen noticia	Principal problema enunciado	Tensión respecto a la privacidad	Referencia a la política del miedo
Telefé Noticias 1/8/2019	*"Lo detuvieron por Sistema de Reconocimiento Facial y denuncian que es un error".*	Se describe el caso a través de un tratamiento mediático sensacionalista y recupera los dichos de su familia.	Se aborda el problema a través de declaraciones del grupo familiar y que se trató de un error policial. No se registran declaraciones oficiales.	No se menciona	No se menciona

[88] Véase https://www.tiempoar.com.ar/nota/la-pesadilla-del-hombre-que-estuvo-cinco-dias-preso-por-un-error-policial

[89] Véase https://www.tiempoar.com.ar/nota/la-pesadilla-del-hombre-que-estuvo-cinco-dias-preso-por-un-error-policial

[90] Véase https://www.eldiariosur.com/esteban-echeverria/policiales/2019/8/1/insolito-un-vecino-esta-detenido-por-un-robo-en-bahia-blanca-pero-nunca-estuvo-en-esa-ciudad-25053.html

La Brújula 24 1/8/2019	*"Lo detuvieron por un robo en Bahía, pero no conoce la ciudad"*	Refleja la voz de los integrantes de la familia que reclaman su liberación. El medio postula la teoría del mal manejo de la información por parte de la fuerza policial.	Enfatiza el error en la carga de la información por parte de la policía bonaerense.	No se menciona	No se menciona
El diario Sur 1/8/2019	*". "Insólito: Un vecino está detenido por un robo en Bahía Blanca, pero nunca estuvo en esa ciudad"*	Califica el hecho como "insólito" y remarca la intención de los afectados de iniciar causas judiciales al gobierno porteño por lo sucedido.	Error en la carga de datos por parte del personal policial.	No se menciona	No se menciona.
Télam 2/8/2019	*"Pasó seis días preso por un error en la base del Sistema de Reconocimi ento Facial*"	Se califica su experiencia como una *"pesadilla"* debido al mal manejo de la información personal en la base de datos.	Enfatiza el error en la carga de la información por parte de la policía bonaerense.	No se menciona	No se menciona
Infobae 2/8/2019	*" Un hombre estuvo detenido seis días preso por un error policial".*	Reconstrucción desde la perspectiva del ciudadano. Remarca los errores humanos y no al sistema.	Enfatiza la desactualizació n de las bases de datos del CONARC.	No se menciona	El a sistema de reconocimiento facial funcionó bien. Se atribuye el error a la carga de datos.
A24 2/8/2019	*"El hombre que estuvo detenido seis días por un error recuperó la libertad: Me podrían haber arruinado la vida".*	Se construye la noticia en tres apartados breves: ¿"Qué pasó", "Cómo comenzó el caso" y "cuál fue el error?" Se recurre al testimonio audiovisual del sujeto y de su madre que denuncia la errónea detención.	Enfatiza el error en la carga de la información por parte de la policía bonaerense.	No se menciona	Las declaraciones de Santiago Garrido, Secretario General del Ministerio Público de Bahía Blanca defiende el uso del sistema *"La confusión no tuvo nada que ver con el sistema de reconocimiento facial".*

La Izquierda Diario 2/8/2019	*"El gran hermano macrista mantuvo seis días preso a un hombre…pero fue un "error".*	La cobertura es totalmente opositora a la utilización del reconocimiento facial y lo llama "chiche vigilante" Utiliza un discurso que suena burlesco e irónico, considerando a la exministra de Seguridad de la Nación, Patricia Bullrich, "La Gran hermana".	Enfatiza el error de la carga en la base de datos y al sistema de reconocimiento facial como un sistema de vigilancia total.	No se menciona	No se menciona
Clarín 2/8/2019	*"Pasó casi una semana preso por un error policial".*	Muestra la postura de las autoridades de Justicia y Seguridad en defensa del sistema y trasladando la responsabilidad al mal manejo de las bases de datos. Remarca acciones reparatorias del Ministerio Público: pago de cena y micro y sanciones punitivas para los responsables del error.	Error en la carga de datos por parte del personal policial.	No se menciona	Desde el medio sostienen que, para evitar errores como este, las fuerzas policiales de CABA siguen estrictos protocolos de actuación afirmando que la implementación de este sistema de reconocimiento facial es necesario.
Tiempo Argentino 2/8/2019	*"La pesadilla del hombre que estuvo seis días preso por un error policial".*	Enfatiza la construcción de la noticia desde la perspectiva del sujeto, construyendo la información mediante textuales narrados por él. La noticia se engloba en la sección de represión estatal y se recuperan	Error en la carga de datos por parte del personal policial.	Se muestra la tensión implícita con la privacidad de la ciudadanía ya que, según las declaraciones de la Policía de la Ciudad se está trabajando para *"limpiar las bases de datos*". lo que supone que hay información de ciudadanos argentinos que no se deberían	Se da lugar a voces oficiales que afirman que la detención se debió a errores en el manejo de los datos y no a un problema del software de reconocimiento facial.

		las declaraciones de la familia.		encontrar allí, lo que implica una violación a la privacidad.	
Página 12 3/8/2019	*"Seis días arrestado por un error del Sistema de Reconocimiento Facial"*	Amplia cobertura en primera persona. Muestra una postura muy crítica al sistema de reconocimiento facial y al manejo de las bases de datos policiales. También refleja la postura del Ministerio de Seguridad de CABA.	Enfatiza el error de la carga en la base de datos y al sistema de reconocimiento facial como un sistema de vigilancia total.	No se menciona	Retoma las declaraciones del Secretario de Justicia y Seguridad de CABA, Marcelo D'Aleesandro quien defiende la aplicación del reconocimiento facial para combatir delitos: *"hay un error de interpretación, y todos apuntan al sistema cuando en verdad lo que hubo fue un error de carga de los datos en el CONARC".*
RT 4/8/2019	*"A casi una semana entre rejas por un crimen que no cometió: un argentino acaba preso por un error en un Sistema de Reconocimiento Facial*	Mantiene una postura muy crítica frente a la implementación del sistema retomando voces en su contra por parte del Centro de Protección de Datos de la Defensoría de la Argentina.	Enfatiza el error en la carga de datos del CONARC	Referencia indirecta a la privacidad de la ciudadanía al apuntar frases: "*le podrían "haber arruinado la vida" y" le puede tocar a cualquier otra persona por el error de una máquina".*	Las autoridades de la CABA defienden el sistema de reconocimiento facial y afirman que simplemente hubo una carga incorrecta de información en el CONARC

Todo Noticias (TN) 6/8/2019	*"Pasó seis días detenido por un dato mal cargado en el Sistema de Reconocimiento Facial*	Extensa nota en primera persona complementado con material audiovisual que incorpora una entrevista al ciudadano afectado. Se puntualiza el mal manejo de la base de datos y retoma el caso Holway como ejemplo de múltiples situaciones en CABA.	Enfatiza el error de los funcionarios judiciales en la carga de datos en el CONARC.	Remarca la inocencia de Ibarrola y de forma implícita reconoce la invasión a la privacidad del ciudadano.	El Ministerio de Justicia y Seguridad de la Ciudad reconoce un 4% de falencias en el sistema, aunque afirma que ello se debe en buena medida a falencias en la carga de datos de los prófugos.

Fuente: Elaboración propia en base a coberturas periodísticas

Conclusiones análisis cobertura mediática

La cobertura mediática del caso de Ibarrola, independientemente de la línea editorial a la que los medios adhieran, identifican la errónea detención al error en la carga de datos del CONRC por parte del personal policial e integrantes del Poder Judicial. Analizando las coberturas mediáticas sobre este caso se observa un enfrentamiento entre las competencias y responsabilidades de ambas fuerzas y la mutua acusación con respecto a los manejos de las bases de datos de las nuevas tecnologías de control y vigilancia.

Al igual que en el caso de Holway en este también se observa que los medios de comunicación que en su línea editorial muestran mayor afinidad con el gobierno porteño como "Infobae", "Clarín", "Todo Noticias" o "A24", consideran que la detención del ciudadano se debió a errores policiales en la carga de información ("A24" y "Clarín") mientras que "Todo Noticias" atribuye el error a la gestión incompetente de los datos del individuo pero, en este caso, responsabilizando a los funcionarios judiciales. Por su parte, "Infobae" sostiene que la detención se produjo por la desactualización de la base de datos del CONARC sin destacar puntualmente a ningún actor por el error.

En los cuatro medios mencionados afines al gobierno porteño, la cobertura periodística retomó las voces de funcionarios que puntualizaron que la equivocación en la detención del sujeto se debió a falencias humanas porque el sistema de reconocimiento facial no presentó errores. Las voces de las autoridades reflejaron que se trata de una herramienta necesaria para combatir la criminalidad y remarcaron que las fuerzas policiales de CABA siguen estrictos protocolos de actuación para evitar que se produzcan errores como el contemplado ("Clarín").

Se puede afirmar, entonces, que en ambos casos estudiados se observa que a través de la alianza entre la dirigencia política de turno y estos medios de comunicación se produce la transmisión de discursos referidos a la política del miedo de manera tal, que la ciudadanía convalide la implementación de las nuevas tecnologías de control y vigilancia, como el reconocimiento facial para su seguridad personal. En este sentido, se puede evidenciar que los medios de comunicación afines al gobierno porteño (como en el caso de Holway) no han considerado la implementación del reconocimiento facial como tecnología propia de la sociedad de control o un sistema de vigilancia generalizada como sí lo han hecho los medios opositores al oficialismo porteño como "Página 12" o "La Izquierda Diario", quienes consideran que el error no sólo se debió a la carga de datos en las bases del CONARC.

Estos medios reflejan una postura muy crítica respecto a la implementación del reconocimiento facial en CABA por considerarlo un sistema de vigilancia total. La cobertura de la "La Izquierda Diario" juega mucho con la ironía al sostener que los funcionarios del área de seguridad de CABA buscan replicar las tecnologías de vigilancia de Estados Unidos. Las declaraciones de este medio remiten a capítulos anteriores de esta tesis en los que se ha destacado el carácter global en cuanto a la implementación de las nuevas tecnologías y modalidades de vigilancia surgidas, en primera instancia, en los países desarrollados y posteriormente incorporadas al resto de las naciones, pero siempre respetando las particularidades de cada territorio. Este medio no sostiene la posición discursiva de considerar la implementación de estas herramientas como instrumentos para combatir la criminalidad como afirman los medios oficialistas, sino que considera que la implementación del reconocimiento facial en el espacio público y, sobre todo, su uso incorrecto, ya sea por errores técnicos o humanos, supone una represión hacia la ciudadanía y sus libertades y derechos.

Otro de los medios opositores al gobierno porteño es "Tiempo Argentino" el cual marca una fuerte crítica a la incorporación del reconocimiento facial. Y al igual que la mayoría de los medios sostiene que el desacierto fue producido por un mal manejo en la base de datos y en este caso responsabiliza al personal policial enfatizando el peligro que el sistema implica para la privacidad de la población al mencionar las declaraciones de las autoridades de la policía de la Ciudad que apuntan a la necesidad de una limpieza en dichas bases. Pero, uno de los aspectos más llamativos de esta cobertura mediática es el hecho de englobar la noticia del sujeto en una sección denominada *"represión estatal"*.

El caso también recibió la cobertura de un único medio internacional: el canal ruso RT. Este medio puede ser considerado como opositor a las políticas desplegadas por las gestiones tanto nacionales como locales. RT adhiere a la postura de la mayoría de los medios de comunicación

abordados en este análisis al considerar que el error en la detención del sujeto se relaciona a la carga de datos del CONARC y retoma las voces de las autoridades de CABA, quienes destacan el correcto funcionamiento del sistema de reconocimiento facial y adjudican la detención a errores producidos en el manejo de la carga de datos.

La cobertura recibió, a su vez, la atención de medios de comunicación a los que el tratamiento mediático del caso no permite que se los considere como oficialistas y opositores. Tal es el caso de la agencia Télam, el medio "La Brújula 24" o el "Diario Sur", quienes consideran que la principal problemática en la detención se debió a errores de carga de la información por parte del personal policial.

El análisis de las coberturas mediáticas permitió encontrar otros dos aspectos de interés en relación con el caso aquí mencionado. El primero se vincula a la forma en la que la mayoría de los medios de comunicación han construido el caso personalizando e individualizando la historia del detenido para transmitir la idea de que a cualquiera le puede suceder lo mismo. Muchos de los medios abordados en este análisis han construido la noticia recopilando citas textuales de sus declaraciones o de su círculo familiar, transmitiendo, incluso, la información a través de un recorte sensacionalista que generara emotividad en el público e identificación con el caso[91]. Este tipo de cobertura no se logró registrar en el de Rachel Holway, donde los medios de comunicación no reconstruyeron su caso valiéndose de tantas declaraciones personales y apelando al sensacionalismo. Además, cabe mencionar que el tratamiento mediático que ambos recibieron ha sido diferente a pesar de que los dos se presentaron con escasa diferencia temporal (Holway el 11/7/19 e Ibarrola el 27/7/19).

Básicamente, se puede evidenciar que en los análisis realizados es posible diferenciar aquellos medios que poseen una posición más favorable hacia la implementación del reconocimiento facial (aunque no excluye que reconozcan errores en el funcionamiento del sistema), de aquellos medios que se muestran fuertemente contrarios a su incorporación por parte de la Policía de la Ciudad.

En el caso de Ibarrola, se muestran más tolerantes frente al error que derivó en el arresto del ciudadano y evidencian una firme posición de defensa en torno al correcto funcionamiento del reconocimiento facial. El caso supuso una afectación más profunda a los derechos de privacidad y libertad (detenido 6 días mientras Holway sólo estuvo unas horas). A pesar de

[91] En "La Brújula 24" se expresó *"me podrían haber arruinado la vida"*; en TN *"ver a mi madre, a mi novia, a mi hija, verlas desconsoladas, jamás tuve que pasar por eso, no me voy a olvidar más";* en " Página 12*"me tocó a mí, pero le puede tocar a cualquiera"* y en" Tiempo Argentino" *"hoy estoy tranquilo, con mi familia, pero fue una pesadilla que jamás pensé que me iba a tocar vivir".*

ello, no se ha encontrado cobertura mediática condenatoria ante la detención equivocada ni se han registrado declaraciones de altos funcionarios aceptando el error y pidiendo disculpas.
En cambio, el caso de Holway supuso una condena más firme por parte de los medios de comunicación a la desactualización de las bases de datos del CONARC aun cuando, como se ha visto que el caso de Ibarrola representaba una mayor gravedad.
Cabe preguntase entonces, si una de las posibles razones en la diferencia del tratamiento mediático se deba al hecho de que Holway es un personaje público con presencia en los medios de comunicación a través de la tarea que realiza en la ONG "Alerta Vida". Este escenario se repite en ambos casos donde ninguno representaba una amenaza para la convivencia ciudadana.

3. Análisis comparado de casos: Efectos de la práctica del ejercicio del poder

Para profundizar en el análisis de los casos de Rachel Holway y Federico Guillermo Ibarrola es necesario retomar el pensamiento de Foucault desplegado en este trabajo de investigación. A lo largo de estos capítulos se abordó la idea del autor que sostiene que el poder se encuentra en su ejercicio entendido como la capacidad de conducir las conductas y de hacer circular a la población a través de un camino establecido, pero sin necesariamente recurrir al ejercicio de la violencia física. Asimismo, para Foucault, el poder es una fuerza productiva que puede encauzar la conducta de la ciudadanía, y como tal, ejercido en el marco de las sociedades de control produce prácticas en el día a día como se contempla en el análisis de los casos analizados para la construcción de esta tesina.

3.1 Normativas, derechos y latitudes: Efectos en la legislación y en las fuerzas policiales

En el recorrido de este trabajo es posible observar que tanto las legislaciones a nivel nacional como las propias de la Ciudad Autónoma de Buenos Aires son efectos del poder en las sociedades de control contemporáneas y, al mismo tiempo, se producen por otros factores definiendo y produciendo un "mapa" de acción para los diferentes actores presentes en la sociedad: la ciudadanía y las fuerzas de seguridad.
Si se observa la aplicación de las nuevas tecnologías de vigilancia y control en el espacio público, y las legislaciones destinadas a revocar y monitorear su operación, es posible encontrar algunos efectos de las prácticas de poder. Por un lado, en Argentina como a nivel global, el avance de la lógica de sociedad de control expresado claramente a través de los cambios en el paradigma de seguridad del siglo XXl, sumado al desarrollo e implementación de nuevas tecnologías y modalidades de control y vigilancia han dado como resultado una vigilancia masiva e invisible sobre la población sea esta digna o no de sospecha. Todo ello bajo

la premisa de que esta vigilancia constante resulta necesaria a fin de garantizar una sociedad "segura" frente a las amenazas internas como el terrorismo o la criminalidad que pudiesen tener lugar en las sociedades actuales. Este efecto de la práctica de poder se encuentra fuertemente relacionado con otro efecto abordado: la opacidad propia de las fuerzas de seguridad en el marco de las nuevas tecnologías de control como el software de reconocimiento facial, y el manejo de las bases de datos que almacenan información personal y sensible de la ciudadanía. Cabe preguntar entonces ¿en cuántas ocasiones se habrán presentado situaciones, similares a los casos analizados, en el manejo de las bases de datos sin que hayan recibido cobertura mediática como sí lo recibieron los ciudadanos en cuestión? Y aquí surge otra pregunta: ¿Argentina cuenta con los medios técnicos/tecnológicos y de infraestructura para el correcto despliegue del sistema de reconocimiento facial?[92]

Las detenciones erróneas de Holway e Ibarrola se debieron a manejos inadecuados o carga incorrecta de las bases de datos ya sea por parte de miembros del Poder Judicial o por efectivos de las fuerzas de seguridad. Es decir, en ambos casos se puede evidenciar que uno de los efectos de la operación de los sistemas de videovigilancia masiva es el poder presentar graves errores humanos por parte de funcionarios judiciales o policiales.

