revista pensamiento penal

La tecnología aplicada a la seguridad de la Nación y su intromisión al derecho a la intimidad

Tomás Francisco Di Cecco[1]

SUMARIO: I.- Introducción; II.- El derecho a la privacidad conforme el art. 18 del CN; III.- La Videovigilancia y su marco normativo; IV.- La Videovigilancia como amenaza a derechos individuales; V.- La existencia de un bien superior y la necesidad de las órdenes judiciales; VI.- La manipulación por parte del Estado de datos sensibles individuales; VII.- La Video vigilancia y el derecho penal del enemigo; VIII.- Conclusión; IX.- Referencias.

RESUMEN: El presente trabajo tiene por objeto demostrar la relación de tensión entre el derecho a la privacidad personal y el avance de la tecnología en materia de cibervigilancia en la vía pública, posibilidad técnica que permite el almacenamiento, registro y tratamiento de datos, en especial de la imagen de los individuos y el seguimiento de sus movimientos de modo sistemático y sin posibilidad de control sobre los datos almacenados. El progreso evidenciado en las tecnologías de la información y las comunicaciones (TICs) aplicadas a la seguridad interior del Estado frente a las nuevas manifestaciones de criminalidad organizada, en particular, el terrorismo, han propiciado sin quererlo un avance paulatino, pero imperceptible, sobre áreas de la personalidad individual que hasta hace poco tiempo estaban restringidas. Ese intrusismo informático por parte de agencias

[1] Abogado por la Universidad de Buenos Aires, Especialista en Derecho Penal por la Universidad de Belgrano, Diplomado en Delitos del Crimen Organizado por la Universidad de San Isidro.

estatales obliga a una reevaluación del derecho a la privacidad en los términos empleados en los arts. 18 y 19 de la Constitución Nacional.

ABSTRACT: This article aims to demonstrate the conflict between the right to privacy and the advancement of technology in the matter of cyber surveillance on the public space, a technical possibility that allows the storage, registration and processing of data, especially of the image of individuals and the track of their movements in a systematic manner and without any possibility of control over the stored data. The progress shown in information and communication technologies (ICT) applied to national security, in face of new manifestations of organized crime, like terrorism, have lead to a gradual but imperceptible advance over areas of the individual personality that until recently were restricted. This technology assisted intrussionism carried out by state agencies requires a reassessment of the right to privacy under terms of the articles 18 and 19 of the National Constitution.

PALABRAS CLAVE: cibervigilancia, videovigilancia, datos personales, privacidad, enemigo.

KEYWORDS: cyber surveillance, video surveillance, personal data, privacy, enemy.

I.- Introducción

El avance tecnológico en materia de cibervigilancia, aplicadas a la seguridad interior del Estado, mantiene una relación de tensión con el derecho a la privacidad personal consagrado en los arts. 18 y 19 de la Constitución Nacional.

Demuestran lo expuesto casos como el del sistema de lectura de patentes de vehículos existentes en el país, cámaras de reconocimiento facial y de monitoreo, identificación biométrica para el ingreso en estadios deportivos, entre otros. Todos estos casos, serán materia de desarrollo en el presente e intentarán demostrar la existencia de un avasallamiento por parte del Estado en libertades individuales en relación con la necesidad, idoneidad y proporcionalidad de esas medidas de vigilancia electrónica.

Sin embargo, la circunstancia de afirmar dicho avasallamiento por parte del Estado lleva a indagar sobre una segunda cuestión relacionada con la existencia de un interés superior que legitime una reducción en el ámbito de las libertades esenciales, en especial, respecto del derecho a la privacidad de las personas.

Ambas cuestiones serán abordadas de manera integral y sistemática para demostrar la tesis de este trabajo sobre la relación de tensión entre el deber del

Estado de asegurar el orden y la paz sociales y los derechos de los ciudadanos frente a la injerencia de las nuevas tecnologías en el ámbito de su privacidad.

II.- El derecho a la privacidad

Con el objeto de efectuar un correcto análisis sobre el derecho a la privacidad corresponde traer a colación el art. 18 de nuestra Constitución Nacional, en donde se centran los pilares de ese derecho tan preciado. En el citado artículo se sostiene que: "*Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. 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. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquélla exija, hará responsable al juez que la autorice*".

De la lectura de dicho articulado, son dos las consideraciones que habremos de efectuar preliminarmente. La primera de ellas, es que resulta claro que nuestros constituyentes plasmaron su intención de que las decisiones relacionadas a las invasiones a la intimidad queden en la órbita de los jueces. Tal como sostiene Vélez Mariconde la "autoridad competente" no es otra que el poder que la propia constitución estableció para administrar la justicia, es decir, el Poder Judicial[2].

El control judicial de la actividad investigativa del Estado a cargo de los agentes fiscales, en relación con la garantía del debido proceso, la imparcialidad del juzgador y el derecho de defensa en juicio, es una condición insoslayable en la legalidad del proceso. La función de control a cargo de los jueces es un resguardo contra la arbitrariedad estatal y ellos son los que se encuentran en una situación de mayor serenidad y objetividad para resolver sobre cuestiones atinentes a la limitación de derechos individuales. Esto, ha sido afirmado por la Corte Suprema de Estados Unidos en diversos fallos, por ejemplo, en "Johnson v. United States"[3].

[2] Vélez Mariconde, *Derecho Procesal Penal*, 3 ed., vol II, p. 487.

[3] 333 US 10, 14 (1948)

En este precedente, personal policial detectó olor a opio que egresaba de una habitación de hotel por lo que decidieron irrumpir en el lugar sin una orden de registro. Una vez dentro, hallaron opio y aparatos para fumar como así también la presencia de una única persona en el lugar, quien fue detenida. La Corte Suprema de Justicia de los Estados Unidos resolvió que no existía causa probable para arrestar a la acusada hasta tanto el personal policial irrumpió en el domicilio por lo que no era posible justificar, al mismo tiempo, el arresto por medio del registro domiciliario y el registro en virtud del arresto[4]. En definitiva, se sostuvo que no era el personal policial quien debía decidir en qué casos el derecho a la privacidad debe ceder ante el Estado, sino que el encargado de esa función son los jueces. En palabras del Juez Jackson se dijo que *"En qué casos el derecho a la privacidad debe razonablemente ceder a favor del derecho estatal a practicar una requisa, es algo que, como regla, debe ser decidido por un juez; no por un policía ni por ningún otro agente del Gobierno"*.

En definitiva, como observamos la jurisprudencia internacional también ha receptado esta idea de que sean los jueces, y no el personal policial, quienes deben decidir en qué casos el derecho a la privacidad debe ceder ante el Estado. No olvidemos que el jefe de las fuerzas de seguridad, en última instancia, no es otro que el Presidente de la Nación, como cabeza del poder Ejecutivo Nacional, por lo que resulta lógico que en el marco del sistema Republicano existente en nuestro País sea otro Poder del Estado (el Poder Judicial), quien limite las injerencias de éste a través de las fuerzas de seguridad u de otros agentes del gobierno sobre la privacidad de los individuos.

La segunda cuestión está relacionada con las limitaciones interpretativas de ese artículo 18 de la Constitución Nacional que regula las garantías judiciales al compararlo con los avances tecnológicos en el campo de la criminalidad moderna.

En razón de ello, resulta necesario acudir a una interpretación dinámica de la Constitución Nacional de modo tal que pueda adaptarse rápidamente a los avances tecnológicos.

[4] Paradójicamente, esta dicotomía sí fue sostenida por nuestra Corte Suprema de Justicia de la Nación en el fallo CSN-Fallo, 326:41 "Szmilowsky" (con cita al fallo del mismo Tribunal, LL, 1999-B-282, "Fernández Prieto") al sostener que la sospecha del funcionario policial actuante, fue razonable para realizar una requisa sin orden judicial dado que "*ulteriormente fue corroborada con el hallazgo de efectos vinculados a la tenencia de estupefacientes*" (ver consid. 8 de fallo).

Un ejemplo de esta interpretación dinámica la dio nuestra Corte Suprema de Justicia de la Nación en el fallo "Rodríguez María Belén c/ Google Inc."[5]. Allí se discutía la responsabilidad de motores de búsqueda (Google) en la facilitación de acceso a sitios web que tenían contenido que agredía el derecho al honor y a la imagen de la parte actora. Así, se precisó que el caso colocaba al derecho de expresión y libertad en conflicto con el derecho a la imagen y al honor.

Lo interesante del fallo, en lo que hace al presente trabajo, es el modo dinámico en que la Corte Suprema de Justicia de la Nación entendió que la libertad de expresión (consagrado en nuestro art. 14 de la CN) comprendía también el derecho a expresarse a través de internet.

Recordemos, que el art. 14 de la CN reza que "*Todos los habitantes de la Nación gozan de los siguientes derechos conforme a las leyes que reglamenten su ejercicio; a saber: de trabajar y ejercer toda industria lícita; de navegar y comerciar; de peticionar a las autoridades; de entrar, permanecer, transitar y salir del territorio argentino;* ***de publicar sus ideas por la prensa sin censura previa****; de usar y disponer de su propiedad; de asociarse con fines útiles; de profesar libremente su culto; de enseñar y aprender.*"

En este sentido, como sabemos, cuando se redactó el mismo no existía internet por lo que adaptar el derecho de expresión a la nueva realidad era algo vital e internet, sin lugar a dudas, es una de esas nuevas realidades que llegaron para modificar el mundo en el que vivimos.

Así, nuestro máximo Tribunal en el considerando número once del precedente citado sostuvo que "*el derecho de expresarse a través de Internet fomenta la libertad de expresión tanto desde su dimensión individual como colectiva. Así, a través de Internet se puede concretizar el derecho personal que tiene todo individuo a hacer público, a transmitir, a difundir y a exteriorizar -o no hacerlo- sus ideas, opiniones, creencias, críticas, etc. Desde el aspecto colectivo, Internet constituye un instrumento para garantizar la libertad de información y la formación de la opinión pública.*"

Como vemos, las nuevas realidades impuestas por los avances tecnológicos obligan a hacer una interpretación dinámica de la Constitucional Nacional a fin de preservar los derechos consagrados en ellas y en definitiva impedir que nuestra Carta Magna se convierta en un conjunto de derechos que no pueden aplicarse a la realidad actual, transformándolos en obsoletos.

[5] Fallo 337:1174

Del mismo modo, esta circunstancia provocó la necesidad de ir adaptando el alcance de nuestro art. 18 de la CN a nuevos escenarios que se fueron presentando en la vida diaria. Ese fue el caso de las escuchas telefónicas que fue alcanzado por "la correspondencia epistolar y papeles privados" e incluso la correspondencia electrónica y la solicitud de los listados de llamadas entrantes y salientes de abonados telefónicos, entre otras cosas. Así lo considero nuestra Corte Suprema de Justicia en los precedentes "Quaranta"[6] y "Halabi"[7].

En ese lineamiento, nuestro máximo tribunal sostuvo en el precedente "Gutheim v. Alemann"[8] que "*el derecho a la privacidad comprende no solo la esfera doméstica y al círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas tales como la integridad corporal o de imagen, nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de los familiares autorizados para ello, y solo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen*".

Cabe destacar, que desde el inicio nuestra Corte Suprema de Justicia de la Nación reconoció la necesidad de resguardar un ámbito de privacidad frente a la injerencia estatal arbitraria. Muestra de ello fueron los fallos "Charles Hermanos"[9] y "Ventura"[10].-

En el primero de los casos fue objeto de análisis el actuar de funcionarios de Aduana, que habían efectuado un allanamiento, sin orden judicial, en el comercio "Charles Hermanos" y resultas del cual se secuestraron documentos que fueron base de una imputación por contrabando. Sin embargo, la Corte declaró inadmisible la prueba obtenida sosteniendo que "*auténticos o falsos (los documentos), ellos no pueden servir de base al procedimiento ni de fundamento al juicio. Si lo primero (auténticos) porque siendo el resultado de una sustracción y de un procedimiento injustificable y condenado por la ley, aunque se ha llevado a cabo con el propósito de descubrir un delito…la ley, en interés de la moral, de la seguridad, y secreto de las relaciones sociales las declara inadmisible; y si lo segundo (si son falsos), porque su naturaleza misma se opone a darles valor y mérito alguno*".

[6] Fallo 333:1674
[7] Fallo 270.XLII
[8] CSJN, fallo 316:703
[9] CSJN-Fallo 46:36
[10] LL, 2005-B-319

Por otra parte, en el caso "Ventura" funcionarios aduaneros efectuaron un allanamiento sin orden judicial en una oficina comercial, pero esta vez consignó en el acta que el imputado Ventura había prestado consentimiento para que los uniformados accedieran al lugar. Sin perjuicio de ello, la Corte sostuvo que es necesario que el consentimiento del afectado haya estado precedido de la información necesaria para advertirle sobre los peligros que se ciernen sobre su derecho a la privacidad; circunstancia no verificada en el caso.

En ese sentido, la Corte concluyó que *"teniendo en cuenta que de las constancias del sublite surge que el allanamiento (que en sí mismo constituye una severa intervención del Estado en el ámbito de la libertad individual)… fue ejecutado pese a que no fue dispuesto en las actuaciones que dieron origen a esta causa, se apartó claramente de la ley reglamentaria del art. 18 CN, quebrantándose de ese modo la garantía constitucional protectora del domicilio*".