Por lo tanto, suenan preguntas concretas al respecto: ¿la preparación y capacitación recibidas para el uso de estas tecnologías es apropiada? O ¿el afán por parte del gobierno de la Ciudad de sumar nuevos efectivos contra la inseguridad ha ido en desmérito y afectado el proceso de formación de los efectivos incorporando de esta forma cantidad, pero no calidad a las fuerzas de seguridad?

Con respecto a este escenario hay que remarcar que el Artículo Nº146 de la Ley Nº5688 del Sistema Integral de Seguridad Pública establecida por el gobierno de CABA afirma en su inciso 1º que las capacitaciones de los integrantes de las fuerzas de seguridad deben aspirar a lograr *"desarrollo de aptitudes y valores necesarios para el ejercicio responsable de funciones y labores asignados con conciencia ética, solidaria, reflexiva y crítica".* Mientras que el inciso 4º del mismo artículo apunta al *"logro de la formación y capacitación especializada, científica*

[92] Este interrogante fue planteado de manera irónica por algunos medios de comunicación como "La Izquierda Diario" al sostener que a través de la política de seguridad desplegada por Patricia Bullrich y el gobierno porteño de Horacio Rodríguez Larreta *"el gobierno macrista en estos temas gusta seguir como sombra al cuerpo los pasos del Gran Hermano Imperial. Estados Unidos, por decisión de Donald Trump utiliza desde el año pasado en la frontera con México, la misma tecnología contra los migrantes*". Por eso, desde el medio se busca afirmar que las políticas de seguridad del país pretendan ser iguales que las de Estados Unidos debido a la cercanía manifestada entre ambos gobiernos mientras Macri y Trump eran presidentes. Véase http://www.laizquierdadiario.com/El-Gran-Hermano-macrista-mantuvo-6-dias-preso-a-un-hombre-pero-fue-un-error

y técnica general procurando siempre su contenido humanístico, sociológico y ético". Por lo que se debe entender que, al menos en teoría, la capacitación del personal de las fuerzas de seguridad incluiría formación respecto a la privacidad e intimidad de la población y por ende al manejo de su información personal. Sin embargo, como se ha mencionado a lo largo de la tesis, las fuerzas de seguridad se caracterizan por su opacidad tanto en su preparación como en su operatividad escapándose del control y supervisión civil.

Ahora bien, otro interesante efecto detectado de la práctica de poder se centra en el rol de las fuerzas policiales encargadas de la operación y manejo del sistema de reconocimiento facial y de las bases de datos de la población.

Retomando el capítulo dos de esta tesina es conocido que a nivel global se ha producido un fuerte proceso de tecnologización de las fuerzas policiales, pero, ello no implica necesariamente que sus integrantes hayan recibido la preparación correspondiente para utilizarlas sin cometer equivocaciones.

Esta investigación no ha podido encontrar el manual de procedimiento de los Centros de Monitoreo Urbano utilizado por las fuerzas de seguridad, pero, el análisis del caso de Ibarrola permite concluir que tanto los errores y manejos humanos inadecuados de las bases de datos, así como la opacidad propia de las fuerzas de seguridad supone una violación del Artículo Nº75 de la Ley Nº5.688 que establece que la innovación e incorporación de nuevas tecnologías a las fuerzas policiales tiene el objetivo, entre otros, de mejorar la gestión institucional y la transparencia de la fuerza. Contrariamente a lo manifestado en el artículo esto no parece ocurrir actualmente en CABA.

El efecto de la práctica de poder también permite observar que el despliegue y uso de las nuevas tecnologías de vigilancia y control no sólo generan una tensión con el derecho a la privacidad e intimidad de la población argentina sino que, en ocasiones, las legislaciones que buscan garantizar estos derechos, como aquellas que buscan regular el funcionamiento del sistema de reconocimiento facial y videovigilancia son pasadas por alto por parte de las fuerzas de seguridad en el espacio público, como se vio replicada en los casos de análisis. En ambos existió una violación a la Ley N°25.326; una de las mayores legislaciones de Argentina en cuanto a la protección de los datos personales donde uno de los ejes centrales es la protección integral de los datos personales de la ciudadanía. El cuerpo de la ley deja en claro que debe existir un manejo respetuoso y cuidado de esta información, y que los datos deben ser exactos y actualizados, lo que desafortunadamente no sucedió en ninguno de los casos analizados en este capítulo. Esto también se evidencia respecto de la tensión generada en cuanto a los

derechos de privacidad e intimidad presentes en el resto de las normativas nacionales y de CABA mencionadas previamente.

Cabe mencionar otro efecto de poder vinculado a las legislaciones y la operación de las fuerzas de seguridad a través de estas tecnologías digitales que apunta a que la respuesta que ejecutan a dichas amenazas parece excesiva. Recordemos que legislaciones como la Ley N°2.602 de CABA establece que el funcionamiento de estas tecnologías deberá basarse en los principios jurídicos de proporcionalidad y razonabilidad de acuerdo con el delito que se busca combatir o prevenir. Sin embargo, en los dos casos examinados se observa que el despliegue de medios técnicos y humanos parece un tanto desequilibrado en comparación a la peligrosidad del supuesto criminal. Ello se contempla con claridad, sobre todo, en el caso Holway cuyo supuesto delito había sido aclarado y el mismo no representaba una situación de amenaza para la convivencia social, pero, desde la Policía de la Ciudad se accionó recurriendo a una de las tecnologías más modernas con las que cuenta la fuerza de seguridad. Por lo tanto, uno de los efectos de la práctica del poder a destacar es la respuesta desmedida y desproporcionada de las fuerzas de seguridad en la sociedad de control ante escenarios que no parecen necesitar una respuesta tan exacerbada. Aquí parece oportuno utilizar la analogía *"matar a una mosca empleando una bazuca"*[93] aunque, tampoco se puede descartar la posibilidad de que la respuesta de las fuerzas haya sido calculada en un intento de mostrar su accionar, como práctica de espectacularidad para luchar contra la inseguridad, reclamo constante y central de los vecinos porteños.

Analizando los casos se evidencia otro efecto de las prácticas de poder referidas al aspecto legislativo de la problemática. El despliegue de las nuevas tecnologías y modalidades de vigilancia han proporcionado una tensión y, en ocasiones, han llevado a la violación de las legislaciones ya sea en la regulación de su funcionamiento como de aquellas establecidas para proteger el derecho a la privacidad e intimidad de la ciudadanía. El uso del reconocimiento facial; en ambos casos, supuso una violación de las normas nacionales como de las establecidas por la propia Ciudad Autónoma de Buenos Aires. El análisis realizado en este trabajo permite suponer que el despliegue de este sistema en otros espacios geográficos de la Argentina también supondría una tensión respecto a las regulaciones nacionales, provinciales y municipales de esos territorios que buscan proteger la privacidad de sus habitantes.

[93] Frase utilizada para analizar casos jurídicos donde hay clara desproporción en el costo-beneficio de la aplicación de normas.

Indudablemente, se puede observar que este efecto también tiene su correlato en otros países del mundo (abordados en este trabajo de investigación), en los cuales, se ha observado que el despliegue del reconocimiento facial en China y Estados Unidos ha provocado graves consecuencias en sus sociedades generando un perjuicio hacia la privacidad de su ciudadanía. Por ende, se puede percibir que su uso masivo implica siempre un grave riesgo hacia la privacidad, independientemente de la ideología o geografía en la que son desplegadas.

En el análisis realizado se observa otro efecto de la práctica de poder y se refiere a los ataques que puede sufrir la honra, la reputación, la imagen, la identidad e incluso, la dignidad de un ciudadano, lo cual cabe recordar, se encuentra regulado en el Artículo Nº52 del nuevo Código Civil y Comercial.

En el caso de Ibarrola, su identificación y detención errónea ha supuesto un ataque no sólo respecto a su derecho a la privacidad sino también a su reputación y honor al ser considerado por parte de las fuerzas de seguridad del Estado como un criminal peligroso. Aunque posteriormente (seis días más tarde) el Estado se percató y rectificó su error, el daño al ciudadano fue un hecho. Si bien a través de la cobertura mediática que tuvo el caso se ha buscado "limpiar" la imagen del individuo y sostener su inocencia atribuyendo su detención a errores humanos en la operación del sistema de reconocimiento facial, no es posible afirmar que todos los integrantes de la población se convencieran de su inocencia por lo que el prejuicio y las sospechas sobre su detención pueden continuar latentes. El recuerdo de la experiencia traumática vivida puede perdurar en su memoria ya que él mismo reconoció que podrían *"haberle arruinado la vida",* situación que no se borra con una simple disculpa por parte de las autoridades. En este sentido, el error cometido ocasionó que el nombre de Ibarrola fuese difundido masivamente siendo objeto de conjeturas mediáticas por medios locales, nacionales e internacionales provocando daño a su imagen lo que también puede conllevar una violación a su derecho a la intimidad y privacidad al ver replicada su historia por parte de los medios de comunicación. Entonces, es posible sostener que la implementación de nuevas tecnologías y prácticas propias de la sociedad de control genera efectos de poder como el ataque a la reputación, la honra y la imagen de la ciudadanía además de la tensión que supone con el derecho a la privacidad e intimidad de los sujetos.

3.2. Los (efectos en) medios y sus efectos

Existe otro efecto de las prácticas de poder el cual se puede identificar en las coberturas periodísticas destinadas a los casos analizados.

En esta tesina se ha ahondado en torno al rol de los medios de comunicación y su protagonismo respecto a la práctica de gubernamentalidad denominada "política del miedo". Se ha remarcado

cómo los medios de comunicación pueden actuar siendo aliados estratégicos del poder político de turno para lograr persuadir a través de sus coberturas periodísticas a la ciudadanía para que ella reconozca o incluso solicite la implementación de tecnologías de vigilancia y control cada vez más avanzadas.

A pesar de ello, en la cobertura periodística de los casos abordados en este análisis se observó que todos los medios de comunicación tomaron una postura llamativa poniéndose del lado de las víctimas y considerando (aunque en la mayoría de los casos de forma mesurada) los errores humanos que han llevado a las detenciones equivocadas de ambos ciudadanos. Sin embargo, también se han encontrado importantes diferencias discursivas entre los medios más y menos afines al gobierno de turno.

Respecto de los medios de comunicación más afines al gobierno macrista como "Clarín", "Infobae" y "TN", estos buscaron reflejar en sus coberturas periodísticas la necesidad de implementar el reconocimiento facial y los impactos "positivos" que esta tecnología aporta en la lucha contra la inseguridad, aunque esto se realizó sólo moderadamente y recurriendo a citas textuales de los funcionarios del gobierno de la Ciudad. Y, si bien han demostrado cierto nivel de critica acerca de los errores que llevaron a las detenciones, respaldaron la continuidad en la operación del sistema. Es importante resaltar esta situación ya que tanto Clarín como Todo Noticias son dos de los principales medios de comunicación de Argentina y su importancia en el panorama de medios se ve acentuado no sólo por la enorme audiencia a la que llega su contenido sino al hecho de que otros medios de comunicación pueden escogerlos como fuente informativa a la hora de construir sus propias noticias, transmitiendo entonces, total o parcialmente, la postura que adopta el medio sobre el tema. Cabe destacar que ambos medios forman parte del mismo grupo mediático por lo que su visión en torno a la temática tendrá muy fuertes similitudes que se vio reflejado en sus coberturas periodísticas.

Al analizar la operatoria mediática presente en ambos casos se observa que la responsabilidad de la detención de los ciudadanos recae en el sistema de reconocimiento facial que opera en CABA, y no debido justamente a errores técnicos sino humanos, propios de la impericia o desidia de los funcionarios judiciales y policiales encargados de las bases de datos y del manejo de la información de la población. De hecho, las coberturas mediáticas de los casos por parte de los medios oficialistas otorgan importancia al sistema de reconocimiento facial por su capacidad de actuar frente a la criminalidad en el espacio público y recuperan las voces de los funcionarios que reconocen el valor de esta tecnología aplicada a la Policía de la Ciudad.

Sin embargo, como se ha visto durante el recorrido del capítulo, los casos también recibieron una cobertura de medios de comunicación cuya línea discursiva se encuentra en clara oposición

al gobierno de Mauricio Macri como “La Izquierda Diario”, “Página 12” o el canal ruso “RT”, los cuales han mostrado un grado mayor de crítica hacia el manejo del reconocimiento facial por parte de las fuerzas policiales de CABA alzando una fuerte crítica contra el sistema y las nuevas modalidades de vigilancia y control implementadas por el gobierno de la Ciudad.

Entonces, cabe la siguiente pregunta: ¿las críticas realizadas a la implementación del reconocimiento facial y a su operatividad son formuladas bajo una genuina preocupación por la privacidad de la ciudadanía o constituyen una crítica a las políticas en materia de seguridad establecidas por “Juntos por el Cambio”?

Si bien sabemos que los medios de comunicación no son meras cadenas de transmisión de discursos producidos por el gobierno no es un secreto que se puedan producir alianzas entre ambos para transmitir discursos que corresponden a la práctica de gubernamentalidad en lo relativo a temas sobre la seguridad interna como el terrorismo o la criminalidad. Estos discursos apuntan a ser transmitidos a la mayor cantidad posible de población y es aquí donde se vuelve a destacar la participación de medios como” Clarín” o “Todo Noticias” quienes forman parte de grandes conglomerados mediáticos y posibilitan la llegada a enormes sectores de la población. Cabe destacar que el análisis de los casos retomados para esta tesina refleja que la cobertura mediática del caso de Rachel Holway ha registrado una mayor cantidad de menciones respecto a las afectaciones que el despliegue del reconocimiento facial conlleva para la privacidad de la ciudadanía en comparación al caso de Ibarrola en el cual la mención con respecto al derecho de la privacidad e intimidad de la población es mucho menor por parte de los medios.

4. Similitudes y diferencias entre los casos de Estados Unidos, China y Argentina

Para profundizar en el estudio de los casos de la Ciudad Autónoma de Buenos Aires en el marco de la expansión de la sociedad de control como configuración de poder a nivel global, es pertinente que se pongan los casos en diálogo con respecto al escenario que atraviesan Estados Unidos y la República Popular China en torno a la temática de vigilancia sobre sus poblaciones.

Recordemos que tanto en estas dos potencias como en Argentina se ha implementado la nueva doctrina de seguridad que permite a los gobiernos instalar una vigilancia permanente y exhaustiva sobre los sujetos buscando identificar y neutralizar cualquier “amenaza” que surja desde el interior de las sociedades y pueda hacer peligrar la convivencia social. Sin embargo, esta doctrina implica realizar una vigilancia constante y muchas veces invisibilizada sobre la población por parte de las fuerzas de seguridad, aun, cuando no existan causas que justifiquen dicho accionar.

Realizando un paralelismo entre los tres países se observa que la aplicación de tecnologías de vigilancia y control social, como los sistemas de reconocimiento facial utilizados por las fuerzas de seguridad, se han convertido en un factor común en las sociedades actuales permitiendo establecer una vigilancia constante en los espacios públicos generando que toda la ciudadanía sea susceptible de ser identificada y controlada.

Esta acción remite a lo expuesto por Lío (2015) en el primer capítulo de este trabajo de investigación quien sostiene que el desarrollo de tecnologías de vigilancia y su aplicación al entorno público puede ser interpretado como una nueva expresión del poder panóptico en las grandes metrópolis contemporáneas.

Si bien, el estar a la vanguardia del desarrollo técnico y tecnológico les permite a las naciones, en especial, a las superpotencias mundiales mencionadas incorporar tecnologías de reconocimiento facial en cada uno de los integrantes que componen las fuerzas de seguridad (como en el caso de China) esto conlleva un control a escala mayor que en otras naciones.

Al tomar a Estados Unidos y a China como países que ejemplifican la puesta en práctica del nuevo paradigma de seguridad, no debe omitirse una diferencia importante que ellos poseen con la realidad argentina. Tanto en China como en Estados Unidos se emplean las tecnologías de control y vigilancia para realizar un control sobre el conjunto de poblaciones enteras, como en el caso de la ciudadanía china que se encuentra inmersa en el sistema de *"ranking de seguro social"*. Sin embargo, como se ha observado, la aplicación de estos sistemas de control y vigilancia también son utilizados para vigilar grupos y poblaciones específicos, en el caso de China, el control férreo es sobre la minoría islámica de la etnia Uigur en la región de Sinkiang, lo que ha provocado que la organización internacional Human Rights Watch denunciase al gobierno chino por la creación de banco de datos biométricos para identificar a los miembros de la etnia considerada como disidente. Este fenómeno también se replica en Estados Unidos que en 2019 ha implementado la aplicación de sistemas de reconocimiento facial en sus fronteras, política llevada a cabo por la Agencia de Aduanas y Protección Fronteriza como una medida para monitorear la entrada y salida de territorio estadounidense, pero, sobre todo, para controlar la migración ilegal en la frontera sur del país.