Sentado ello, recordemos que la doctrina acudió al criterio de *expectativa razonable de privacidad* para zanjar la cuestión de la relación de tensión entre la injerencia razonable y el derecho a la privacidad. Para ello ha elaborados dos criterios para definir el concepto de "expectativa razonable de privacidad": 1) que el individuo haya actuado de manera tal de exhibir un interés de mantenerlo, y 2) dicha expectativa de privacidad deberá ser soportada por el Estado como razonable[11].

En tal sentido, la garantía de la inviolabilidad de las comunicaciones ha sido interpretada de manera dinámica a la luz de los avances tecnológicos. En el caso de las conversaciones telefónicas convencionales, el precedente "Katz v. United States" [12] sentó las bases del ámbito de tutela extendido a las conversaciones mantenidas por ese medio y forjó el sentido y el alcance del secreto de las comunicaciones. A partir de ese precedente resultó claro para todos que en una comunicación telefónica, al igual que en el envío de una carta epistolar, existe una expectativa razonable de reserva en el contenido de las comunicaciones establecidas entre el emisor y su destinatario.

Incluso la Corte Suprema de ese país ha extendido la expectativa razonable de privacidad sobre el contenido de los datos almacenados en un celular al considerar que esos dispositivos operan como minicomputadoras que almacenan una enorme cantidad de información personal y sobre la cual el individuo tiene un derecho a la

[11] Alejandro D. Carrió, *Garantías Constitucionales en el Proceso Penal*, 5.a. ed., Editorial Hammurabi, pág. 438.

[12] 389 US 347 (1967)

reserva compatible con los avances técnicos en la era digital. Este fue el caso de "Riley vs. California"[13] y "United States vs. Brima Wurie"[14].

En el primero de ellos, personal policial secuestró y reviso información almacenada en el teléfono celular tipo "Smart Phone" perteneciente a Riley, quien había sido recientemente detenido por el delito de portación de arma de fuego verificada durante un control vehicular. Fue así, que mediante esa pesquisa ilegal se obtuvieron fotos y videos que vinculaban a Riley con una pandilla callejera denominada "The Bloods" y finalmente se logró atribuirle su participación en un tiroteo y asalto que concluyó con la muerte de una persona.

Por otra parte, en el caso "Wurie" el imputado había sido detenido por su vinculación con el tráfico de drogas y personal policial secuestró dos teléfonos celulares de su pertenencia, y procedieron a revisar el contenido sin orden judicial. Así, por medio del análisis de llamadas efectuadas lograron identificar un abonado agendado como "my house" y luego de verificar la dirección correspondiente a ese número telefónico, se realizó un allanamiento (con la debida orden judicial) que culminó con la detención de otra persona y el secuestro de estupefacientes.

Como observamos, ambos casos se focalizaron en la búsqueda de información almacenada en un teléfono celular inteligente por parte de las fuerzas de seguridad sin contar con la debida orden judicial que así lo disponga. Fue así, que la Corte Suprema de Justicia de los EEUU entendió que el examen del contenido de los datos almacenados en un teléfono celular de una persona detenida debía ser precedido de una orden judicial que autorizara el registro de esa información.

Así en esos precedentes el máximo tribunal de ese país sostuvo que "*una de las más notables características de los modernos teléfonos celulares es su inmensa capacidad de almacenaje. Antes de la existencia de los teléfonos celulares, el registro de una persona estaba limitado generalmente por la existencia física y tendía a constituir una estrecha intrusión en la privacidad…La mayoría de las personas no pueden cargar consigo cada carta recibida en los últimos meses, toda foto que toman, o todo libro o artículo que leyeron, tampoco habría una razón para hacerlo. Y si lo hicieran, deberían arrastrar detrás de ellos un baúl que estaría sujeto a una orden de requisa… Finalmente, hay un elemento dominante que caracteriza a los teléfonos celulares, pero no a los registros físicos. Antes de la era digital, las personas no llevaban consigo*

[13] 573 US 132 (2014)

[14] 573 US 212(2014)

información personal sensible. Ahora la persona que no lleva consigo un celular, con todo lo que el celular contiene, constituye una excepción".

Por último, debemos destacar que el resguardo de la privacidad de los individuos resulta además correlativo del principio de reserva establecido en el art. 19 de la CN, el cual reza: "*Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe*". En tal sentido, lo que se busco fue otorgarle cierta inmunidad al conjunto de acciones que desenvuelven los seres humanos, exentas de la autoridad judicial, que podemos llamar "acciones privadas", como es el caso de una comunicación telefónica.

En tal contexto, la doctrina incluso ha entendido que "*El concepto de privacidad elaborado y desarrollado durante décadas a través de la doctrina y la jurisprudencia atraviesa en la actualidad un período de crisis como consecuencia de la irrupción de los medios informáticos en la moderna sociedad tecnológica. La expectativa de privacidad en las redes telemáticas se ha contraído de manera grave por las posibilidades crecientes de injerencias extrañas. Lo que una sociedad entendía hace varias décadas atrás como una expectativa razonable de privacidad, ha quedado en cierta medida desactualizado gracias al avance de la tecnología y las posibilidades crecientes de comunicación intersubjetiva entre los integrantes de la sociedad. El almacenamiento masivo de datos, registros y documentos por parte de las empresas prestadoras del servicio de Internet y el interés desbordante de los gobiernos por esa big data acorrala de manera subrepticia el derecho de privacidad de las personas. El concepto de privacidad ya no puede ser asimilado a lo que un individuo puede o no hacer dentro de su domicilio o al derecho de exclusión de terceros.*"[15]

En este lineamiento, y como ya he adelantado el avance de la tecnología presenta nuevos desafíos para analizar a la luz de los arts. 18 y 19 de la CN y establecer si se pudieran encontrar abarcados por ese amparo constitucional.

III.- La video vigilancia y su marco normativo

El principal tema para abordar en el presente y que es un resultado del avance de la tecnología, es sin lugar a duda, la video vigilancia. La misma, encuentra diversas facetas y en la que nos vemos inmiscuidos en la vida cotidiana desde las cámaras de monitoreo instaladas en toda la ciudad, las cámaras de reconocimiento facial que se encuentran en estaciones de tren y subte, sistema de lectura de datos

[15] *Técnicas de Investigación y Vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información*, Gustavo Eduardo Aboso, elDial.com – DC2325

biométricos y hasta las cámaras de lectura de patentes de vehículos instaladas en distintos puntos estratégicos de la ciudad. Las personas en su vida cotidiana desarrollan inmensidad de actividades que implican, lógicamente, trasladarse por la vía pública. Sin embargo, no son conscientes de que existe un monitoreo constante por parte del Estado sobre sus actividades.