La aplicación de estas medidas puede llevar a una estigmatización de las poblaciones migrantes, en especial, aquellas provenientes de las naciones latinoamericanas. No se debe olvidar que su aplicación se produce en un contexto en el cual el entonces presidente norteamericano, Donald Trump ha dado fuertes discursos catalogando a los inmigrantes centroamericanos como "ladrones y violadores". Por lo tanto, la aplicación de estas tecnologías de control en las fronteras se encuadra en un discurso político racista y xenófobo proveniente del oficialismo estadounidense.

Hasta el momento, en Argentina no se ha registrado que el uso de tecnologías de reconocimiento facial vaya dirigido puntualmente a un grupo social, cultural o religioso que habita en la Ciudad Autónoma de Buenos Aires. Pero, como se ha sostenido previamente, la

aplicación de estas tecnologías de vigilancia y control es muy reciente en el país y no ha sido aplicada de forma tan masiva como ha ocurrido en las potencias mundiales mencionadas.

Conclusión

En el último capítulo de esta tesina de investigación se abordaron dos casos puntuales los cuales fueron analizados minuciosamente: el de Rachel Holway y el de Guillermo Federico Ibarrola, ambos detenidos por error en la Ciudad Autónoma de Buenos Aires debido a fallas humanas en el sistema de reconocimiento facial.

El capítulo seis de esta tesina ha descripto detalladamente cada caso en particular haciendo énfasis en el análisis de la cobertura mediática recibida por parte de los medios oficialistas y opositores. También se ha realizado un análisis exhaustivo con respecto a las legislaciones locales y nacionales que entran en tensión. En este sentido, los casos ocurridos en el 2019 demuestran cómo la implementación del sistema en el espacio público tensiona la normativa nacional y local destinada a proteger el derecho a la privacidad e intimidad de la población. Tanto un caso como el otro han recibido una extensa cobertura mediática por medios locales nacionales e internacionales[94].

El despliegue del sistema de reconocimiento facial como tecnología de control y vigilancia masiva no sólo es catalogada como un instrumento propio de la sociedad de control, sino que, además, responde al nuevo paradigma de seguridad del siglo XXl el cual establece una vigilancia permanente sobre la población existan o no causas que la ameriten.

Este estudio ha permitido descubrir múltiples efectos que resultan de las prácticas y ejercicios de poder. Uno de ellos se revela en relación con las legislaciones que buscan proteger y garantizar los derechos fundamentales de la ciudadanía. Existe un avance de las prácticas de vigilancia vinculadas a las tecnologías digitales sobre las legislaciones que resguardan el derecho a la privacidad e intimidad siendo algunos más notorios como lo es la violación a los principios de razonabilidad y proporcionalidad y el descuido respecto a los manejos de las bases de datos e informaciones sensibles de la población, lo que supone justamente, la violación a su privacidad.

Existe otro efecto que produce la aplicación del reconocimiento facial y se refiere a la afectación de la honra, la imagen y la reputación de los ciudadanos incorrectamente identificados por el sistema. Entonces, se puede afirmar que la implementación de estas

[94] Sobre esto último, cabe mencionar que el uso de las nuevas tecnologías digitales posibilita que todos los medios de comunicación tengan un alcance global.

tecnologías y prácticas de control no sólo conlleva avances sobre la privacidad, sino también sobre otros aspectos inalienables en la vida de los individuos.

Sin lugar a duda, este capítulo encontró un efecto de poder producido a raíz de las nuevas prácticas de vigilancia de las fuerzas de seguridad implementadas en el espacio público. Uno de los que se logra visualizar con más claridad es la falta de transparencia y control civil que caracteriza el funcionamiento de las fuerzas de seguridad, en especial referido a los encargados del manejo de la base de datos y a los efectivos que operan este sistema de vigilancia. Esto se comprueba en los casos presentados: sus detenciones se producen debido a errores humanos de funcionarios policiales y judiciales, pero, dado el marco de opacidad y secretismo que caracteriza su funcionamiento, no se ha podido encontrar finalmente al responsable lo que conlleva a violaciones de las leyes que resguardan la privacidad de la población, ni se han podido conocer medidas reparatorias que se le brindarán a los ciudadanos afectados. Por lo tanto, este efecto demuestra que no sólo en CABA se ha incorporado un sistema de vigilancia masivo, sino que el mismo dispone de mecanismos que escapan al monitoreo civil generando más dudas que certezas en torno al proceso de formación y operación cotidiano de los responsables de estas nuevas tecnologías.

Existe otro claro efecto de la práctica de poder y es el fuerte avance en la capacidad de actuación de las fuerzas policiales cuyo accionar viola las legislaciones establecidas bajo la premisa de generar sociedades más seguras.

Y finalmente, también se observan los efectos de la práctica del reconocimiento facial en relación con el tratamiento mediático dado a los casos. La cobertura mediática al respecto se presenta como dividida más allá de coincidir en señalar los errores detrás del accionar policial en cada caso. De este modo, los medios más afines al gobierno de turno defienden las medidas como mecanismos para garantizar la seguridad de la población, mientras que los opositores critican la implementación de estos sistemas y alertan sobre las consecuencias que este accionar supone sobre los derechos de la ciudadanía.

Tanto los medios de comunicación oficialistas como opositores muestran una actitud de apoyo hacia los ciudadanos sosteniendo que los errores que provocaron las detenciones se debieron a fallas humanas y no a errores técnicos propios del sistema de reconocimiento facial, aunque, en la mayoría de los casos, esta postura ha sido transmitida en forma mesurada. Los medios opositores al gobierno porteño han realizado una cobertura de los casos con una postura mucho más crítica hacia la implementación de las nuevas tecnologías de vigilancia y control que hacen a la nueva política de seguridad de CABA, considerando que las mismas no sólo son tecnologías de control masivo, sino también un sistema de vigilancia “orwelliano”. Se puede

remarcar así el rol que poseen los medios de comunicación al convertirse en aliados estratégicos de los gobiernos de turno ya que, es a través de sus coberturas periodísticas que la práctica de gubernamentalidad, actúa en la sociedad generando que la misma ciudadanía exija su implementación masiva.

En relación a las coberturas periodísticas, cabe preguntarnos si las fuertes críticas a la implementación del reconocimiento facial en el ámbito de la Ciudad realizadas por los medios de comunicación que poseen una línea editorial contraria al gobierno nacional y al de CABA, corresponden realmente a un interés legítimo y genuino hacia la protección de los derechos a la privacidad e intimidad de la población o si, por el contrario, el ataque a las nuevas medidas implementadas por la política de seguridad de CABA se debe más a una identificación de estos medios con los partidos políticos opositores al gobierno de turno. Es preciso recordar que los casos de análisis de este trabajo ocurrieron a mediados del año 2019, año en el cual, Argentina realizó elecciones presidenciales y legislativas en un marco de gran polaridad política y posturas divergentes en múltiples temas entre las que la seguridad fue uno de los ejes de las campañas electorales. Por lo tanto, no es descabellado sostener que los medios opositores podrían haber hecho uso político de los casos de Holway e Ibarrola con vistas a favorecer a determinados candidatos.

El análisis de ambos casos permite observar el despliegue e instrumentación de este sistema y modalidad de vigilancia en el entorno público por parte de las fuerzas de seguridad, su forma de utilización y los efectos de dicho ejercicio del saber-poder, lo que es a su vez, resultado del proceso de tecnologización experimentado por las fuerzas policiales.

Los hallazgos encontrados en este capítulo permiten observar mecanismos de control presentes en el espacio público de CABA que hacen a la configuración de un panóptico digital, el cual supone la vigilancia y control masivo de la ciudadanía existan o no causas para ello. El reconocimiento facial, como nueva tecnología de vigilancia, y las modalidades de control desplegadas por las fuerzas de seguridad en la Ciudad ha provocado que en el espacio público se desarrolle una vigilancia constante que opera de manera casi imperceptible a los ojos de la población, pero cuya presencia y operación les provoca un cierto condicionamiento a sus prácticas cotidianas.

Todos estos elementos ayudan entonces; a avanzar en la comprensión de estas prácticas específicas dentro del marco de las estrategias de gubernamentalidad propias de la sociedad de control y vigilancia. Estrategias de saber-poder que buscan poco a poco configurar una situación de "guerra preventiva interna" modulándola en torno a su normalización en la figura de una experiencia cotidiana. Por lo tanto, luego de percibir los efectos de las prácticas de poder

mediante el análisis presentado se puede notar que la aplicación de las nuevas tecnologías de control y vigilancia como el reconocimiento facial en CABA, efectivamente implica una tensión y violación de las legislaciones nacionales y locales para la protección de los derechos de la privacidad e intimidad.

Si se retoma el contenido plasmado en el capítulo tres, el análisis de los casos de CABA en 2019 permite ilustrar las características particulares que adopta en este territorio el fenómeno de la vigilancia masiva cuya implementación ha sido uno de los elementos clave que establece el nuevo paradigma de seguridad del siglo XXl. De este modo, analizar estos casos permite observar en la Argentina una realidad propia aunque con fuerte rasgos de similitud a lo que sucede en países como China y Estados Unidos, entendiendo que, si bien los países pueden experimentar diferencias políticas, culturales, regulatorias e ideológicas , en la mayoría de las naciones del mundo se vislumbra un avance de las sociedades de control cuyas formas de ejecución pueden variar de acuerdo al contexto, pero que, sin embargo, en todos los casos, se observa un avance hacia el derecho de la privacidad de la ciudadanía.

En este capítulo también se ha realizado una comparación entre la actual situación de China, Estados Unidos y Argentina en lo referido a la implementación del reconocimiento facial en sus sociedades. Si bien en las tres naciones se ha comenzado a implementar este sistema por parte de los integrantes de las fuerzas de seguridad, es en las dos superpotencias mundiales donde se contempla un uso mucho más extendido y generalizado, tanto que incluso, se lo destina al control y vigilancia de grupos específicos de la sociedad como ya se ha mencionado. Contrariamente, en la Argentina esta tecnología no parece estar destinada al control de poblaciones específicas, aunque, en general, no se descarta que su aplicación puede suponer no solamente una violación de la privacidad sino también la posibilidad de que sea empleada con fines discriminatorios e incluso persecutorios de grupos específicos como los mencionados anteriormente.

Para finalizar, retomemos por un momento más los casos estudiados en este trabajo. Contemplar especialmente el caso de estos dos ciudadanos de CABA ha permitido individualizar e identificar con nombre y apellido sus historias personales, (lo que en muchas ocasiones no ocurre cuando se habla de políticas públicas como la seguridad, donde la población es considerada solamente una cifra).

De esta forma, se puede concluir que en lo que respecta a las prácticas y tecnologías de videovigilancia y al accionar vinculado a ellas por parte de las fuerzas de seguridad, como la materialización de aristas fundamentales de la sociedad de control, en los casos relevados de

CABA es el Ministerio de Justicia y Seguridad de la Ciudad el que reconoce un 4% de falencias en el sistema, aunque afirma que ello se debe, en buena medida, a falencias en la carga de datos. Sin embargo, los casos relevados ayudan a evidenciar que todos los ejercicios de saber-poder de estas prácticas de control y vigilancia se realizan mayormente de forma desproporcionada entrando en tensión con la regulación que los habilita ignorando, omitiendo o directamente violando lo que corresponde a la privacidad e intimidad, honra e imagen de los ciudadanos.

Conclusiones generales

1. Recorrido realizado

Llegando al final del recorrido de este trabajo de investigación es necesario enfocarse en las conclusiones generales recuperando los conceptos presentados en el capítulo uno: sociedades de control, control social y panóptico digital.

El abordaje de nuestro primer capítulo demuestra que nociones que parecían propios de otros períodos históricos, como el caso del panóptico, vuelven a entrar en escena debido al desarrollo de novedosas tecnológicas digitales y prácticas vinculadas, generando una vigilancia que no sólo se ha tornado mucho más sofisticada por el veloz avance científico-tecnológico, sino que parece estar prácticamente invisibilizada a los ojos de la población.

Estos ejes fundamentales, ya expuestos ampliamente, entran en diálogo y se enlazan con otros conceptos transversales presentados en los capítulos dos y tres como política del miedo o fuerzas de seguridad, los cuales permiten comprender el fenómeno de la implementación de las nuevas tecnológicas de control y vigilancia masiva en las sociedades actuales.

En el capítulo dos se recuperó el proceso de tecnologización experimentado por las fuerzas de seguridad a nivel global, lo que ha dado como resultado el surgimiento de nuevas modalidades y tecnologías de vigilancia que reformularon el rol de las fuerzas de seguridad. La implementación de las nuevas herramientas utilizadas para la vigilancia de la ciudadanía posee, como ya se ha mencionado, características técnicas que no sólo logran la individualización de los ciudadanos a través de sus rasgos físicos, sino que, además, representan graves riesgos sobre los derechos inalienables de las personas como lo es la privacidad.

El tercer capítulo ha colocado su mirada sobre dos de las principales potencias del mundo: China y Estados Unidos. Esta observación permitió contemplar cómo la sociedad de control posee una configuración global en el mundo contemporáneo donde la implementación de nuevas tecnologías de control y vigilancia como el reconocimiento facial suponen graves riesgos para la privacidad de la sociedad en su conjunto y también para grupos sociales específicos de la población. Aquí se recuperaron conceptos importantes para comprender la implementación de la vigilancia masiva en las sociedades de control. Uno de ellos es el cambio en el paradigma de seguridad del siglo XXl y la práctica de gubernamentalidad denominada "política del miedo", esta última fuertemente relacionada a los procesos de tecnologización de las fuerzas de seguridad de las sociedades contemporáneas.

El uso masivo del reconocimiento facial en las principales potencias y la progresiva implementación de este sistema en la Argentina torna necesario el estudio de las legislaciones

y normativas que operan en nuestro país y que están destinadas a salvaguardar los derechos de la población frente a su implementación. Por lo tanto, el capítulo cuatro avanzó sobre el tratamiento y definición de los derechos fundamentales de la ciudadanía para lograr comprender la problemática de la implementación de estos sistemas y los riesgos que representan para sus derechos esenciales. Es justamente la privacidad uno de esos derechos. Su definición es una de las metas primordiales de este capítulo que demuestra las diversas etapas que ha atravesado en la Argentina hasta llegar finalmente a la tercera en la que se establece un fuerte vínculo con el de la información personal como resultado de la penetración de las tecnologías digitales en la vida diaria de los sujetos.

Esto se relaciona directamente con lo expuesto en el primer capítulo donde se presenta el concepto de capitalismo cognitivo y la gran importancia que pasan a tener los datos de la ciudadanía tanto para el sector público como para el privado, los cuales buscan acceder a ellos a través de prácticas lícitas o ilícitas yendo en detrimento de la privacidad de los sujetos. Aquí también se trataron las leyes establecidas a nivel nacional cuyos objetivos apuntan a proteger el derecho a la privacidad e intimidad de las personas. Asimismo, se observó la regulación del funcionamiento del sistema de vigilancia en suelo argentino y la necesidad de realizar una renovación y actualización profunda de las normativas vinculadas a estos temas, sobre todo, las legislaciones destinadas a la protección de datos personales. El conocimiento de estas normas permitió avanzar en un análisis más minucioso y profundo con respecto a la implementación y operación del sistema de reconocimiento facial.

El capítulo cinco se ha centrado puntualmente en la Ciudad Autónoma de Buenos Aires y en la operación del sistema de reconocimiento facial en este espacio público en el 2019, su funcionamiento cotidiano y las respectivas características técnicas/tecnológicas propias que permiten la identificación y el seguimiento de la ciudadanía por parte de las fuerzas de seguridad y el rol ejercido por ellas en el marco de la sociedad de control actual.

Se hizo hincapié en la operatividad de dichas fuerzas encargadas del manejo del sistema en los Centros de Monitoreo Urbano (CMU), y se trazó un puente con el capítulo dos al presentar el rol de las fuerzas de seguridad las cuales, en este marco de control, están registrando un fuerte proceso de tecnologización.

Paralelamente se analizaron diferentes posturas: algunas a favor y otras en contra sobre este sistema en CABA. Se trataron las legislaciones específicas referidas a la operación de los sistemas de reconocimiento facial y videovigilancia en la Ciudad, así como aquellas destinadas a proteger el derecho a la privacidad de la ciudadanía porteña. Ello permitió desmenuzar con

mayor precisión los casos elegidos para este trabajo: el de Rachel Holway y Guillermo Federico Ibarrola que se detallan en profundidad en el último capítulo.

Finalmente, el sexto capítulo de este trabajo de investigación realizó un análisis específico de las detenciones de los ciudadanos ya mencionados. Aquí se estableció un hilo conductor entre los conceptos presentados a lo largo de toda la tesina enfatizando la tensión provocada entre privacidad y vigilancia debido a la implementación de tecnologías propias de la sociedad de control como el reconocimiento facial.

Este capítulo retomó legislaciones abordadas en los capítulos cuatro y cinco y las analizó en base a los casos seleccionados de manera que, se observa cómo las legislaciones y normativas tanto nacionales como locales son avasalladas por las nuevas tecnologías y modalidades de control y vigilancia a cargo de las fuerzas de seguridad.

También se observó el rol de los medios de comunicación en relación con la práctica de gubernamentalidad mencionado en el segundo y tercer capítulo al enfocar la cobertura mediática que los casos de análisis recibieron y el accionar de algunos en defensa del sistema y otros en abierto ataque.

Por último, este capítulo se centró en analizar los efectos que produce la práctica de poder a nivel legislativo y mediático, ofreciendo también una mirada a la producción de efectos a nivel operacional de la Policía de la Ciudad debido a la incorporación de nuevas tecnologías de control social por parte de las fuerzas de seguridad de CABA, entendiendo que estos efectos no solamente condicionan la cotidianeidad de la ciudadanía, sino que suponen un riesgo o directamente la vulneración de los derechos esenciales de la población como la privacidad, derecho a la imagen, honra y reputación de los ciudadanos.

De todo este recorrido surgen tres preguntas que se debieran formular y reflexionar sobre ellas con detenimiento: ¿las fuerzas de seguridad de la Argentina han recibido la correcta instrucción y preparación para utilizar estas nuevas tecnologías de vigilancia?, ¿las bases de datos policiales y judiciales han sido correctamente depuradas de manera que no existan datos erróneos de la ciudadanía que comprometan su privacidad? ¿Puede garantizarse el correcto funcionamiento del sistema en el marco de opacidad y secretismo que caracteriza a las fuerzas de seguridad?

2.Diferentes tiempos, diferentes guerras, los mismos daños: Guerra preventiva y daños colaterales

El abordaje de los diversos ejes conceptuales incorporados a esta tesina invita a distinguir una serie de conclusiones derivadas de la implementación de las nuevas tecnologías y modalidades de vigilancia en el marco de las sociedades de control del mundo contemporáneo.

Cabe destacar el gran entramado de relaciones existentes entre los aparatos estatales, las fuerzas armadas y los servicios de inteligencia. Estas son relaciones permanentes y poco conocidas en la mayoría de los casos por parte de la sociedad civil que establecen una red en donde se produce una mezcla de intereses políticos y económicos tanto en el plano nacional como internacional y una transferencia de tecnología.

Básicamente, el sistema de reconocimiento facial, al igual que muchas otras tecnologías utilizadas en nuestra vida diaria estaban destinadas al sector militar. Paulatinamente se han ido incorporado para el uso de la vigilancia y control de la sociedad civil, por lo que, en la actualidad, se observa una transferencia de tecnología pensada originalmente para la guerra convencional pero que hoy es aplicada a la "guerra preventiva" con el objetivo de combatir las amenazas internas que enfrenta la sociedad.

Este concepto de guerra preventiva que elabora Alcántara (2008) en su escrito se retoma para realizar una comparación entre el concepto de guerra moderna y el de guerra preventiva, entendiendo a esta última como el despliegue técnico y tecnológico que a nivel global llevan a cabo las sociedades de control bajo el argumento de combatir aquellas amenazas internas de las sociedades tales como la criminalidad, el narcotráfico y el terrorismo y establecer una sociedad más segura pero, ejerciendo una vigilancia constante sobre la población, generando que cualquier persona sea susceptible de ser vigilada en cualquier contexto como sostiene Gendler (2017), lo que supone una vulneración a los derechos de la privacidad e intimidad de la ciudadanía.

Como se fue desplegando a lo largo del trabajo, la idea de sociedad de control que opera en el mundo contemporáneo implica establecer una vigilancia productiva constante sobre la población existan o no causas que la ameriten. Esta vigilancia opera bajo la premisa de que el mundo vive en un estado de guerra y peligro constante donde el "enemigo" ahora no sólo proviene desde el exterior sino desde el interior de las mismas sociedades. Una guerra donde ya no es fácil identificar al enemigo, porque en apariencia general, se ve de la misma forma que los "ciudadanos de bien" y, por lo tanto, para lograr identificar y neutralizar estas posibles amenazas, la vigilancia que se realiza en toda sociedad ahora se acentúa y es llevada a límites

insospechados por parte de las fuerzas de seguridad, originando que el conjunto de individuos se convierta en sospechoso. Esto se relaciona a la idea de modulación que aborda el trabajo de Gendler (2017), donde se afirma que el concepto de gubernamentalidad orienta y despliega ciertas pautas para la acción de los individuos de una sociedad y evita la ejecución de otras ayudando a comprender la modulación constante en la existencia de los sujetos.

En este sentido, esta modulación

> *"no sólo representa una continua producción y modificación del cuerpo y subjetividad del individuo sino también la producción y modificación constante de los posibles caminos y acciones a ejecutar de acuerdo con las pautas de normalización válidas en un momento determinado".* (Gendler, 2017, p.10).

Según el autor, en las sociedades de control, tanto las tecnologías de control y vigilancia, las cámaras de videovigilancia, como las fuerzas de seguridad del Estado, entre otros elementos, *"componen, describen y posibilitan las prácticas de control, monitoreo, vigilancia y represión, así como también las producciones de cuerpos, territorios y subjetividades en esta modulación constante".* (Gendler, 2017, p.23).

Si bien esta comparación entre la idea de guerra moderna y guerra preventiva podría parecer que responde a una corriente de pensamiento donde priman los pensamientos tecno-fóbicos y el pesimismo tecnológico en la cual la tecnología es considerada solo por sus efectos negativos sobre la sociedad, es importante refutar esto. No se puede considerar que los adelantos técnicos y tecnológicos aplicados específicamente a los dispositivos de control y vigilancia tales como, las cámaras de videovigilancia o sistemas de reconocimiento facial impliquen únicamente consecuencias negativas para el conjunto de la sociedad, pues, como toda tecnología, su desarrollo y las modalidades de vigilancia implican siempre y de forma inevitable, una serie de condiciones referentes a las relaciones humanas y encierran en forma intrínseca una naturaleza política a la vez que despliegan toda una serie de efectos productivos que ayudan a configurar y modular el mapa social donde los actores se movilizan.[95]

[95] Gendler (2019) retoma esta cuestión al observar el gran avance que han registrado las tecnologías digitales y las tecnologías de la información (TIC) en las últimas décadas del siglo XX en la vida diaria de la sociedad provocando la generación y el despliegue de las posiciones y construcción teórico-prácticas opuestas entre sí en torno al avance y penetración de Internet y de las tecnologías digitales. El autor sostiene que el posicionamiento tecnófilo se remite a un amor a las tecnologías digitales a las que se considera un mecanismo de progreso para la humanidad y una posible solución para los problemas que la aquejan en su sociedad y cultura. Asimismo, Gendler retoma el posicionamiento tecno-fóbico, el cual alerta sobre los riesgos que conlleva el alcance de Internet y de las tecnologías digitales en la cotidianeidad, considerando que la implementación masiva de estas tecnologías representa un peligro para los puestos de trabajo, la democracia, la educación, la libertad y los lazos sociales, entre otras áreas.

El nuevo paradigma de seguridad del siglo XXI establece así una "guerra preventiva[96]" contra las amenazas que puedan surgir de la propia sociedad. Al plantear esta mirada de Alcántara, parece oportuno trazar un paralelismo con la idea de guerra moderna tradicional para demostrar que no existen demasiadas diferencias entre ambos conceptos. En infinidad de ocasiones; fuerzas militares convencionales realizan ataques contra blancos enemigos con el pretexto de que se trata de ataques preventivos contra objetivos potencialmente peligrosos.

En las sociedades contemporáneas ocurre algo similar. Se gestiona al conjunto de la ciudadanía para detectar y neutralizar comportamientos y/o integrantes de la sociedad considerados como "potencialmente peligrosos" y que conforman un riesgo para la convivencia social.

A diferencia de las acciones bélicas modernas, esta guerra preventiva no se pelea con bombas o tanques. Es llevada a cabo con dispositivos y tecnologías que, en buena medida, han nacido del complejo militar industrial el cual ha producido técnicas y tecnologías originalmente destinadas a las fuerzas armadas de las grandes potencias del planeta, como tecnologías de reconocimiento facial o cámaras de videovigilancia pero que, posteriormente, se han trasladado a las fuerzas de seguridad de las sociedades de todo el mundo. Esto ha generado una lógica de tecnologización de las fuerzas de seguridad con el objetivo de combatir el delito y la criminalidad como remarca Lechner (2006) *"(...) Los estados se han tecnificado con métodos y diseños tanto de prevención como de punición contra los delitos".* Sin embargo, esto ha dado como resultado una extensión y consolidación de la sociedad de control a nivel global.

Si continuamos con la comparación entre la guerra preventiva y las operaciones militares convencionales no se puede omitir que, en estas últimas, frecuentemente se habla de "daños colaterales", es decir, población civil muerta o herida como consecuencia del accionar militar para neutralizar un objetivo enemigo. En la "guerra preventiva", propia de las sociedades de control, ocurre algo similar, no con decesos físicos de la población, por supuesto, pero con daños colaterales hacia la privacidad de la ciudadanía como consecuencia de la vigilancia masiva que opera en ciudades como la planteada en esta tesina: CABA.

Puede catalogarse entonces, como "daño colateral" a los casos analizados de Holway e Ibarrola, detenidos por error debido a equivocaciones humanas. Sí, *"daño colateral"* ya que en el esfuerzo de identificar, prevenir y combatir los peligros que *"amenazan a la ciudadanía*", el

[96] Para esta posición, el avance de las nuevas tecnologías aplicadas a la vigilancia de la sociedad supondrá un fuerte riesgo para la libertad de la ciudadanía, entendiendo el derecho a la privacidad e intimidad de la población como factores cruciales para preservar la naturaleza democrática de la sociedad contemporánea, en nuestro caso puntual, el de Argentina.

sistema de vigilancia y control que opera en las ciudades vulnera la privacidad e intimidad de la población.

En los dos casos mencionados se observó una violación de la tercera etapa de la privacidad del ciudadano, porque la idea de privacidad pasa a ser vista como el derecho a que toda información sobre la vida privada de los sujetos que se encuentre en poder del Estado o de grandes conglomerados comerciales no sea utilizada en perjuicio de los intereses del titular de dicha información. Asimismo, se observó una fuerte tensión o directamente, diversas violaciones a las legislaciones nacionales y locales que, en teoría, intentan regular el accionar de las fuerzas de seguridad para que se contemple y respete la privacidad e intimidad de los sujetos.

Al igual que cuando un bombardeo militar mata o mutila a poblaciones civiles surgen voces contrarias con más o menos fuerza para condenar y criticar este accionar y pedir reparaciones de daños, en las sociedades de control ocurre un fenómeno similar. Voces contrarias alertan sobre los peligros y riesgos que conlleva la aplicación de estos sistemas para la privacidad e intimidad de la ciudadanía.

Estas organizaciones no gubernamentales tienen la misión de promover y defender los derechos fundamentales de la población en entornos sociales mediados por la implementación de tecnologías (en nuestro caso específico: tecnologías de control y vigilancia) estableciendo especial énfasis en el seguimiento e implementación de políticas públicas sobre el uso de este sistema sobre la ciudadanía. ONGs como las abordadas, consideran que la posibilidad de ejercer el pleno derecho a la intimidad por parte de la ciudadanía argentina es fundamental no sólo para construir sino para sostener la naturaleza democrática de nuestras sociedades, por lo que es crucial la protección del derecho a la privacidad e intimidad de los sujetos frente a una vigilancia cada vez más compleja que proviene del sector privado y en especial del público en nuestro caso específico. Ciertamente, se llega a la conclusión que es muy importante el rol ejercido por las ONGs, ya que poseen la capacidad de promocionar debates sobre temáticas vinculadas a las tecnologías que impactan en el ejercicio de los derechos humanos en el marco de las sociedades de control.

3.Un escenario global, una obra mundial: vigilancia alrededor del mundo. China, EE. UU. y Argentina

Además de lo relevado respecto de CABA, en la presente tesina se han contemplado puntualmente dos casos buscando darle un marco global a la sociedad de control y videovigilancia: China y Estados Unidos. Es en estos países donde se produce una masiva materialización de la sociedad de control a través del desarrollo e implementación de nuevas

tecnologías y modalidades de vigilancia que suponen una vigilancia masiva y permanente para la población en pos de generar una "sociedad más segura". Este fenómeno de la sociedad de control es observado también en múltiples países a pesar de las diferencias culturales, políticas e ideológicas que presenten.

El uso de las nuevas tecnologías de vigilancia y control ha sido implementado en diferentes países siguiendo una lógica de vigilancia y control constante e invisibilizada en gran parte a los ojos de la población que se mueve por el espacio público, pero, que, al mismo tiempo, es sometida a un control férreo por parte de las fuerzas de seguridad existan o no motivos que ameriten este accionar. A pesar de que la incorporación de estas nuevas modalidades de vigilancia parece más desarrollada y consolidada en países como China y Estados Unidos, progresivamente se observa que su uso también es adoptado por otros países como Argentina. Sin embargo, a diferencia de estas potencias mundiales, el país latinoamericano aún no ha recibido denuncias o críticas de organismos internacionales respecto al empleo del reconocimiento facial con fines discriminatorios o persecutorios de grupos religiosos, políticos o raciales específicos.

4. La configuración de la sociedad de control en CABA

4.1 Configuración técnica

En este trabajo de investigación se puntualizó la aplicación del sistema de reconocimiento facial en la Ciudad Autónoma de Buenos Aires en 2019, especialmente al retomar los casos de análisis de Rachel Holway y Guillermo Federico Ibarrola.

Si bien se investigaron las características técnicas del sistema de reconocimiento facial que opera en CABA y se especificó que el sistema podía presentar errores a la hora de identificar a los ciudadanos debido a factores como iluminación, aditamentos utilizados, no fue ninguno de estos factores lo que provocó la detención de ambos ciudadanos. De hecho, el sistema de reconocimiento facial operó correctamente y el error provino de una desactualización o incorrecto uso de las bases de datos de las fuerzas de seguridad y/o del Poder Judicial del país. Durante el 2019, año en que se realizó esta investigación, este escenario fue constante. De acuerdo con los datos del GCBA, sólo el 18.41**%** de los detectados por el sistema de reconocimiento facial quedaron detenidos acusados de delitos graves mientras que el 81.59% restante fue liberado por el Poder Judicial pero no debido a errores maquínicos del sistema de videovigilancia. Por lo tanto, este escenario conduce a establecer una serie de conclusiones.

El siglo XXl y el cambio en el paradigma de seguridad trajo aparejado un profundo proceso de modernización tanto en las tecnologías como en las modalidades de vigilancia aplicadas por

las fuerzas de seguridad a nivel global, incluida Argentina. Con el fin de incorporar nuevas tácticas para combatir las amenazas internas en la sociedad argentina se observó una fuerte implementación del sistema de videovigilancia y más recientemente, del software de reconocimiento facial.

Sin embargo, al observar en especial el caso de Ibarrola, cabe preguntarse si los integrantes de las fuerzas encargadas de operar las nuevas tecnologías, como las bases de datos de la población, recibieron la formación y capacitación adecuadas para la operación correcta y eficaz de estas herramientas. Desafortunadamente, el marco de opacidad y secretismo que caracteriza la operatividad de las fuerzas de seguridad impide obtener una respuesta efectiva a esta pregunta, ya que, como se demostró en este caso, basta con sólo equivocarse en la carga de un dato para comprometer gravemente la privacidad e intimidad de un ciudadano (como efectivamente ocurrió), donde no sólo implicó el riesgo de comprometer la privacidad sino también la libertad del sujeto.

Situación similar ocurrió con el caso Holway, detenida e imputada por un delito que no representaba una amenaza para la sociedad como estipula la legislación destinada a la regulación del sistema de videovigilancia, Resolución 398/19 del Ministerio de Justicia y Seguridad de la CABA, la cual establece que su funcionamiento debe brindar una respuesta basada en la proporcionalidad a la amenaza que busca combatir.

Contrariamente, en este caso se observa un despliegue por parte de las fuerzas de seguridad que parece sumamente exagerado frente al supuesto delito atribuido. Esta impronta permite considerar que los Estados nacionales, provinciales y/o municipales, buscan demostrar su capacidad de acción y respuesta frente a las amenazas internas de la población para convencer al ciudadano que la implementación de estas herramientas es eficaz para garantizar la protección de la sociedad sea la amenaza de gran envergadura o no.

Como se ha visto, ambos casos registraron una incorrecta detención no debido a fallos técnicos del sistema de reconocimiento facial sino a errores humanos propios de la impericia y el descuido de funcionarios del poder judicial y de miembros de las fuerzas de seguridad en el manejo de las bases de datos e informaciones sensibles y personales de la ciudadanía, lo que supone la consecuente violación de los derechos a la privacidad e intimidad de la población.

4.2 A necesidades desesperadas, ¿medidas extremas? Del rol de los medios y la vigilancia como respuesta frente a la inseguridad.

Al momento de analizar los casos de Holway e Ibarrola, este trabajo de investigación ha realizado un relevamiento en torno a la cobertura mediática que han recibido. Ambos fueron

cubiertos por medios nacionales e internacionales, pero cabe poner en duda si solo el caso de estos dos ciudadanos llegue a concientizar a la sociedad sobre las amenazas respecto de la privacidad e intimidad que pueden implicar estas tecnologías y modalidades de vigilancia.

No debe olvidarse que, en múltiples ocasiones, es la propia ciudadanía, influenciada por el discurso de la "política del miedo" anunciado por la dirigencia política y amplificada por los medios de comunicación que, en oportunidades, realiza una cobertura periodística que se caracteriza por el sensacionalismo, la que solicita el despliegue de más efectivos policiales y mejores mecanismos para combatir estas amenazas, fenómeno que no ocurre solamente en Argentina sino en gran parte del globo.