Si bien existe un marco normativo que respaldan ese tipo de pesquisas por parte del Estado, no menos cierto es que corresponde analizar detenidamente los alcances de ello y para lo cual en primer lugar hare un rápido abordaje sobre el marco normativo previsto para la video vigilancia.

En el ámbito nacional encuentra regulación en la resolución 283/2012 del Ministerio de Seguridad de la Presidencia de la Nación y su anexo complementario; y la disposición 10/2015 de la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos de la Presidencia de la Nación. Ambas en consonancia con la ley 24.059 de Seguridad Interior.

Mediante la resolución 283/12 se aprobó el reglamento para el Protocolo General de Funcionamiento de Videocámaras en Espacios Público en el que se establece que es el Ministerio de Seguridad el ente encargado de controlar y supervisar los centros de monitoreo de video vigilancia respetando el derecho de privacidad de los individuos.

Asimismo, establece que la finalidad de las imágenes captadas es "*La utilización y posterior tratamiento de imágenes que se obtengan, tendrán como finalidad exclusiva contribuir a la prevención y conjuración de ilícitos, brindando un aporte probatorio relevante para la investigación judicial, apreciando el derecho humano a la seguridad como valor esencial propio de un Estado de Derecho y una sociedad democrática para la protección de derechos, libertades y garantías de las personas.*".

Por otra parte, mediante la ley 5688 de la Ciudad de Buenos Aires se adhirió a la ley nacional 24.059 de Seguridad Interior. En el art. 474 de la ley 5688 se creó el **Sistema Público Integral de Video Vigilancia** de la Ciudad de Buenos Aires destinado a grabar imágenes en lugares públicos y cuya autoridad de aplicación es el Ministerio de Justicia y Seguridad de la CABA.

El art. 476 de la mencionada ley sostiene que **"***La utilización del sistema integral de video vigilancia 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 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, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública.

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

Los principios rectores del Sistema Integral de Video Vigilancia conforme el art. 477 de la ley 5688 son:

- Planificación estratégica: se rige por medio de planes de acción basados en criterios estratégico institucionales que son comprobados mediante los ejercicios de la gestión.
- Tecnología e innovación: promueve el uso intensivo de nuevas tecnologías para el abordaje de sus funciones y la mejora de la gestión institucional.
- Información estadística confiable: reúne registros de datos sobre la estadística y de los mapas de ocurrencia de hechos delictivos, a los efectos de desarrollar informes eficaces y oportunos sobre la materia en la Ciudad de Buenos Aires.
- Coordinación: articula su esfuerzo operacional con el resto de los componentes que intervienen en el sistema integral de seguridad pública.

En el contexto del Sistema Público Integral de Video Vigilancia y en apoyo en el principio rector de "Tecnología e Innovación" antes mencionado se ha impulsado el Decreto PEN N° 1766/11 (modificado por Decreto PEN N° 243/17) el cual creó el "Sistema Federal de Identificación Biométrica para la Seguridad" (SIBIOS), a fin de contribuir a la identificación de personas mediante información brindada a sistemas automatizados de identificación de huellas digitales y rostros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad.

Dicha resolución sostiene que "*Que el SISTEMA FEDERAL DE IDENTIFICACION BIOMETRICA PARA LA SEGURIDAD (SIBIOS), cuya implementación se propicia a través de esta medida, posee como finalidad principal instrumentar un servicio informático para permitir la comprobación idónea y oportuna de identificación de personas y rastros para fines de seguridad pública y de investigación judicial, contribuyendo al*

desarrollo de políticas eficientes de prevención y conjuración de ilícitos en el ámbito de la seguridad ciudadana y al mejoramiento de las diligencias investigativas requeridas por autoridades judiciales."

Asimismo, establece que la autoridad de aplicación es el Ministerio de Seguridad y los usuarios de dicho sistema son las fuerzas de seguridad.

Cabe recordar que dentro del plan "Tribuna Segura" lanzado por el Estado se estableció un nuevo régimen de seguridad para espectáculos futbolísticos mediante el decreto N° 246/17 y por medio del cual se instruye al Ministerio de Seguridad a dictar un nuevo Reglamento de Prevención contra la Violencia en Espectáculos Futbolísticos.

Asimismo, mediante resolución 355/17 el Ministerio de Seguridad aprobó un nuevo Reglamento de Prevención contra la Violencia en Espectáculos Futbolísticos, el cual se encuentra en el anexo complementario de dicha resolución (ANEXO IF-2017-06658355-APN-JGA#MSG). El art. 11 de dicho reglamento establece que "*El Organizador deberá comprobar la identidad de los concurrentes a un espectáculo futbolístico a través de la presentación del Documento Nacional de Identidad (D.N.I.) o Pasaporte, según el caso, o identificación biométrica, sin perjuicio del control que pudiese llevar adelante la DIRECCIÓN NACIONAL DE SEGURIDAD EN ESPECTÁCULOS FUTBOLÍSTICOS."*

Como vemos dicho reglamento autoriza a las fuerzas de seguridad a efectuar controles de índole biométrica a los ingresantes a espectáculos futbolísticos, tal cual sucede en la propia experiencia de concurrir a eventos de esas características.

En igual sentido, mediante resolución N° 398/MJYSGC/19 se creó el sistema de Reconocimiento Facial de Prófugos y cuyo funcionamiento quedo regulado por el anexo IF-2019-12925085-GCABAMJYSGC.

Dicho sistema conforme dicha resolución consiste en utilizar una cámara de video vigilancia para reconocer los rostros de las personas requeridas por orden judicial, registradas en las Bases de Datos del Sistema de Consulta Nacional de Rebeldías y Capturas (CONARC) del Registro de Reincidencia del Ministerio de Justicia y Derechos Humanos de la Nación. Asimismo, se establecido que dicho programa opere en el Centro de Monitoreo Urbano de la Policía de la Ciudad de Buenos Aires, dado que cuenta con los medios técnicos necesarios, personal idóneo para su correcta aplicación, y posee competencia respecto al Sistema Público Integral de Video Vigilancia de la Ciudad Autónoma de Buenos Aires;

Como mencionara se encuentra regulado en el anexo IF-2019-12925085-GCABAMJYSGC y en su art. 2 sostiene que "*El Sistema de Reconocimiento Facial de Prófugos será empleado únicamente para tareas requeridas por el Ministerio Público Fiscal, el Poder Judicial de la Nación, Provincial y de la Ciudad Autónoma de Buenos Aires, como así también para detección de personas buscadas exclusivamente por orden judicial, registradas en la Base de Datos de Consulta Nacional de Rebeldías y Capturas (CONARC). Salvo orden judicial, se encuentra prohibido incorporar imágenes y registros de otras personas que no se encuentren registradas en el CONARC*".

A su vez, en su art. 3 sostiene que la base de datos del CONARC únicamente estará nutrida de personas que registren una orden restrictiva de la libertad por autoridad competente.