Es importante remarcar que, como afirman Marcela Muratori y Agustín Salvia en *"Inseguridad ciudadana en la población urbana argentina (2010-2016) del año 2017" (...) "en la Argentina, como en gran parte de los países latinoamericanos, el problema de la inseguridad es un tema socialmente relevante, configurándose como centro de las preocupaciones públicas."* (Muratori y Salvia, 2017, p.7).

Desde hace décadas, la ciudadanía reclama constante y permanentemente una "acción" por parte de las fuerzas de seguridad del Estado y exige que se combatan las amenazas de la inseguridad y del delito, siendo una de las principales peticiones aumentar el número de efectivos policiales en el ámbito público, así como el despliegue de nuevas medidas de seguridad, puntualmente, de cámaras de seguridad, a pesar de los riesgos que esto supone para la privacidad. En este sentido, la construcción de la noticia que sigue una lógica sensacionalista está caracterizada por generar un fuerte impacto social, apelar a la emotividad de la audiencia y poseer la capacidad de despertar un fuerte interés por parte del público en el tema abordado, pero sin llevar a cabo una profundización real del tema en cuestión. Por lo tanto, se puede sostener que la construcción de este tipo de noticia persigue más una lógica vinculada al espectáculo y al entretenimiento que al rigor informativo. Estas características son factibles de identificar en la construcción periodística de las noticias relacionadas a la criminalidad e inseguridad en la Argentina en lugar de alertar en torno a los potenciales peligros que supone la aplicación masiva del sistema de videovigilancia y el software de reconocimiento facial en el espacio público.

Este trabajo ha remarcado el rol de los medios de comunicación y las coberturas periodísticas referidas a la problemática de la inseguridad en el espacio público. Esta problemática es uno de los temas más recurrentes en la construcción de la agenda setting de los medios argentinos, y, por ende, también uno de los principales temas de la agenda pública de la población. Además, se trata de una de las preocupaciones primordiales de las sociedades actuales, no sólo en

Argentina sino a nivel global. La inseguridad es un tema frecuente y a lo largo del registro de las coberturas mediáticas de los casos de análisis se pueden encontrar algunos framing recurrentes en la construcción de la información. Por ejemplo, en el caso de los medios oficiales se reconoce el error en las detenciones de Holway e Ibarrola, pero se remarca la importancia del reconocimiento facial, mientras que en los medios opositores se presenta un framing caracterizado por el sensacionalismo, la ironía y la crítica hacia la nueva política de seguridad implementada por "Cambiemos".

Uno de los principales hallazgos encontrados es la vinculación entre la práctica de gubernamentalidad de la política del miedo y los medios de comunicación para lograr convencer a la sociedad que acepte de buen grado la implementación de nuevas tecnologías de control y vigilancia en el espacio público por considerarlas necesarias. Esto adquiere profundidad al observar cómo los medios oficialistas se convierten en aliados estratégicos del gobierno al avalar y justificar la implementación de las nuevas políticas de seguridad por considerarlas como algo necesario en la generación de sociedades más seguras y combatir así las amenazas internas de la misma. Como plantea el nuevo paradigma de seguridad, son estos medios oficialistas los que remarcan que el sistema de reconocimiento facial funciona correctamente y que las erróneas detenciones de ambos ciudadanos se debieron a errores humanos y no propios del aparato técnico del sistema.

Por su lado, los medios opositores han mostrado un alto nivel de crítica a la implementación del reconocimiento facial en CABA y los efectos adversos que puede suponer hacia los derechos inalienables de la población. Sin embargo, como se planteó en el capítulo seis cabe preguntarse si esta crítica responde a una preocupación genuina por la privacidad de la población o simplemente consiste en un ataque al gobierno porteño basado en diferencias e intereses políticos e ideológicos.

Existe un efecto más que se desprende del análisis de la cobertura mediática a la luz de observar estos casos puntuales y es contemplar que todos los medios analizados acertaron en torno al equívoco y se solidarizaron con ambos ciudadanos, aunque, algunos siguen justificando la implementación de esta tecnología.

Evidentemente, en gran medida las cámaras de videovigilancia y reconocimiento facial son consideradas como la respuesta adecuada a la problemática de la inseguridad en la Argentina. Si se retoman las afirmaciones realizadas en este trabajo, su implementación en el espacio público son el resultado de una política de seguridad en sintonía con el nuevo paradigma de seguridad del siglo XXI, pero, también la respuesta al pedido de la sociedad, que alentados por los discursos de la política del miedo transmitidos por los medios de comunicación aliados al

gobierno de turno reclaman la incorporación de nuevas cámaras para lograr una sociedad más segura.

Esto se corresponde con lo mencionado por Lío (2015) dado que la autora sostiene que *"las cámaras de seguridad se presentan en los discursos políticos y mediáticos como la respuesta a las demandas ciudadanas de seguridad"* (p.16). Y remarca que las cámaras de seguridad aparecen como una de las demandas más crecientes para el combate de la inseguridad llegando a considerarse como "*el quinto servicio público*" (Lio, 2015, p.16) por los vecinos. De hecho, una de las promesas de campaña de Horacio Rodríguez Larreta para ser reelecto como Jefe de Gobierno de CABA en el 2019 ha sido la promesa de incorporar 10 mil nuevas cámaras de videovigilancia con reconocimiento facial como una de las medidas para responder al reclamo de mayor seguridad esgrimidas por los porteños.

De esta manera, se puede contemplar cómo la implementación de estos sistemas aparece en las sociedades contemporáneas como" la respuesta" a las amenazas visibles e invisibles presentes en el espacio público. En el caso puntual de Argentina, estas amenazas internas estarían englobadas en la categoría de crímenes y delitos penales.

Al retomar el análisis de los casos elegidos es necesario remarcar que la incorporación de estas tecnologías, como el software de reconocimiento facial de la Policía de la Ciudad, brinda la posibilidad de llevar a cabo una vigilancia prácticamente invisible a los ojos de la ciudadanía, ejecutando un control permanente sobre la población que, salvando las distancias, podría asemejarse a un "ojo que todo lo ve" ya plasmado en el capítulo uno.

Esta situación plantea el interrogante acerca de la mutación del panóptico en el contexto de las sociedades actuales de control debido al desarrollo y expansión de la infra cultura digital, como lo es la implementación masiva de cámaras de videovigilancia.

Tanto el caso de Holway como el de Ibarrola invitan a analizar el funcionamiento de las modalidades de vigilancia ejercidas por las fuerzas de seguridad en CABA. A partir de este proceso de tecnologización que han tenido las fuerzas de seguridad, la vigilancia a la cual es sometida la ciudadanía es constante y permanente, sin contemplar si un ciudadano tiene motivos legalmente válidos que justifiquen la sospecha sobre él, y, por ende, se aplique la vigilancia para evitar cualquier amenaza al conjunto de la sociedad.

Ambos casos son ejemplificadores de lo que se ha ido postulando a lo largo de esta investigación: la implementación de nuevas tecnologías y modalidades de vigilancia son desplegadas para combatir las amenazas a la "paz y seguridad" en las sociedades modernas.

Preguntamos entonces: ¿qué gravedad de amenaza representaba para la sociedad una causa por supuesta falsificación de documentación? (caso Holway) o ¿la libertad de la ciudadanía será

dependiente de los usos correctos o incorrectos que las fuerzas de seguridad y el aparato judicial hagan de su información personal (caso Ibarrola)?

4.3 Del rol de la legislación

En Argentina se ha producido un fuerte proceso de tecnologización de las fuerzas de seguridad del Estado, extendiendo y amplificando su capacidad de concretar tareas de control y vigilancia de la ciudadanía hasta límites casi insospechados por ella. El análisis de los casos puntuales abordados ha permitido observar una serie de efectos, producto de las prácticas de poder, resultado de la implementación del reconocimiento facial que han afectado a las fuerzas de seguridad. Con respecto a ello se ha hallado un efecto referido a la deficiente o mediocre preparación y capacitación de los miembros de las fuerzas de seguridad y del Poder Judicial encargado de la operación del sistema y de las bases de datos del ciudadano, que deberían procurar ser contemplativos respecto a lo ético y humanístico de la población. Esta posible falta de preparación y capacitación se encuentra en sintonía con otro efecto de poder demostrado en el capítulo seis que remite a la opacidad y secretismo que caracteriza su funcionamiento en el país.

A pesar de que la Ley Nº5.688 establece que la innovación e incorporación de nuevas tecnologías a las fuerzas de seguridad persigue el objetivo de mejorar la gestión institucional y la transparencia de la policía, esto no parece cumplirse en CABA. El uso del reconocimiento facial en la Ciudad, en el marco de la sociedad de control, ha generado una mayor vigilancia y transparencia en la vida de la sociedad civil, pero ha contribuido a crear el efecto contrario en las fuerzas de seguridad, ya que; específicamente la policía de CABA continúa operando bajo un marco de opacidad y secretismo que muchas veces escapa al control de la ciudadanía.

Fundamentalmente, y en sintonía con el aspecto legislativo y regulatorio de la implementación del reconocimiento facial; es necesario mencionar otro hallazgo el cual se centra en la violación de los principios de razonabilidad y proporcionalidad en el uso de las tecnologías para prevenir y combatir delitos y amenazas para la convivencia ciudadana. Sin embargo, el proceso de tecnologización en las fuerzas de seguridad ha expandido exponencialmente sus capacidades de vigilancia sobre la población generando violaciones a las legislaciones específicamente destinadas a regular el sistema de videovigilancia y reconocimiento facial y proteger sus derechos inalienables.

Sin lugar a duda, es posible llegar a conclusiones que se relacionan íntimamente con la legislación argentina y de CABA y que enlaza los casos de Holway e Ibarrola.

Si bien en Argentina existen legislaciones destinadas a regular el funcionamiento del sistema de videovigilancia como la Resolución Nº238/2012 del Ministerio de Seguridad de la Argentina y la Disposición 10/2015 del DNPDP que esclarecen los lineamientos para la captación, almacenamiento y uso de la información recogida por los sistemas de videovigilancia, el análisis de los casos presentados demuestra que muchas veces las legislaciones son pasadas por alto por la operación de las nuevas tecnologías de control y vigilancia, lo que originan una vulneración de los derechos a la privacidad e intimidad de los individuos que estas mismas legislaciones buscan preservar.

Con respecto a otros hallazgos, se encontró que la implementación de las nuevas tecnologías y modalidades de vigilancia genera efectos que involucran no sólo al aspecto legislativo sino a la operatividad de las fuerzas de seguridad, especialmente a la Policía de la Ciudad de Buenos Aires. En este aspecto se ven afectadas las legislaciones nacionales y locales que buscan regularlo y proteger los derechos de la ciudadanía.

Si se observa con detenimiento el análisis de los casos mencionados, asoman faltas y descuidos por parte de las fuerzas de seguridad y de los miembros del Poder Judicial sobre las bases de datos de la ciudadanía y de su información personal. Ello supone una trasgresión a las legislaciones que buscan proteger dichos datos con la consecuente vulneración a la privacidad contemplada en el capítulo cuatro, privacidad fuertemente vinculada a la de datos personales.

Cabe destacar que, si bien el foco de esta tesina señala la violación que supone la implementación del reconocimiento facial respecto a la privacidad e intimidad de la población, no se deben omitir otros derechos como el derecho a la imagen, a la honra y/o a la reputación. Estos derechos mencionados, contemplados y protegidos por las legislaciones nacionales y locales también están en juego y se ven afectados y vulnerados por la incorporación de las tecnologías de control y vigilancia masivas.

Asimismo, no se puede omitir la Ley Nº25.326 de Protección de Datos Personales cuya finalidad es proteger la información personal de la ciudadanía que se encuentra en las bases de datos públicos o privados garantizando su correcto uso y almacenamiento. Aquí se torna urgente comprender la importancia y el cuidado que conlleva el manejo de la base de datos a fin de respetar el derecho innato e inalienable del ser humano a la privacidad. Sobre todo, entender que la sociedad actual está inmersa en un nuevo estadio del capitalismo informacional conocido como “Capitalismo Cognitivo”; donde la reestructuración de la actividad económica ha provocado que el conocimiento y la información se transformen en fundamentos que reorganizan el mundo productivo y social. En este contexto, los datos y la

información personal son elementos cruciales con gran valor para el Estado y para los privados. Ello supone que los datos de la población se convierten en el *"nuevo petróleo*", recurso buscado y anhelado con desesperación por ambos sectores recurriendo a su extracción masiva y/o utilizando prácticas poco transparentes y sin consentimiento o, al menos, conocimiento concreto del proceso por parte de sus titulares.

Este escenario deja en claro la necesidad no sólo de adecuar esta ley, sino también de readecuar otras e incluso establecer nuevas regulaciones que garanticen el derecho a la privacidad e intimidad de la población en torno al manejo de sus datos. La ley N°25.326 ha sido formulada a comienzos del siglo XXl y los intentos de reformularla y actualizarla a la luz de la aparición de las nuevas tecnologías y modalidades de vigilancia y sus usos han sido infructuosos[97]

Indudablemente, las nuevas legislaciones no sólo deberán adecuarse a las prácticas y tecnologías emergentes, sino que, además, deberán ser mucho más rigurosas a la hora de proteger la información de los sujetos.

Es imperioso remarcar, entonces, la necesidad de que exista un consenso entre los diferentes partidos políticos del país, independientemente del partido político que se encuentre en el poder, a fin de actualizar las legislaciones vigentes de protección de datos personales y adecuarlas para que logren resguardar de manera clara y eficaz el derecho a la privacidad e intimidad de los individuos. Y, a su vez, si fuera meritorio, establecer nuevas normativas legales específicas para controlar el funcionamiento de estas tecnologías de desarrollo muy reciente como lo es el reconocimiento facial.

En la recta final de este trabajo de investigación es necesario retomar el concepto de ley para Foucault abordado en el capítulo uno. Para el autor, la ley es un efecto de los ejercicios de poder que genera mapas productivos para que los actores se ubiquen y movilicen en el espacio público, aunque orientando su conducta, pero sin determinarla del todo.

El abordaje de los casos de análisis demostró que existen legislaciones a nivel nacional y local que buscan preservar y garantizar el derecho a la privacidad e intimidad de la ciudadanía estableciendo mapas para su accionar en el espacio público en el presente marco de las sociedades de control. Sin embargo, como se ha demostrado, el despliegue de nuevas tecnologías y prácticas de vigilancia en CABA vinculadas a ellas ha generado violaciones a estas leyes y los efectos de estos ejercicios del poder han cambiado la forma en la cual la ciudadanía se moviliza por la Ciudad. Frente a este escenario se evidencia como imprescindible

[97]Desde su elaboración, la ley N°25.326 de Protección de Datos Personales ha registrado varias enmiendas y, a pesar de los diversos intentos de las distintas dirigencias políticas por adecuarla al contexto actual, nunca ha logrado ser sometida a una reformulación o actualización integral.

la revisión y reformulación de las actuales legislaciones nacionales y de CABA y/o la elaboración de nuevas normativas que se adecúen al marco actual de sociedad de control que atraviesa la sociedad. De esta manera, se plantea la sugerencia de implementar nuevos mecanismos de supervisión y/o mejorar los existentes con respecto a los nuevos dispositivos de control y vigilancia de manera que, el mapa elaborado por las legislaciones actuales que producen y orientan el accionar y los movimientos de la población puedan gozar de medidas y mecanismos de supervisión en el accionar de las fuerzas de seguridad que ayuden a intentar preservar en mayor medida los derechos fundamentales de la ciudadanía frente a los que están desplegados hoy. En resumen, se torna imprescindible establecer nuevas leyes o reformular las existentes con mejores mecanismos de supervisión cuyo objetivo primordial se enfoque hacia la protección de los datos privados e información personal almacenada en las bases de datos del Estado y de privados. Asimismo, también se considera necesario establecer mecanismos efectivos de cumplimiento de las legislaciones actuales donde se determine específicamente los casos en los que el sistema podrá ser empleado por parte de las fuerzas de seguridad. Es importante que se clarifique el modo preciso en que los datos serán captados, almacenados y empleados, estableciendo las consecuencias en caso de que estas disposiciones sean violadas.

Retomemos por unos instantes la idea de guerra preventiva desplegada en esta conclusión. Al igual que en los conflictos militares tradicionales donde los excesos y crímenes de guerra son denunciados, a menudo entran en escena organizaciones no gubernamentales que no responden a ningún gobierno y cuyo grado de independencia les permiten tener un mayor nivel de crítica a la política desplegada.

En el concepto de guerra preventiva desarrollada sucede algo similar y ONG como ADC o Fundación “Vía Libre” toman la palabra buscando alertar sobre los riesgos que supone para los derechos y libertades de la población la implementación del reconocimiento facial. Sin embargo, los discursos de las ONGs formuladas por expertos y académicos del área en cuestión, en ocasiones, es invisibilizada en la sociedad y parecen como voces que gritan en el desierto llegando a oídos sordos. Y es que, la eficacia de la política del miedo es indiscutible a la hora de implementar nuevas modalidades y tecnologías de vigilancia en el espacio público ya que, la población considera que los beneficios que aporta esta política de seguridad en el afán de tener sociedades más seguras son mayores que sus riesgos.