Finalmente, en el art. 5 de ese anexo se sostiene que "*Todo archivo que se genere a partir de la ejecución del Sistema de Reconocimiento Facial de Prófugos quedará en poder de la autoridad policial y recibirá el tratamiento que corresponda de acuerdo con sus protocolos en materia de seguridad, privacidad y confidencialidad*" y en su art. 8 que "*una vez cumplida la orden judicial de restricción de la libertad, o que la misma haya cesado, los datos personales tratados deberán ser destruidos. Todo ello en consideración a los principios que emanan del Título III de la Ley Nº 1845 de Protección de Datos Personales y de la Ley Nacional Nº 25.326*".

Por último, en el marco de la ley del Sistema Público Integral de Video Vigilancia se celebró con fecha 7 de junio del 2016 el convenio 2016-14886349-AJG relacionado al tendido de fibra óptica, instalación de cámaras de seguridad para lectura de chapa patentes. Asimismo, mediante resolución 34/SECS/2018 se creó la División Anillo Digital de la Policía de la Ciudad a cargo del monitoreo de los sistemas de lectura de patentes instalados en la ciudad.

IV.- La video vigilancia como amenaza a derechos individuales

Luego de analizar el cuadro normativo del sistema de video vigilancia implementado por el Estado Nacional son dos cuestiones las que se disparan como incognitos a resolver. La primera de ellas, es si efectivamente existe una intromisión por parte del Estado en el derecho a la privacidad de los individuos, amparado constitucionalmente, y la segunda se relaciona al almacenamiento y tratamiento de los datos obtenidos de la videovigilancia (incognito que será tratado en otro apartado).

Por ello, comenzare con el análisis de la primera de las cuestiones y para la cual utilizare como disparador el art. 481 de la ley 5688 CABA, el cual reza: "*La*

captación y almacenamiento de imágenes en los términos previstos en este Libro, así como las actividades preparatorias, no se consideran intromisiones ilegítimas en el derecho a la intimidad personal y familiar y a la propia imagen, siempre y cuando no contradigan lo establecido en la Constitución Nacional, la Constitución de la Ciudad Autónoma de Buenos Aires, la Ley Nacional N° 25.326 y la Ley 1845".

De dicha lectura resulta llamativo que la propia ley de videovigilancia establezca que "*la captación y almacenamiento de imágenes …no se consideran intromisiones ilegitimas al derecho de la intimidad*" pues pareciera ser que el legislador notó cierto rose con libertades individuales que intento zanjar con la simple incorporación de dicho articulado. No menos cierto es que el artículo continúa diciendo que ello es así siempre y cuando no contradigan lo establecido en la Constitucional Nacional, y de este modo anula, en cierto modo, lo escrito con anterioridad. Claro está que el control de las garantías constitucionales se encuentra bajo la órbita del Poder Judicial y no del Poder Legislativo por lo que no es posible determinar por ley que una determinada actividad no resulta ilegítima y violatoria de derechos constitucionales. Esta circunstancia claramente fue percibida por el legislador e intentó corregir dicha circunstancia agregando la ya citada parte del artículo que alude a la Constitución Nacional.

En definitiva, con este análisis queremos dejar a salvo que la simple redacción del art. 481 de la ley 5688 de CABA en nada obsta a efectuar un análisis profundo y concreto en relación a sí las acciones que toma el Estado en el marco del cumplimiento de dicha ley pueden ser violatorias del derecho a la privacidad de las personas.

El avance de la tecnología como es el caso de la videovigilancia aplicada a la seguridad de la Nación actúa, en muchos casos, de modo sigiloso, sin siquiera que los individuos se percaten de ello. Es decir, que cuando una persona se traslada con su vehículo, se registran los lugares, días y horarios que transita habitualmente, o incluso cuando lo hace caminando puede ser seguido por las cámaras que existen instaladas en casi todas las cuadras de la ciudad o bien puede ser escaneado su rostro a la hora de tomar un tren a efectos de ser comparado con una base de datos de delincuentes y hasta individualizarlo mediante un sistema de datos biométricos al ingreso de estadios deportivos. Todo ello, ocurre de modo sistemático y sin siquiera que reparemos a pensar si ello implica o no un avance sobre nuestro derecho a la intimidad, pues no somos conscientes de que cada movimiento que hacemos es controlado por el Estado en una constante vigilancia.

Este accionar *sigiloso* de la tecnología sobre las personas impone la necesidad de encontrar casos análogos a ellos pero en otro momento de la historia, es decir cuando estos avances tecnológicos no existían y para de ese modo desentrañar si efectivamente existe una expectativa de privacidad en esas acciones que son tan habituales para los seres humanos.

Las cámaras instaladas en casi toda la ciudad que se encuentran dentro del programa de Sistema Público Integral de Video Vigilancia (ley 5688 CABA) si bien dependen del Ministerio de Justicia y Seguridad de la Ciudad, son operadas por el Centro de Monitoreo Urbano de la Policía de la Ciudad. La ley establece que las grabaciones se resguardaran por 60 días sin perjuicio de lo cual el Centro de Monitoreo Urbano compulsa las cámaras en tiempo real para contribuir a la detección de hechos ilícitos y prevención de los mismos.

Esto último implica que mediante las numerosas cámaras instaladas en la ciudad pueda efectuarse el seguimiento de un individuo mientras se traslada por la vía pública de modo imperceptible. Como manifesté anteriormente buscar un caso análogo, pero en otra época de la historia quizá nos ayude a echar luz a la cuestión. Un ejemplo de ello, podría ser el seguimiento por parte de personal policial a un determinado individuo, pero ahora ese accionar dejó de ser sigiloso, quizá sea advertido por el sujeto que es perseguido y se cuestione si ello no resulta intimidatorio y consiste en una violación a su derecho a la privacidad y a la libertad física.

Pareciera ser que el segundo de los casos es más invasivo a nuestra intimidad, que el seguimiento por cámaras de seguridad. La presencia física de un uniformado persiguiéndonos, no es algo que pueda agradarle a nadie y sin embargo, ese control es exactamente el mismo que el que se efectúa atrás de una cámara con la diferencia de que no resulta perceptible para nosotros.

Situaciones similares han implicado la presentación de habeas corpus[16] en resguardo de la libertad personal y consagrada en el art. 43 de la CN, lo que demuestra que el segundo caso quizá sea mucho más agresivo para un individuo

[16] En la causa "Cavolina" JA, 1968-I-44, se interpuso acción de habeas corpus debido a que personal policial se presentó en el domicilio de Cavolina informándole que su comparendo era requerido en la seccional policial, pero al no existir motivos para ello, lejos de concurrir a la seccional, interpuso una acción de habeas corpus considerando que no existían motivos que justificaran acciones persecutorias contra su persona.

por el solo hecho de que lo percibe, pero igual de invasivo a su intimidad que la videovigilancia.

Otro supuesto que preocupa respecto a la videovigilancia son los casos en que las cámaras de seguridad son apuntadas directamente a la puerta de un domicilio particular para pesquisar a un individuo. Si bien pareciera ser que la cámara no va a captar las acciones que efectúe una determinada persona en el interior de su vivienda no menos cierto es que se pueden determinar los días y horarios de entradas y salidas tanto de esa persona como de su grupo familiar como así también que personas visitan ese domicilio. Corresponde una vez más analizar si ello no puede ser violatorio del derecho a la privacidad y para lo cual recurriré nuevamente a ejemplos que puedan ser análogos a ello.

Un ejemplo que podría equipararse a esa conducta es: la solicitud de registros telefónicos como llamadas entrantes y salientes. Este caso, se asemeja a mi entender dado que los registros telefónicos como lo son las llamadas entrantes y salientes (como explicara en el capítulo sobre derecho a la privacidad) se encuentran protegidos por el art. 18 de la CN sin perjuicio de que esos registros no implican revelar el contenido de una comunicación telefónica pero sí el flujo de las mismas y la identidad de las personas con las que se contacta. Del mismo modo, una cámara de video apuntada a un domicilio en donde registra días y horarios de entradas y salidas de personas, deberían también ser abarcadas por el art. 18 de la CN.

Recordemos que la solicitud de registros telefónicos se encuentra bajo la órbita de un juez por auto fundado tal como reza nuestro art. 263 del CPP, segundo párrafo (incorporado por el art. 7 de la ley 25760).

En los precedentes emitidos por nuestra Corte Suprema de Justicia en los casos "Halabi" y "Quaranta" (citados en el capítulo I) la Corte hace una interpretación extensiva del art. 18 de la CN a nuevos tiempos y para lo cual aborda las comunicaciones telefónicas.

Así, en "Quaranta" la Corte sostuvo que "*al referirse al art. 18 de la Constitución Nacional, ha expresado que en él se consagra el derecho individual a la privacidad del domicilio de todo habitante Correlativo al principio general del art. 19 en cuyo resguardo se determina la garantía de su inviolabilidad, oponible a cualquier extraño, sea particular o funcionario público" (ver "Fiorentino" Fallos: 306:1752). Si bien allí no se hizo mención a las comunicaciones telefónicas ni a la protección de su secreto, una interpretación dinámica de su texto más lo previsto en su artículo 33 y en los artículos 11, inciso 2°, de la Convención Americana sobre Derechos*

Humanos, y 17, inciso 1°, del Pacto Internacional de Derechos Civiles y Políticos, en cuanto contemplan, en redacción casi idéntica, que nadie puede ser objeto de injerencias arbitrarias en su vida privada, en la de su familia, en su domicilio o en su correspondencia, permiten hacer extensivas aquellas consideraciones a casos como el presente."

Del mismo modo, la Corte ha sostenido en "Halabi" que "*En relación con los aspectos reseñados resulta oportuno señalar que las comunicaciones a las que se refiere la ley 25.873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúa contra toda "injerencia" o "intromisión" "arbitraria" o "abusiva" en la "vida privada" de los afectados (conf. art. 12 de la Declaración Universal de Derechos Humanos y art. 11, inc. 2°, de la Convención Americana sobre Derechos Humanos y tratados, ambos, con jerarquía constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional y art. 1071 bis del Código Civil). 24)".*

Dicho ello, no cabe duda que nuestra Corte Suprema de Justicia de la Nación ha hecho una interpretación dinámica y extensiva del art. 18 de la CN que ha abarcado las comunicaciones telefónicas y la totalidad de registros que se almacenen en relación a ellas.

Asimismo, un caso trascedente en cuanto a la vigilancia electrónica y que se relaciona con el supuesto analizada es "United States v. Cuevas-Pérez"[17] de la Corte Suprema de Justicia de EEUU. En el dicho caso, el imputado estaba siendo investigado por tráfico de drogas y para lo cual se instaló un sistema de videovigilancia en la proximidad de su domicilio y se colocó un GPS en su automóvil particular, todo ello sin orden judicial, y con el objeto de registrar sus movimientos habituales. Finalmente, la Corte concluyó que existió una violación al derecho a la privacidad amparado por la Cuarta Enmienda.

Es por ello por lo que, a nuestro entender, este mismo alcance deberían tener casos como el señalado en el que una cámara de vigilancia se apunta intencionalmente a un domicilio con el objeto de observar con detalle el movimiento de una determinada persona, claramente se encuentra dentro de la esfera de privacidad de las personas.

Asimismo, otro avance tecnológico muy peculiar son los lectores de patentes instalados en puntos estratégicos de la ciudad cuyo fin inicial fue disparar una alerta

[17] 640 F. 3d 272 (7th Cir. 2011)

respecto a un rodado que posea pedido de secuestro activo pero lo cierto es que además se guarda un registro de la totalidad de vehículos que pasaron por un lector de patentes determinado. Ello, implica que el Estado puede saber con detalle los movimientos que efectuamos cuando nos trasladamos en un automóvil, pudiendo obtener un patrón de conducta respecto a los lugares a los que concurrimos a diario y los horarios en que lo hacemos.

Es decir que el Estado cuenta con una base de datos sobre la totalidad de movimientos que efectuamos al momento de trasladarnos con nuestros vehículos y no mucho se sabe sobre el correspondiente resguardo de esa información personal, circunstancia que tratare con mayor amplitud más adelante.

Volviendo al esquema de ejemplos análogos podría sostenerse que este nuevo sistema de lector de patentes podría asemejarse a la ubicación que disparan los teléfonos celulares al efectuar una llamada mediante el impacto en una antena celular. Es decir, en ambos casos, se revela la ubicación de una persona ya sea por el impacto de un llamado en una antena determinada o bien por el paso con un vehículo por un lector de patentes ubicado en un lugar específico; toda información que se almacena en una base de datos. Asimismo, en ambos casos no existe un consentimiento expreso por brindar esa información, sino que se almacena compulsivamente, el único método para evitarlo sería, en un caso, no utilizar teléfono celular y en el otro no trasladarse con un vehículo por la ciudad.

En tal sentido, corresponde traer a colación un antecedente jurisprudencial de la Corte Suprema de Estados Unidos "Carpenter vs. United States"[18] en donde se ha hecho una interpretación extensiva de la "expectativa razonable de privacidad".

En dicho antecedente jurisprudencia se analiza la evolución sobre la "expectativa razonable de privacidad" y sostiene que el desarrollo de la tecnología ha requerido la forma de preservar la privacidad por parte de acciones de Estado, cuando dichos avances han mejorado la capacidad de invadir áreas que anteriormente se encontraban protegidas. Asimismo, menciona que la tecnología ha tenido grandes cambios y hoy en día ello implica la posibilidad de obtener una crónica de la presencia de una persona compilada día a día, en cada momento por varios años.