Sin embargo estos gritos y acciones que llevan a cabo las ONGs son realmente necesarios en el marco de las sociedades de control contemporáneos de manera que, poco a poco se empiece a generar en la población prácticas de concientización en torno a los riesgos que supone la

implementación en el espacio público de las nuevas tecnologías de control y vigilancia masiva para los derechos inalienables de la ciudadanía, de manera que en un futuro no muy lejano, esta situación logre ser revertida y las prácticas de seguridad se realicen cada vez en menor medida en desmérito de la privacidad de las personas.

5. Sugerencias, recomendaciones y posibles líneas de acción

Para concluir este trabajo de investigación resta brindar algunas sugerencias que se desprenden de todo lo aquí plasmado con el objetivo único de intentar reducir o eliminar (en la mayor medida posible) los riesgos que supone la implementación masiva de tecnologías propias de la sociedad de control.

Concretamente, se hace necesario adecuar o readaptar las legislaciones establecidas para preservar y proteger los datos personales de la ciudadanía frente a los intentos de recolección del sector público y privado de hacerse con los mismos a como dé lugar. En caso de no ser posible readaptar estas legislaciones sería recomendable la formulación de nuevas leyes que posean la capacidad de adecuarse con flexibilidad y prontitud a las diversas operaciones que buscan hacerse con la información de la población, cuyos intentos pueden provenir de distintos ámbitos de la sociedad.

De igual forma, es importante revalorizar el rol de las ONG, que, especializadas en la problemática de la vigilancia masiva puedan monitorear y vigilar de cerca el accionar de las fuerzas de seguridad respecto al uso de los sistemas de vigilancia masiva. Un control civil claro y transparente permitiría avanzar en torno a proteger los derechos de la población y garantizar la libertad y democracia en el territorio.

Por supuesto que se torna más que imprescindible que los integrantes de las fuerzas de seguridad y los miembros del Poder Judicial dediquen tiempo, esfuerzo y capacidad para recibir la correcta formación, idoneidad, y preparación en el manejo tanto de las bases de datos como del funcionamiento del reconocimiento facial de manera que, las autoridades encargadas del manejo de las modalidades y tecnologías de vigilancia no cometan errores humanos y se muestren respetuosos y contemplativos de los derechos fundamentales de la población.

Finalmente cabe preguntarnos si acaso podríamos estar ingresando a una cuarta etapa de la privacidad e intimidad donde a la luz del despliegue de las nuevas tecnologías empleadas para la vigilancia masiva que conforman la configuración de la sociedad de control en torno al panóptico digital, se genera un choque permanente con las disposiciones establecidas por las regulaciones y legislaciones que buscan garantizar justamente el derecho a la privacidad e intimidad de la ciudadanía provocando que las prácticas policiales terminen ocasionando una

severa vulneración de derechos fundamentales o vitales del ser humano en pos de crear una "sociedad más segura".

Una de las afirmaciones más radicales puede marcar el comienzo de esta nueva etapa y fue pronunciada por el entonces presidente de los Estados Unidos, Barack Obama en el 2013 cuando afirmó "U*no no puede tener un 100% de seguridad y también un 100% de privacidad con cero inconveniencias. Vamos a tener que hacer algunas elecciones como sociedad".*[98]

Por último, y para concluir este trabajo de investigación, se debe rescatar que poco a poco a nivel global comienzan a surgir movimientos civiles que rechazan la implementación del reconocimiento facial entendiendo a esta tecnología como una herramienta para la vigilancia masiva. Algunas ciudades como San Francisco, en los Estados Unidos la han prohibido. Sin embargo, en países latinoamericanos como Brasil, Uruguay y sobre todo en Argentina ocurre lo contrario aun cuando ya es de público conocimiento que su uso no sólo ha sido repetidamente criticado por su falta de eficacia y capacidad para afianzar la discriminación frente a grupos étnicos específicos sino también por la violación a derechos humanos reconocidos internacionalmente.

La gravedad del escenario argentino es de tal envergadura que incluso, el relator especial de la ONU sobre el derecho a la privacidad, Joseph Cannactaci se refirió a la incorporación de cámaras de reconocimiento facial en el país y sostuvo *"Soy consciente de la necesidad de detener a las personas sospechosas de haber cometido delitos y llevarlas ante la justicia pero no veo la proporcionalidad de instalar una tecnología con grandes implicaciones para la privacidad para buscar en una lista de 46 mil personas que altamente incluye menores y delitos no graves y que no se actualice y compruebe cuidadosamente su exactitud".*[99]

6. Lo vimos en el cine, lo vivimos en la calle. La sociedad de control parece una película.

Abrimos este trabajo de investigación comentando la película "*Enemy of the State*" y nos parece oportuno cerrar mencionando otra película, "*Minority Report*" del año 2002 dirigida por Steven Spielberg y protagonizada por Tom Cruise, quien encarna a un policía del futuro que sólo cuenta con 36 horas para probar su inocencia en un crimen que las nuevas tecnologías (en el caso de la película, tres "videntes" interconectados a complejos mecanismos digitales) han predicho que cometerá en el futuro.

[98] Véase https://www.antena3.com/noticias/mundo/gobierno-obama-asegura-que-controles-ciudadanos-traves-internet-son-legales_2013060757472901658 4a8f86268de61.html

[99] Véase https://www.unsam.edu.ar/tss/seguridad-que-invade/

En castellano la película es conocida como *"Sentencia previa*" y sobre este eje nos detendremos para cerrar el trabajo.

El uso de las nuevas tecnologías en el marco de las sociedades actuales ha dado origen a un escenario en el cual la ciudadanía se encuentra sometida a una vigilancia masiva por parte de las fuerzas de seguridad. También nos encontramos ante un escenario de cuasi "justicia preventiva" donde la población parece ser apresada antes de cometer el supuesto delito y, por ende, sin tener conocimiento de las causas que lo llevan a su detención como bien se observó en los casos de Holway e Ibarrola.

Por supuesto que la película "*Minority Report"* es por el momento, solo eso, una obra audiovisual de ciencia ficción y no exactamente el escenario presente que registra CABA. Sin embargo, se observan algunas similitudes entre el film y la realidad estudiada durante el análisis de los casos de Holway e Ibarrola que permite vislumbrar los extremos (siempre y cuando el desarrollo tecnológico lo permita) a los que podría llegar la vigilancia masiva en las sociedades en el marco de las sociedades de control.

La vigilancia constante, así como la idea de justicia preventiva son resultado de la implementación de los desarrollos tecnológicos aplicados a las fuerzas de seguridad y tienen lugar tanto en el mundo ficticio del film como en la Ciudad Autónoma de Buenos Aires. Ambos conceptos terminan siendo muchas veces injusto para los integrantes de la ciudadanía e incluso violatorio de sus propios derechos. Tanto en el film como en el marco de CABA, donde tienen lugar los casos de análisis de este trabajo, es posible percibir algunas similitudes como lo es el empleo de la tecnología aplicada a una vigilancia masiva e intrusiva sobre la privacidad de las personas. La población tanto en la película como en la realidad de todos los días se enfrenta a la implementación de nuevas políticas que buscan combatir la inseguridad y la criminalidad y aun frente a las potenciales amenazas a sus derechos inalienables, la piden desesperadamente.

En el filme de Steven Spielberg encontramos que la implementación de este sistema de vigilancia y control ha dado origen a "un gran ojo que todo lo ve" asumido enteramente por la población, pero no observado por ella.

En CABA ocurre algo muy similar con la implementación del reconocimiento facial que nos ha llevado a postular la presencia de un panóptico que, montado al lomo de las nuevas tecnologías digitales, parece haber cobrado más presencia y vigencia que nunca en las sociedades contemporáneas.

En *"Minority Report*" podemos entrever que la lógica del universo de la película parece seguir la misma línea que se establece en el cambio de paradigma de seguridad del siglo XXI el cual impone la necesidad de llevar a cabo una vigilancia masiva para combatir las "amenazas

internas" en pos de establecer una sociedad más segura. Cabe mencionar que este cambio en el paradigma de seguridad surge en los primeros años del año 2000 mientras que la película fue filmada en el 2002 a pocos meses de este suceso[100]. De manera que llama la atención la rapidez con la cual el film incorporó rápidamente en su narrativa el nuevo modelo de vigilancia que predica el nuevo paradigma de seguridad en las sociedades contemporáneas. Si agudizamos la mirada observaremos la exactitud en el desarrollo de los acontecimientos del film con respecto a la realidad que atraviesan actualmente las sociedades de control.

Por supuesto, en la película, así como se muestran similitudes también se vislumbran algunas diferencias significativas respecto al actual escenario de CABA. La política de seguridad de la Ciudad Autónoma de Buenos Aires no emplea "videntes" interconectados que predicen el futuro ni detiene a los ciudadanos por delitos que pudiesen cometer, pero, sobre este punto es necesario detenernos nuevamente.

Si bien en el film se aplica una "justicia preventiva", poco a poco esto comienza a verse también en el mundo real, como acontece por ejemplo en China, donde el sistema de ranking social premia o castiga el futuro de la población tomando en cuenta sus acciones pasadas, presentes y presumiblemente futuras.

A pesar de que al momento de escribir la tesina este sistema no se encontraba vigente para ser aplicado a los delitos, no es descabellado suponer que, en un futuro próximo, las fuerzas de seguridad puedan llevar a cabo detenciones preventivas en base al perfil de la persona, sus datos socio/económicos, datos referidos a la raza y religión o afiliación político/ ideológica.

No hay certezas, pero estas son algunas de las posibilidades que perfectamente podrían ser desplegadas en un futuro cercano y, de hecho, algunas de ellas están siendo utilizadas en el presente, aunque no en la Argentina. Por lo tanto, está claro que este continuo cambio y modulación de las nuevas tecnologías aplicadas al control y vigilancia masivo está lejos de llegar a su punto final. ¿Está el ser humano destinado a vivir en sociedades donde prime una vigilancia cada vez más intrusiva? ¿Vigilancia y privacidad se han convertido en términos cada vez más antagónicos? ¿La realidad está en camino de parecerse a la ficción o de incluso superarla? Sólo el tiempo lo dirá.

[100] Cabe destacar que el film de Spielberg se basa en un relato corto titulado *"El informe de la minoría"* escrito en 1956 por Philip K. Dick, pero podríamos suponer que la adaptación de la obra al cine en esta época (y no otra) quizá no haya sido casual como tampoco la incorporación de varios elementos propios del contexto histórico post atentado a las Torres Gemelas.

Bibliografía

- Alcántara, José (2008) "*La sociedad de control: privacidad, propiedad intelectual y el futuro de la libertad"* Disponible en https://www.versvs.net/wp-content/libros/la-sociedad-de-control/jose-alcantara-la-sociedad-de-control.pdf

- Almarcha Amparo, Amando de Miguel, De Miguel Jesús, Romero José Luis (1969) *"La documentación y organización de los datos en la investigación sociológica"* Disponible en http://tsmetodologiainvestigaciondos.sociales.uba.ar/wp-content/uploads/sites/175/2014/03/guia-de-lectura-unidad-1-1C2014-mm.doc

- Arancibia Carrizo, Juan Pablo (2010) *"El concepto de Poder en Michel Foucault"* Disponible en http://repositorio.uchile.cl/bitstream/handle/2250/108666/El-concepto-de-poder-en-la-obra-de-Michel-Foucault.pdf?sequence=3&isAllowed=y

- Aribau Sorrolla, Oscar (2018) "*Las TIC y la ciber soberanía en China, la base del presidente Xi Jinping para perfeccionar el control social Maoísta"* Disponible en http://openaccess.uoc.edu/webapps/o2/bitstream/10609/83827/6/oaribauTFM0618memoria.pdf

- Aruguete, Natalia (2017) *"¿Paraguas común o teorías independientes? El debate entre agenda setting, priming y framing"* Disponible en http://www.teoriascomunicunm.com.ar/archivos/UNIDAD2-Arguguete-ElDebateEntreAgendaSettingPrimingFraming.pdf

- Asociación por los Derechos Civiles (2015) "Pr*ivacidad y vigilancia en entorno digitales"* Disponible en http://www.articaonline.com/wp-content/uploads/2016/01/Programa-privacidad-y-vigilancia-en-entornos-digitales.pdf

- Asociación por los Derechos Civiles *"Desafíos de la biometría para la protección de los datos personales."* (2017). Disponible en https://adc.org.ar/informes/desafios-la-biometria-la-proteccion-los-datos-personales/

- Blanco Navarro, José María (2011)*"Seguridad e Inteligencia 10 años después del 11-S"* Disponible en http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM09-2011SeguridadInteligencia.pdf

- Castaño Saavedra, David Leonardo, Alonso Sierra, Juan David (2019) "*Sistemas de reconocimiento facial para control de acceso a vivienda"* Disponible en https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf

- Castells Manuel (2006) "*La revolución de la tecnología de la información"* Disponible en https://www.fra.utn.edu.ar/upload/de0550bf496309ea7d98d43503aa4338.doc

- Castro Edgardo (2019) "*La noción de policía en los trabajos de Michel Foucault: objeto, límites, antinomias"* Disponible en

https://dialnet.unirioja.es/descarga/articulo/7038660.pdf+&cd=1&hl=es-419&ct=clnk&gl=ar

- Cejas Eileen Berenice y González Carlos César (2015) "*Estado de la normativa sobre videovigilancia en Argentina y su relación con la protección de datos personales"* Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/55549/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

- Cejas Eileen Berenice (2016) "*Centro de monitoreo urbano en Ciudad Autónoma de Buenos Aires: la importancia de la participación ciudadana en el control del sistema*" Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/58266/Documento_completo.pdf?sequence=1

- Constitución de la Ciudad Autónoma de Buenos Aires

- Constitución Nacional Argentina

- Deleuze, Gilles (1991) "*Posdata sobre las sociedades de control"* Disponible en http://www.fundacion.uocra.org/documentos/recursos/articulos/Posdata-sobre-las-sociedades-de-control.pdf

- Delgadillo, Juan Fernando (2012) "*Foucault y el análisis del poder"* Disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=3974352

- De Mayerne, Louis Turquet (1611) "*La Monarchie Aristodemocratique"* Disponible en https://archive.org/details/lamonarchiearist00maye/page/n15/mode/2up

- De San Vicente Iñaki Gil (2007) "*Control, vigilancia y represión, el Estado en activo"* Disponible en https://www.lahaine.org/b2-img/control_social.pdf

- Diccionario Real Academia Española. Disponible en https://dle.rae.es/

- Fernández Leyre Merino (2018) *"La influencia de los medios de comunicación en el desarrollo de las guerras contemporáneas*" Disponible en https://www.recercat.cat/bitstream/handle/2072/326776/TFG-MERINO-2018.pdf?sequence=1

- Foucault, Michel (1990) *"Tecnologías del Yo"* Disponible en https://monoskop.org/images/7/70/Foucault_Michel_Tecnolog%C3%ADas_del_yo_y_otros_textos_afines_1990_2008.pdf

- Foucault, Michel (1975) "*Vigilar y Castigar"* Disponible en http://latejapride.com/IMG/pdf/Foucault_Michel_-_Vigilar_y_castigar.pdf

- Foucault, Michel (1978-1979)" *Seguridad, territorio y población"* Disponible en https://crucecontemporaneo.files.wordpress.com/2012/01/foucault_michel-seguridad_territorio_poblacion.pdf

- Foucault, Michel (1978) *"Qu`est-ce que la critique?* Disponible en http://riull.ull.es/xmlui/bitstream/915/1234/1/Traduccion+del+texto+de+Foucault+Qu%27est+que+la+critique.pdf

- Fundación Vía Libre (2015) *"Privacidad y vigilancia en el entorno digital*" Disponible en http://www.articaonline.com/wp-content/uploads/2016/01/Modulo-1-Privacidad.pdf

- Galeano, Diego (2003) "*Gobernando la seguridad: Entre políticos y expertos"* Disponible en http://www.memoria.fahce.unlp.edu.ar/trab_eventos/ev.6913/ev.6913.pdf

- García Jiménez, Ricardo (2009) *"El panoptismo: nuevas formas de control social,"* Disponible en https://www.eumed.net/rev/cccss/06/rgj2.htm

- Gendler, Martín (2017) "*Sociedades de control: Lecturas, diálogos y (algunas) actualizaciones"* Disponible en http://revistahipertextos.org/wp-content/uploads/2015/12/Gendler.pdf

- Gendler, Martín *(2017) "De ficciones, tecnologías, controles y errores psyco-pass entre el poder, producción, normalización y la resistencia"* Disponible en https://perio.unlp.edu.ar/ojs/index.php/question/article/view/4317/3746

- Gendler, Martín (2019) *"Acompañamiento y mediación algorítmicos de la vida ¿Subyugarse o resistir?"* Disponible en *http://revistabordes.unpaz.edu.ar/acompanamiento-y-modulacion-algoritmica-de-la-vida/*

- Guillen, A Sáenz,K ,Badii,M.H & Castillo,J (2009) *"Origen, espacio y niveles de participación ciudadana"* Disponible en https://www.academia.edu/9155592/Origen_espacio_y_niveles_de_participaci%C3%B3n_ciudadana_Origin_space_and_levels_of_participation

- Han, Byung- Chul Han (2014) *"En el enjambre"* Disponible en https://investigacion.udgvirtual.udg.mx/blogs/wp-content/uploads/2020/02/hans_Byung-Chul-enElEnjambre.pdf