Puntualmente se analiza el caso del impacto de llamadas celulares en determinadas antenas que revelan la ubicación de una determinada persona. En tal

[18] 585, US (2018)

sentido, afirma que como el seguimiento de un automotor con GPS[19] la información que trasfiere el celular es detallada y compilada fácilmente y que pocos podrían haber imaginado que un aparato inalámbrico iría transmitiendo un registro detallado de los movimientos que las personas efectúan a diario. Además, hace hincapié en que la información de ubicación que otorga el celular no es compartida verdaderamente al efectuar un llamado dado que el teléfono móvil es indispensable para participar de la sociedad moderna y que por su naturaleza automática no hay forma de eludir ese registro salvo desconectando el mismo de la red. De este modo permite un estado de vigilancia policial constante.

Finalmente, la Corte de EEUU entendió que en cuanto a la "expectativa razonable de privacidad" existe un interés sobre la privacidad de esos datos que hacen a la ubicación de la persona siendo razonable que una sociedad no registre los movimientos de una persona. **Esos datos proporcionan una ventana a la vida íntima de una persona, revelan no sólo sus movimientos sino también sus asociaciones familiares, políticas, profesionales, religiosas y sexuales[20].**

En conclusión, para la mayoría de la Corte Suprema de EEUU, el gobierno necesita una orden judicial basada en *causa probable* para acceder al historial de ubicación del teléfono celular dado que ello resulta una búsqueda bajo la IV Enmienda.

Como explicara anteriormente los lectores de patentes ubicados en la ciudad recopilan información personal de modo detallado y sistemático generando una especie de crónica sobre los individuos en una base de datos. Además lo cierto es que las personas no prestan consentimiento explícito sobre revelar su ubicación al paso de cada uno de esos lectores de patentes, encontrándose así acorralados entre rehusar del derecho a la libertad ambulatoria (art. 14 de la CN) o su derecho a la privacidad dado que el único modo de evitar ese seguimiento es el de no trasladarse libremente con el uso de un rodado automotor. En definitiva y tal cual se sostuvo en el precedente "Carpenter vs. United States" considero que en este caso existe una expectativa de privacidad, al igual que la ubicación que dispara un llamado telefónico por el impacto en una antena de telefonía celular, dado que esos datos revelan una ventana a la vida íntima de las personas.

---

[19] El rastreo por GPS sin orden judicial ya ha sido tachado como violatorio al derecho a la privacidad en el antecedente "Estados Unidos v. Jones" 132 S. Ct 945, 2012.

[20] *Litigación penal II. Tecnología v. Garantías. Evidencia digital. Intimidad, privacidad y comunicaciones. Regulación procesal en la provincia de Entre Ríos y evolución de la Jurisprudencia del Tribunal Europeo de Derechos Humanos y la Corte Suprema de Estados Unidos,* Chaia Rubén A., elDial.com - DC275B.

Es así, que cualquier método tecnológico que almacene en modo sistemático y detallado, datos personales de los individuos como lo es lo es su ubicación deberían estar amparados por el art. 18 de la CN.

Finalmente, una de las tecnologías más impresionantes que se han aplicado a la seguridad en estos tiempos, son sin lugar a dudas los sistemas de identificación biométrica utilizados por ejemplo al ingreso de estadios deportivos y las cámaras de reconocimiento facial instaladas principalmente en las estaciones de tren y subte de la ciudad. Con esta última, se escanean los rostros de la totalidad de individuos que pasan allí con el objeto de ser cotejadas con la base de datos del CONARC que se encuentra compuesta por personas con poseen ordenes restrictivas de su libertad.

El grave problema en el uso de esta tecnología es que a partir de un rostro individualizado o el cotejo biométrico por huellas dactilares, existe un montón de información personal que puede obtenerse como ser el lugar en donde fue tomado dicha fotografía, huella (o cualquier otra información que hace identificable a la persona), es decir saliendo de una iglesia o de un estadio de futbol, el modo de vestir, entre otras cosas que permiten efectuar un perfil de cada individuo.

Con respecto a las cámaras de reconocimiento facial, si bien el cotejo con una base de datos que únicamente posea personas con órdenes de detención pareciera llevar tranquilidad a los individuos lo cierto es que existe un margen de error en el escaneo de los rostros o en la carga de datos[21] que ha implicado detenciones a personas únicamente por el parecido que tenían con un prófugo y en definitiva ha implicado un grave avasallamiento sobre su libertad individual.

Además ese error ha generado no solo una detención ilegitima sino que se ha guardado su imagen en una base de datos por considerar que resultaba ser un caso positivo y si bien la resolución que regula las cámaras de reconocimiento facial sostiene que una vez cumplida la orden judicial de restricción de la libertad, o que la misma haya cesado, los datos personales tratados deberán ser destruidos, lo cierto es que será un gran desafío saber si ello se cumple de acuerdo a la ley de protección de datos personales, tema que abordare más adelante.

Debemos recordar que si bien el uso de esta tecnología ha llegado a nuestro País como un gran avance en seguridad en otros países del mundo como EEUU,

[21] https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien
https://www.pagina12.com.ar/223372-camaras-de-reconocimiento-facial-larreta-prometio-10-000-mas

ya cuestionan el funcionamiento de este tipo de tecnología debido a su intromisión en la intimidad de las personas[22]. Incluso, en Francia la justicia prohibió la vigilancia por parte de personal policial con la utilización de "drones" dado a la gran capacidad de obtener imágenes que permitan identificar a las personas y en definitiva estaban abarcadas por la ley de procesamiento de datos personales[23].

En definitiva, no es acorde a nuestras libertades individuales vivir con miedo a que una cámara de reconocimiento facial nos confunda con un prófugo con todos los perjuicios que ello atrae, atentando de este modo no solo nuestro derecho a la privacidad sino también de nuestra libertad ambulatoria.

En este caso, puntual creo que la posibilidad de error en cuanto a arrojar un falso positivo por parte del software que utilizan las cámaras de reconocimiento facial es un riesgo demasiado grande que no podemos correr. Más adelante, tratare este caso de modo puntual, y que debo separar de momento del resto de los casos enunciados, pues a mi entender la utilización de dicha tecnología sin existencia de una sospecha de criminalidad hacia los individuos significa no solo un avance contra su derecho a la intimidad sino también la aplicación de los principios de un derecho penal del enemigo con el agravante de que es aplicado a quien siquiera ha infringido norma alguna.