- Harvey, David (1998) "*Comprensión espacio-temporal y condición postmoderna*" Disponible en http://www.ram-wan.net/restrepo/diferencia/harvey-comprension%20espacio-temporal.pdf

- Hidalgo Requena, Jesús (2004) "*De la sociedad disciplinaria a la sociedad del control: la incorporación de nuevas tecnologías a la policía"* Disponible en http://www.ub.edu/geocrit/sn/sn-170-43.htm

- Lechner, Milton (2016) *"Tecnologías aplicadas a la seguridad ciudadana: desafíos para la justicia transicional ante nuevos mecanismos de control social"* Disponible en http://revistadivulgatio.web.unq.edu.ar/wpcontent/uploads/sites/65/2016/11/D1_A6_lechner_2016-1.pdf

- Lío, Vanesa (2015) "*Ciudades, cámaras de seguridad y videovigilancia*: *Estado del arte y perspectivas de investigación"* Disponible en https://revistas.unc.edu.ar/index.php/astrolabio/article/view/9903/13441

- López Puerta, Rebeca "*Término CRIMIPEDIA: Teorías del control social" (2014)* Disponible en https://aprenderly.com/doc/3419719/t%C3%A9rmino-crimipedia--teor%C3%ADas-del-control-social?page=2

- Martínez Félix Pérez, Blanco Ruiz, Francisco, Prieto Viñuela, Juan José (2007)"*Las Nuevas Tecnologías Aplicadas a la Seguridad"* Disponible en https://www.infodefensa.com/wp-content/uploads/Ponencia%5B1%5D.pdf

- Merino Mauricio (1995) *"La participación ciudadana en la democracia*" Disponible en https://tecnologias-educativas.te.gob.mx/RevistaElectoral/content/pdf/a-1995-01-006-157.pdf

- Mieles, Ernesto (2005) "*El concepto de derecho. Foucault, la ley y la crítica del paradigma liberal"* Disponible en https://www.researchgate.net/publication/309452804_El_concepto_de_derecho_Foucault_la_ley_y_la_critica_del_paradigma_liberal/fulltext/5cc3519fa6fdcc1d49b21a63/El-concepto-de-derecho-Foucault-la-ley-y-la-critica-del-paradigma-liberal.pdf

- Muratori Marcela, Salvia Agustín (2017*) "Inseguridad ciudadana en la población urbana argentina del 2010-2016* del año 2017" Disponible en https://ri.conicet.gov.ar/bitstream/handle/11336/112817/CONICET_Digital_Nro.3d897539-6341-4686-9ef5-10ab13e37ebe_A.pdf?sequence=2

- Nuevo Código Civil y Comercial de la Nación (2015)

- Pellegrini, Silvia. *"Medios de comunicación, poder político y democracia"* (1993) Disponible en https://dialnet.unirioja.es/descarga/articulo/2955014.pdf

- Ramírez Barrientos Franklin (2008) "*La política antiterrorista de Estados Unidos"* Disponible en https://dialnet.unirioja.es/descarga/articulo/5622194.pdf

- Rodríguez, Pablo Esteban (2008) *"¿Qué son las sociedades de control"* Disponible en http://www.sociales.uba.ar/wp-content/uploads/21.-Qu%C3%A9-son-las-sociedades-de-control.pdf

- Romero, Alexis, Rujano, Raima, Del Nogal, José (2002) *"Control social: nuevas realidades, nuevos enfoques"* Disponible en https://www.redalyc.org/pdf/122/12211406.pdf

- Rubio Ferreres, José María (2009) *"Opinión pública y medios de comunicación. Teoría de la agenda setting"* Disponible en http://www.ugr.es/~pwlac/G25_01JoseMaria_Rubio_Ferreres.html

- Sánchez Ávila, Carmen (2012) *"Aplicaciones de la biometría a la seguridad"* Disponible en http://oa.upm.es/20071/1/INVE_MEM_2012_143061.pdf

- Sánchez, Georgina (2011) "*La política de defensa y seguridad de Estados Unidos a principios del siglo XXI"* Disponible en https://www.casede.org/PublicacionesCasede/seguridad-y-defensa-en-america-del-norte/seguridad-y-defensa-en-america-del-norte-Benitez-Wilson-22-111.pdf

- Sozzo, Máximo (2011) "*Policía, gobierno y racionalidad: Incursiones a partir de Michel Foucault*" Disponible en *https://www.santafe.gob.ar/index.php/web/content/download/221162/1154826/*

- Valderrama, Carlos Eduardo (2012) *"Sociedad de la información: hegemonía, reduccionismo tecnológico y resistencias"* Disponible en https://www.redalyc.org/pdf/1051/105124264002.pdf

- Valles, Miguel (1999*) "La investigación documental"* Disponible en http://pdfhumanidades.com/sites/default/files/apuntes/Valles%201999.pdf

Anexo I: Notas periodísticas utilizadas

- Télam (2013 diciembre 16) "*Las principales revelaciones de Edward Snowden"* Disponible en https://www.telam.com.ar/notas/201312/44925-las-principales-revelaciones-de-edward-snowden.html

- Revista Channel News (2012Noviembre) *"Reconocimiento facial: Te veo y te reconozco".* Disponible en http://www.emb.cl/channelnews/articulo.mvc?xid=2209

- Plataforma Wikipedia "*Sistema de reconocimiento facial"* Disponible en https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial

- Informe político (2019, octubre, 11) "*Ciudad: Chicanas entre Larreta y Lammens en el debate de candidatos*." Disponible en
- https://informepolitico.com.ar/ciudad-chicanas-entre-larreta-y-lammens-en-el- debate-entre-candidatos/
- El País (2018 Febrero 8*)" La policía china usa gafas con reconocimiento facial para identificar a sospechosos"* Disponible en https://elpais.com/internacional/2018/02/07/mundo_global/1518007737_209089.html

- El Comercio (2019 Febrero20) "*Cómo China usa reconocimiento facial para vigilar a más de 2,5 millones de habitantes*" Disponible en https://elcomercio.pe/tecnologia/ciencias/china-reconocimiento-facial-vigilar-2-5-millones-habitantes-noticia-609576-noticia/

- Noticias con la gente (2018 Febrero 8)" La *policía china usa gafas con reconocimiento facial para identificar a sospechosos* " Disponible en https://conlagentenoticias.com/la-policia-china-usa-gafas-con-reconocimiento-facial-para-identificar-a-sospechosos/

- El País (2017 Diciembre 14*)"El Estado de vigilancia de alta tecnología de China"* Disponible en https://elpais.com/tecnologia/2017/12/14/actualidad/1513243284_855531.html y https://es.bitterwinter.org/el-estado-de-vigilancia-de-alta-tecnologia-de-china/

- ABC (2019 Febrero 18) *"China'smass surveillance of Uyghur Muslims in Xinjiang provincerevealed in data security flaw"*

- Disponible en https://www.abc.net.au/news/2019-02-18/chinas-mass-surveillance-of-uyghur-muslims-revealed-in-data/10820634

- Infobae (2018 noviembre 6) "*Así funciona el "Gran Hermano" estatal en China: un sistema que identifica a la gente según su forma de caminar".* Disponible en https://www.infobae.com/america/tecno/2018/11/06/asi-funciona-el-gran-hermano-estatal-en-china-un-sistema-que-identifica-a-la-gente-segun-su-forma-de-caminar/

- La Vanguardia (2019 mayo 18) "*La inquietante apuesta china por el reconocimiento facial*" Disponible en https://www.lavanguardia.com/tecnologia/20190518/462270404745/reconocimiento-facial-china-derechos-humanos.html

- Todo Noticias (2019 julio 9) "*El FBI recopila sin permiso fotos del carnet de conducir para el reconocimiento facial"* Disponible en https://tn.com.ar/tecno/f5/el-fbi-recopila-sin-permiso-fotos-del-carnet-de-conducir-para-el-reconocimiento-facial_977144

- El Español (2019 mayo 30) "*Ya es real el reconocimiento facial en colegios: EE.UU empieza a probarlo"* Disponible en www.elespanol.com/omicrono/tecnologia/20190530/real-reconocimiento-facial-colegios-eeuu-empieza-probarlo/402461088_0.html

- Infobae (2019 agosto 13) *"EEUU ampliará uso de reconocimiento facial en fronteras"* Disponible en https://www.infobae.com/america/eeuu/2019/08/13/eeuu-ampliara-uso-de-reconocimiento-facial-en-fronteras/

- La Vanguardia (2019 Mayo15) *"San Francisco prohíbe el uso del reconocimiento facial para identificar a criminales"* Disponible en https://www.lavanguardia.com/internacional/20190515/462256381193/san-francisco-reconocimiento-facial-prohibe.html

- El País (2019 Mayo15) *"San Francisco, primera ciudad en prohibir la tecnología de reconocimiento facial en EE. UU.".* Disponible en https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html

- La Nación (2019 mayo 15) "*San Francisco prohíbe a la policía usar tecnología de reconocimiento facial; en Londres, el 96 por ciento de las veces da falsos positivos*" Disponible en https://www.lanacion.com.ar/tecnologia/san-francisco-prohibe-policia-usar-tecnologia-reconocimiento-nid2247555

- Agencia EFE (2019 octubre10) *"Aplauden veto a reconocimiento facial en cámaras de la policía en California"* Disponible en https://www.efe.com/efe/america/ame-hispanos/aplauden-veto-a-reconocimiento-facial-en-camaras-de-la-policia-california/20000034-4083420

- Sensebyte "*La privacidad ha muerto. Hoy es confianza y control del usuario"* Disponible en http://www.sensebyte.com/es/principales-tendencias-de-la-industria/85-privacy-it-s-dead-get-over-it-it-s-about-trust-and-user-control-es%7D

- Lobo Suelto (2017 octubre 11*) "Felicidad asegurada (I)"* Disponible en http://lobosuelto.com/felicidad-asegurada-i-carolina-di-palma/

- El Español (2017 setiembre 9) *"100% de seguridad o 100% de privacidad"* Disponible en https://www.elespanol.com/opinion/tribunas/20170908/245345464_12.html

- Asociación por los Derechos Civiles (2019 mayo23) *"#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires*" Disponible en https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/

- Gobierno de la Ciudad de Buenos Aires (2019 abril26) "*Rodríguez Larreta presentó el Sistema de Reconocimiento Facial de Prófugos: "El objetivo es que los vecinos estén más seguros"* Disponible en https://www.buenosaires.gob.ar/jefedegobierno/noticias/rodriguez-larreta-presento-el-sistema-de-reconocimiento-facial-de-profugos

- Infobae (2019 Febrero27) "*Adiós a la privacidad: un registro nacional de ADN como Gran Hermano de la nueva era"* Disponible en https://www.infobae.com/opinion/2019/02/27/adios-a-la-privacidad-un-registro-nacional-de-adn-como-gran-hermano-de-la-nueva-era/

- iProfesional (2019 abril 11*) "Cuestionan el sistema de video vigilancia porteño por vulnerar derechos humanos"* Disponible en https://www.iprofesional.com/tecnologia/289744-delitos-informaticos-ley-procesal-Cuestionan-el-sistema-de-videovigilancia-porteno-por-vulnerar-derechos-humanos

- Vía Libre (2012 enero10) "*Biometría en Argentina: la vigilancia masiva como política de estado"* Disponible en https://www.vialibre.org.ar/2012/01/10/biometria-en-argentina-la-vigilancia-masiva-como-politica-de-estado/

- La Nación (2013 noviembre 9) *"En busca de las armas de vigilancia masiva"* Disponible en https://www.lanacion.com.ar/tecnologia/en-busca-de-las-armas-de-vigilancia-masiva-nid1636661

- AM 750. (2019 agosto 2) *"Reconocimiento facial: Hay un 80% de falsos positivos con este sistema"* Disponible en https://750.am/2019/08/02/reconocimiento-facial-hay-un-80-de-falsos-positivos-con-este-sistema/

- Vía Libre (2019 mayo 13) *"El gran hermano porteño"* Disponible en https://www.vialibre.org.ar/2019/05/13/el-gran-hermano-porteno/

- Todo Noticias (2019 julio 11)" *Sistema de reconocimiento facial: retuvieron por error a una referente de la lucha contra la explotación de menores*" Disponible en https://tn.com.ar/sociedad/sistema-de-reconocimiento-facial-retuvieron-por-error-una-referente-de-la-lucha-contra-la_977335

- Página 12 (2019 octubre 4) *"Cámaras de reconocimiento facial: Larreta prometió 10.000 más"* Disponible en "https://www.pagina12.com.ar/223372-camaras-de-reconocimiento-facial-larreta-prometio-10-000-mas

- Clarín (2019 julio 22) "*Identificaron a 14 personas por día con el reconocimiento facial, pero el 81% quedó libre*" Disponible en https://www.clarin.com/policiales/identificaron-14-personas-dia-reconocimiento-facial-81-quedo-libre_0_O_WhA1FAf.html

- Vía País (2019 julio 11*)" Por un error en el sistema de reconocimiento facial detuvieron a una referente de la lucha contra la pedofilia"* Disponible en https://viapais.com.ar/buenos-aires/1136492-por-un-error-en-el-sistema-de-reconocimiento-facial-detuvieron-a-una-referente-de-la-lucha-contra-la-pedofilia/

- País 24 (2019 julio 13*)" Detuvieron a una activista que acusó a Macri de explotación sexual"* Disponible en http://www.pais24.com/index.php?go=n349691

- RT (2019 julio 27) "*Sólo detiene a inocentes": Las polémicas fallas en el sistema de seguridad con reconocimiento facial de Buenos Aires"* Disponible en

https://actualidad.rt.com/actualidad/322341-fallas-sistema-seguridad-reconocimiento-facial-argentina

- De la Bahía (2019 julio 29) *"Aciertos y errores del nuevo sistema de reconocimiento facial en las calles de Buenos Aires*" Disponible en https://www.delabahia.com.ar/aciertos-y-errores-del-nuevo-sistema-de-reconocimiento-facial-en-las-calles-de-buenos-aires/

- Tu Mercedes (2019 julio 12*) "El nuevo Reconocimiento Facial de Prófugos ya mostró los primeros errores"* Disponible en https://www.tumercedes.com/noticia/220989

- Argentina Today (2019 agosto 3) *"Argentina: Víctimas del reconocimiento facial estatal"* Disponible en https://argentinatoday.org/2019/08/03/argentina-victimas-del-reconocimiento-facial-estatal/

- Clarín (2019 agosto 2) "*Pasó casi una semana preso por un error policial"* Disponible enhttps://www.clarin.com/policiales/paso-semana-preso-error-policial-sistema-reconocimiento-facial_0_6KiuCu0fy.html

- Infobae (2019 agosto 2)"*Un hombre estuvo seis días preso por un error policial*" Disponible en https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial/

- A24 (2019 Agosto 2) "El *hombre que estuvo detenido seis días por un error recuperó la libertad: "Me podrían haber arruinado la vida"* Disponible en https://www.a24.com/actualidad/hombre-estuvo-detenido-seis-dias-error-recupero-libertad-haber-arruinado-vida-08022019_SJSieA-XB

- La Brújula 24 (2019 Agosto 1) "*Lo detuvieron por un robo en Bahía pero no conoce la ciudad"* Disponible en https://www.labrujula24.com/2019/08/01/lo-detuvieron-por-un-robo-en-bahia-pero-no-conoce-la-ciudad-n7319

- El patagónico (2019 agosto 2) *"Estuvo detenido seis días por un error del Sistema de Reconocimiento Facial"* Disponible en https://www.elpatagonico.com/estuvo-detenido-seis-dias-un-error-del-sistema-reconocimiento-facial-n5046354

- Telefé Noticias (2019 agosto1) "*Lo detuvieron por Sistema de Reconocimiento Facial y denuncian que es un error"* Disponible en https://telefenoticias.com.ar/actualidad/lo-detuvieron-en-retiro-por-el-sistema-de-reconocimiento-facial-su-familia-sostiene-que-es-un-error/

- Tiempo Argentino (2019 agosto 2) *"La pesadilla del hombre que estuvo cinco días preso por un error policial*" Disponible en https://www.tiempoar.com.ar/nota/la-pesadilla-del-hombre-que-estuvo-cinco-dias-preso-por-un-error-policial

- Télam (2019 agosto 2) "*Pasó cinco días preso por un error en la base del Sistema de Reconocimiento Facial"* Disponible en https://www.telam.com.ar/notas/201908/381060-un-hombre-paso-cinco-dias-preso-por-un-error-en-la-base-del-sistema-de-reconomiento-facial.html

- La Izquierda Diario (2019 agosto 2) "*El Gran Hermano macrista mantuvo 6 días preso a un hombre…pero fue un "error"* Disponible en http://www.laizquierdadiario.com/El-Gran-Hermano-macrista-mantuvo-6-dias-preso-a-un-hombre-pero-fue-un-error

- El Diario Sur (2019 agosto 1) *"Insólito: un vecino está detenido por un robo en Bahía Blanca pero nunca estuvo en esa ciudad"* Disponible en https://www.eldiariosur.com/esteban-echeverria/policiales/2019/8/1/insolito-un-vecino-esta-detenido-un-robo-bahia-blanca-pero-nunca-estuvo-esa-ciudad-n25053

- BBC (2017 noviembre 18) "*El "orwelliano" plan de China para puntuar y monitorear el comportamiento de sus ciudadanos"* Disponible en https://www.bbc.com/mundo/noticias-internacional-41970041

- Diario las Américas (2019 julio 9) "*Inmigración: Preocupa uso de tecnología de reconocimiento facial por ICE"* Disponible en https://www.diariolasamericas.com/eeuu/inmigracion-preocupa-uso-tecnologia-reconocimiento-facial-ice-n4180672

- Naked Segurity (2018 agosto 26)"*El sistema de reconocimiento facial de la escuela genera preocupaciones sobre la privacidad*" Disponible en https://nakedsecurity.sophos.com/es/2018/06/26/school-facial-recognition-system-sparks-privacy-concerns/

- Ámbito (2019 mayo 15)" *Por poner en peligro derechos y libertades, San Francisco prohíbe el reconocimiento facial"* Disponible en https://www.ambito.com/mundo/san-francisco/por-poner-peligro-derechos-y-libertades-prohibe-el-reconocimiento-facial-n5031664

- Antena 3 (2013 Junio,7*)"Obama: "No se puede tener un 100% de seguridad con un 100% de privacidad" Disponible en* https://www.antena3.com/noticias/mundo/gobierno-obama-asegura-que-controles-ciudadanos-traves-internet-son-legales_2013060757472901658 4a8f86268de61.html

- Todo Noticias (2019, agosto,6) "*Pasó seis días detenido por un dato mal cargado en el sistema de reconocimiento facial"* Disponible en https://tn.com.ar/policiales/paso-seis-dias-detenido-por-un-dato-mal-cargado-en-el-sistema-de-reconocimiento-facial_984084/

Anexo II

Cuadro Nº8: Comparación de ambos casos de análisis.

Regulación	***Tensión Holway***	***Tensión Ibarrola***	***Comparación***
Constitución Nacional			
Ley de Protección de Datos Personales.	Se observa tensión respecto a los derechos de privacidad e intimidad debido a la desactualización de las bases de datos por parte del poder judicial.	Se genera tensión respecto a la privacidad debido a manejos incorrectos de los datos personales del ciudadano por parte de integrantes de las fuerzas de seguridad y del Poder Judicial.	Detenciones erróneas debido a errores humanos por parte de funcionarios supuestamente preparados para el manejo de datos sensibles de la ciudadanía, pero cuyo accionar denota una desidia por el cuidado a la privacidad de la población.
Nuevo Código Civil y Comercial	Se produce tensión en relación con los derechos dado que esta regulación nacional busca proteger la intimidad, la honra y la reputación de la ciudadanía. Ello no se observa en este caso debido a la errónea detención de la ciudadana y al hecho de que su caso ha tomado trascendencia mediática lo cual también puede suponer un avance contra su intimidad.	La errónea detención ha implicado una violación a los derechos que buscan ser defendidos por el Nuevo Código Civil y Comercial. El ciudadano no sólo vio afectado su derecho a la privacidad sino también su honra y reputación, lo que podría verse en mayor medida ya que debió pasar varios días detenido a la espera que se aclarase su situación judicial. Por lo tanto, se ha visto afectado su derecho a la imagen, luego de que su caso tomara una relevancia mediática nacional e internacional aún mayor que la de Holway.	El uso del reconocimiento facial supone una invasión a la privacidad y un perjuicio a la reputación y honra de los actores involucrados y que no suele tomarse en cuenta a la hora de analizar el despliegue de las nuevas tecnologías de vigilancia y control con la consecuente afectación que supone el derecho a la imagen de los sujetos, producto de la difusión masiva por parte de los medios. Sin embargo, no es lo mismo en ambos casos. Holway ha tenido reiteradas apariciones mediáticas a raíz de su trabajo en la ONG "Alerta Vida" pero ello no quita que, en ambos casos, los medios han replicado una experiencia traumática para los

			dos y la imagen de ambos haya tenido un alcance masivo independientemente de la voluntad de los ciudadanos.
Resolución 238/2012 del Ministerio de Seguridad	Se observa una tensión debido a que la legislación establece que el uso de las nuevas tecnologías de vigilancia no debe ser intrusivo hacia la privacidad de la ciudadanía. El empleo de esta herramienta no sólo debe conjurar el ilícito en la vida pública, sino que debe brindar pruebas relevantes para la investigación judicial. En este caso no se cometía ningún delito que pusiera en peligro la convivencia ciudadana. Además, la causa judicial por la cual se la imputada había sido cancelada hacía más de una década.	Se observa una tensión referida al uso de esta tecnología que no ha sido empleada para conjurar un delito que representase un riesgo inmediato para la sociedad, mientras que, el uso del reconocimiento facial también supuso una intrusión en la privacidad del ciudadano que circulaba en el ámbito público. La resolución establece que el uso de estas nuevas tecnologías de vigilancia debe ser realizado por funcionarios con idoneidad técnica y legal conforme a las funciones a desempeñar buscando la protección de los derechos de la ciudadanía, algo que no ocurrió en el caso analizado.	En ambos casos el uso del reconocimiento facial en el espacio público no fue utilizado para prevenir ni combatir ninguna amenaza real que pudiera estar ocurriendo, ni ha servido para la recolección de pruebas para futuros procesos judiciales. El caso de Ibarrola pone en tela de juicio la capacidad y preparación de los funcionarios policiales y judiciales para el uso de esta tecnología sin perjuicio de los derechos de la población. En ninguno de los dos casos se puede detectar que el uso del reconocimiento facial haya servido para recabar pruebas relevantes que puedan ser utilizadas en un proceso judicial.
Disposición 10/2015 DNPDP Constitución Nacional	Se produce una tensión respecto a esta legislación y el derecho a la privacidad de la ciudadana, ya que en la legislación se establece que la información recabada por las nuevas tecnologías de control y vigilancia debe ser adecuada, pertinente y no excesiva en torno a la finalidad perseguida y debe garantizar el cuidado y protección de la privacidad. La causa judicial en la que se	Se produce una violación a la privacidad debido a que el sistema de reconocimiento facial ha generado una recopilación excesiva y de carácter no pertinente de información respecto al ciudadano. También existe una violación del ArtículoNº4 de la legislación que dicta que los responsables del manejo de la información sensible	En ambos casos se produce una recolección excesiva de información por parte de las nuevas tecnologías de vigilancia operadas por las fuerzas de seguridad con la consecuente invasión a la privacidad de la población. En el caso de Ibarrola, las disposiciones que buscan resguardar la información sensible de la ciudadanía frente

	involucraba a Holway ya estaba cerrada y no existían motivos que ameritaran seguir investigando el particular.	de la ciudadanía deben adoptar medidas que eviten errores técnicos y/o humanos, intencionales o no relacionados en torno al tratamiento incorrecto de la información de la población a fin de garantizar su privacidad.	a los posibles "errores" humanos o técnicos son pasadas por alto en el accionar de las fuerzas de seguridad.
Constitución Nacional Artículo Nº43	No existe tensión	No existe tensión	
Constitución Nacional Artículo Nº19	Se genera tensión con lo establecido por el Artículo Nº19 respecto de la implementación de las nuevas tecnologías y modalidades de vigilancia que aún las actividades diarias (como tomar un subte) sean objeto de una vigilancia permanente. A pesar de que los errores son atribuidos a los mismos funcionarios que deben garantizar el correcto funcionamiento y operación de estas nuevas modalidades.	Se produce una tensión respecto al Artículo Nº19 de la Constitución Nacional, que garantiza la privacidad. El despliegue de las nuevas tecnologías de vigilancia y control parece realizarse de manera descuidada y sin preparación por parte de sus operadores. En este caso, su uso ha supuesto la intrusión en la intimidad de un grupo familiar bajo el erróneo argumento de que el ciudadano era buscado por la justicia sospechoso de haber cometido un robo en otra localidad de la provincia de Buenos Aires.	Al comparar el escenario de ambos casos pareciera que la esfera de la vida privada de la ciudadanía se ve avasallada por la implementación de las nuevas tecnologías de control y vigilancia desplegadas en el espacio público por parte de las fuerzas de seguridad. El reconocimiento facial brinda a la policía de la Ciudad la capacidad de conocer en tiempo real la ubicación y la actividad que realiza cada uno en el espacio público. Esta tecnología posee el potencial de lograr individualizar a los sujetos buscados independientemente de que se encuentren en puntos donde se genera una gran aglomeración de personas, (Holway en el subte, Ibarrola en una estación de tren) por lo que, la frase "*encontrar una aguja*

			en un pajar" ya no es aplicable debido a la implementación de estas tecnologías, lo que respalda lo afirmado en este trabajo de investigación, toda la ciudadanía es susceptible de ser individualizada y vigilada y la esfera privada parecería ir desvaneciéndose gradualmente en las sociedades de control.
Regulaciones Ciudad Autónoma de Buenos Aires.			
Resolución 398/19 MJYSGC	El accionar de las fuerzas de seguridad mediante el uso de reconocimiento facial que derivó en su errónea detención supone una tensión con esta resolución la cual considera que tanto la privacidad y la intimidad son partes inviolables de la dignidad humana. Cabe señalar que ser detenida debido a una tecnología, que posee el potencial de afectar seriamente la privacidad de la población, en un espacio público y sin causa aparente, supone un ataque a la dignidad de la ciudadana	Su detención supone una violación a su privacidad, que, como establece el cuerpo de la ley, afecta la dignidad de la persona. Se debe destacar que la dignidad de la persona se ve afectada no sólo por la errónea detención, sino por el hecho de que el caso ha tomado dominio público al ser abordado por los medios de comunicación, por lo que no se puede descartar que Ibarrola (un personaje no público) haya visto afectada su dignidad tras cobrar una relevancia mediática no buscada ni anhelada.	El concepto de dignidad es propio de cada persona. En ambos casos de análisis se entiende que la dignidad no sólo se ha visto afectada por la detención en sí, sino también por cobrar relevancia mediática (en el caso de Ibarrola aún mayor que en el de Holway). El ataque a la dignidad de la persona, como plantea la Resolución también puede implicar, como se ha mencionado al abordar el Código Civil, el ataque a la honra y la reputación de los ciudadanos.
Ley N°2602	Se presenta una tensión entre la implementación del reconocimiento facial y esta legislación de CABA ya que el cuerpo de la ley establece que el uso de este sistema de	En este caso el despliegue de los medios técnicos, tecnológicos y humanos para su captura es excesiva si se analiza el contexto que rodea al sujeto y el nivel de peligro que	La comparación de ambos casos arroja que las fuerzas de seguridad del Estado parecen valerse de las mismas tecnologías de control y vigilancia para contrarrestar los delitos presentados en

	vigilancia y control debe tener en consideración los derechos fundamentales de la ciudadanía entre los cuales se incluye el derecho a la privacidad garantizado por legislaciones nacionales y locales. El uso del reconocimiento facial supone una invasión a su intimidad en forma desproporcionada en comparación al delito que supuestamente busca ser combatido por las fuerzas de seguridad.	podía representar para la sociedad. El uso del reconocimiento facial se toma la atribución de pasar por alto el derecho a la intimidad y privacidad del ciudadano, entendiéndolo como uno de los derechos fundamentales del ser humano. Esta ley establece que los sistemas de vigilancia y control social en el espacio público deben operar regidos por los principios de razonabilidad y proporcionalidad.	la vida pública sin tomar en consideración el grado de gravedad que presentan para la convivencia ciudadana (en el Código Penal, se considera al supuesto delito de Ibarrola de mayor gravedad que el de Holway.) El empleo del reconocimiento facial parece ser empleado de forma indiscriminada, independientemente del delito que se trate y sin contemplar la debida consideración hacia la privacidad de la ciudadanía.
Ley N°5.688	Esta legislación de CABA genera una clara tensión respecto al derecho a la privacidad, ya que establece que las nuevas tecnologías deberían ser empleadas tanto para combatir y prevenir ilícitos como para transparentar y mejorar el desempeño institucional de las fuerzas de seguridad. La situación judicial de Holway ya había sido resuelta, por lo tanto, no existía ni un crimen que prevenir ni un delito que investigar luego de su consumación. Si bien la legislación dicta que el uso de las nuevas tecnologías debe transparentar el accionar de las fuerzas de seguridad y del poder judicial, la desactualización de las bases de datos y el diario accionar de las fuerzas de seguridad no parecen acatar esta disposición.	Existe una tensión entre esta legislación y el derecho a la privacidad del ciudadano ya que la legislación busca que las nuevas tecnologías sean un instrumento tanto para combatir el delito como para transparentar el accionar de las fuerzas de seguridad, aunque este caso particular revela claramente que el desempeño de los efectivos es mínimo y despreocupado en torno a la protección y resguardo de la información privada de la ciudadanía. Aquí también la legislación reza que el accionar de las nuevas tecnologías debe basarse en principios de razonabilidad y proporcionalidad y en el respeto hacia la privacidad de la población.	Pese a la existencia de normas y legislaciones cuyo espíritu es el de transparentar el accionar de las fuerzas, continúan existiendo errores y manejos incorrectos y poco claros acerca de la información de la ciudadanía luego de la implementación de las nuevas tecnologías de vigilancia y control social, Si bien los errores humanos han provocado las detenciones en ambos casos, cabe remarcar la gravedad que supuso el caso de Ibarrola, tanto por el largo período de detención como por la pena en expectativa que suponía su crimen en caso de que la justicia no rectificara la equivocación.

Decreto Reglamentario 716/2009	Entra en tensión debido a que este Decreto implica la reglamentación de la Ley Nº2602 cuyo objetivo es la regulación de la utilización de videocámaras por parte del Poder Ejecutivo para grabar imágenes en lugares públicos y su posterior tratamiento. Este Decreto Reglamentario establece que el uso de las nuevas tecnologías de control y vigilancia deben respetar los derechos fundamentales y libertades públicas de la ciudadanía, como el derecho a la privacidad. El caso Holway refleja que el accionar de las fuerzas de seguridad no tiene reparos a la hora de generar una vulneración de los derechos de la población cuando pretende alcanzar sus objetivos, buscando "establecer sociedades más seguras".	Se produce una tensión respecto a la privacidad e implementación del reconocimiento facial. Este Decreto Reglamentario tiene por objetivo la regulación del sistema de cámaras de videovigilancia en el espacio público de CABA, aunque siempre manteniendo el espíritu de proteger derechos fundamentales de la población. Este caso demuestra que los derechos más fundamentales e innatos del ser humano como la privacidad e intimidad, respaldados por una gran cantidad de legislaciones nacionales y extrajeras, son pasados por alto y vulnerados debido a la implementación de nuevas tecnologías y modalidades de vigilancia por parte de las fuerzas de seguridad.	En ambos casos se observa que a pesar de que el cuerpo del Decreto Reglamentario tiene el espíritu de establecer reglas de funcionamiento para el sistema de videovigilancia que garanticen el cuidado y respeto de derechos como la privacidad, esto no ocurre. Pero, cabe aclarar que en ninguno de los casos analizados no sólo ha sido el derecho a la privacidad lo que se ha visto afectado, sino que la detención errónea de ambos también ha afectado el derecho a la libertad (Holway algunas horas, Ibarrola seis días), aun cuando la ley de Protección de Datos Personales establece que en caso de existir información errónea hay un plazo de máximo de cinco días para rectificar el error.
Ley N°3.130	Esta ley establece que los operadores de los sistemas de videovigilancia, encargados de la operación de cámaras y sistemas de reconocimiento facial en CABA deben ejercer su misión buscando garantizar al máximo el derecho a la intimidad de la población y desempeñando su trabajo con el máximo de discrecionalidad, con el objetivo de respetar los derechos fundamentales	Ocurre lo mismo con Ibarrola donde el despliegue de las nuevas tecnologías y modalidades de vigilancia producen una fuerte violación respecto a la privacidad del ciudadano, inmiscuyéndose en su intimidad, aun cuando el cuerpo de la legislación establece en forma	En el cuerpo de la ley establece que el uso de las nuevas tecnologías de vigilancia busca respetar el derecho a la privacidad e intimidad de la población. Sin embargo, el análisis de ambos casos revela que independientemente del espíritu de la legislación por

	de la población, como lo establece la Ley Nº2602. En el caso Holway, no se respeta, ya que la ciudadana es identificada en tiempo real y con su ubicación geográfica en el espacio público, aun cuando no existieran motivos válidos para que sea identificada y mucho menos demorada por las fuerzas de seguridad de CABA.	explícita el objetivo de proteger estos derechos. Esta ley dictamina que la videovigilancia y el reconocimiento facial deben operar guiados bajo los principios jurídicos de proporcionalidad y razonabilidad. Pero, la operación de las nuevas tecnologías y modalidades de vigilancia en CABA no parecen tomar en cuenta estos principios a la hora de realizar su accionar en el espacio público ya que parece haberse desplegado el mismo protocolo de acción independientemente de la gravedad de los delitos que se busca combatir.	resguardar los derechos fundamentales de la ciudadanía, la implementación del reconocimiento facial en el espacio público implica en sí mismo la puesta en funcionamiento de un sistema de control y vigilancia de naturaleza intrusiva en la privacidad de los sujetos existan o no motivos válidos para ejercer esta vigilancia. La ley apunta que se acotará de manera indispensable la discrecionalidad del operador de este sistema, sin embargo, ello es algo subjetivo y cabe preguntarse bajo qué parámetros se medirá esta discrecionalidad.
Resolución 10/MJYSGC/11	No hay tensión	No hay tensión	
Resolución 314/MJYSGC/10	No hay tensión	No hay tensión	

Fuente: Elaboración propia en base al cuerpo de las leyes.