La particularidad de los avances tecnológicos como aquellos ya enumerados, es que debido a que el tratamiento de datos se encuentra informatizado surge la posibilidad de efectuar cruce de datos entre ellos, lo que sin lugar a dudas potenciaría un mayor avance sobre la intimidad de los individuos y sobre otros derechos fundamentales. Es decir, que no solo el Estado puede efectuar un seguimiento con una cámara de seguridad sobre una persona a la vez que le efectúa un escaneo de reconocimiento facial o biométrico, sino que también puede registrar los movimientos que hace con su rodado en una base de datos y quizá saber con las personas que se reúne en su domicilio, y los días y los horarios en que lo hace por medio de una cámara apuntando a la puerta de su vivienda.

En tal sentido, considero que la sumatoria de esos avances tecnológicos que "*espían*" sigilosamente la vida de las personas constituye una afectación al derecho a la privacidad de éstas.

---

[22] https://elpais.com/tecnologia/2019/05/15/actualidad/1557904606_766075.html

[23] file:///C:/Users/HP%20I3/Desktop/L%C3%94%C3%87%C3%96+%C3%ABtat%20condamn+%C2%AE%20+%C3%A1%20cesser%20de%20surveiller%20Paris%20par%20drones%20%20Droit%20&%20Technologies.html

Ello, es así toda vez que a mi entender existe una expectativa de privacidad por parte de los individuos en cuanto a que el Estado no debe inmiscuirse en los movimientos que cada uno de ellos hace en su vida cotidiana sin que exista una *causa probable* que amerite una intervención de esa índole.

Es así que, como vengo sosteniendo el conjunto de avances tecnológicos ha puesto en jaque diversos derechos de los individuos que enumeraré a continuación:

- Derecho a la intimidad (art. 18 y 19, CN, art. 17 incs.1° y 2°, PIDCyP, art. 11 incs. 2° y 3°, CADH, art. 12, DUDH, y arts. V, IX, X, DADDH).
- Derecho a la dignidad e integridad física y moral de las personas (art. 5°, ptos. 1 y 2 y art. 11 pto.1, CADH, arts. 7° y 10, PIDCyP, art. 5°, DUDH, y art. I, DADDH).
- Derecho a la libertad ambulatoria (art. 14, CN; art. 7°, CADH; art. 9°, PIDCyP, art. 3°, DUDH, y art. I, DADDH).
- Derecho a no soportar injerencias arbitrarias o abusivas en la vida privada (art. 11 incs. 2° y 3° CADH, art. 17 incs. 1° y 2° PIDCyP, art. 12 DUDH y art. V de la DADDH).

Sin embargo, corresponde analizar si dicha afectación a la intimidad y a los demás derechos enumerados debe ser soportada por los individuos en pos de un bien superior y en su caso de qué modo debe llevarse a cabo; circunstancia que analizare a continuación.

V.- ¿Existencia de un bien superior que amerite la intervención Estatal? ¿Necesidad de contar con orden judicial?

Como quedo claro en el capítulo anterior los avances tecnológicos aplicados a la seguridad implican a su vez un avance sobre derechos individuales consagrados por nuestra Constitución Nacional. Sin embargo, no menos cierto es que los derechos individuales, aún aquellos con rango constitucional, no son absolutos.

Es de destacar, que el propio preámbulo de nuestra Constitución Nacional establece como uno de los fines de la misma "*promover el bienestar general*" y dentro de la búsqueda de ese bienestar general es posible que existan colisiones con derechos individuales.

Así, la ley 24.059 establece las bases para llevar a cabo la Seguridad Interior, que puede ser entendida como parte de esa búsqueda efectuada por el Estado para

lograr el bienestar general, y en sus primeros 3 artículos detalla el alcance de la seguridad interior, los cuales traeré a colación para mayor ilustración.

ARTICULO 1º — La presente ley establece las bases jurídicas, orgánicas y funcionales del sistema de planificación, coordinación, control y apoyo del esfuerzo nacional de policía tendiente a garantizar la seguridad interior.

ARTICULO 2º — A los fines de la presente ley se define como seguridad interior a la situación de hecho basada en el derecho en la 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.

ARTICULO 3º — La seguridad interior implica el empleo de los elementos humanos y materiales de todas las fuerzas policiales y de seguridad de la Nación a fin de alcanzar los objetivos del artículo 2º.

Recordemos que la ley 5688 del Sistema Integral de Seguridad Publica de la Ciudad Autónoma de Buenos Aires, la cual regula la Video Vigilancia, se dictó en consonancia con la ley Nacional de Seguridad Interior antes mencionada.

En definitiva, pareciera ser que el Estado está dispuesto a disminuir ciertas libertades individuales en pos del bienestar general. Sin embargo, el poder del Estado para garantizar la seguridad y el orden público tampoco es ilimitado. Con respecto a ello, la Corte Interamericana de Derechos Humanos sostuvo que la actuación del Estado "*está condicionada por el respeto de los derechos fundamentales de los ndividuos que se encuentren bajo su jurisdicción y a la observación de los procedimientos conforme a Derecho (...) con estricta sujeción a los procedimientos objetivamente definidos en la misma*"[24].

En el mismo, lineamiento nuestra Corte Suprema de Justicia de la Nación en el precedente "Halabi" recordó antecedentes en los que había sostenido "… *que sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen*"[25].

En este sentido, pareciera ser que juega un rol de suma importancia el carácter Republicano que tiene nuestro país, con una división de poderes a tal efecto. Si

[24] Corte Interamericana de Derechos Humanos. Serie C, n° 100, caso "Bulacio v. Argentina", sentencia del 18 de septiembre de 2003, ptos. 124 y 125; ver Fallos: 330:3801

[25] Fallos: 306:1892; 316:703.

bien el Poder Ejecutivo como jefe de las fuerzas de seguridad es el encargado de llevar a cabo la ley de Seguridad Interior y lograr el objetivo enumerado en el art. 2 de la ley no menos cierto es que el Poder Judicial es el encargado por excelencia de interpretar y hacer valer los derechos consagrados en nuestra Constitución Nacional.

En tal sentido, considero que en este sistema de pesos y contrapesos que nos propone nuestra Constitución Nacional, es correcto que el Poder Ejecutivo tome todas las medidas necesarias para cumplir con la Seguridad Interior pero no menos cierto es que cuando alguna de esas medidas implique la disminución de garantías constitucionales a los individuos debe requerirse una **ORDEN JUDICIAL** que así lo disponga para garantizar un Estado de Derecho.

Como vemos el avance de la tecnología ha otorgado un poder indescriptible al Estado, convirtiéndolo en un "Súper Estado" que todo lo ve y todo lo vigila en pos del bienestar general. Resulta indiscutible que la tecnología sea utilizada para colaborar con ese fin tan preciado como lo es el bienestar general pero no es posible utilizar al mismo como una caja de pandora para arrasar indiscriminadamente con los derechos individuales.

Por ello, considero que los avances tecnológicos deben ser tomados con suma cautela y en resguardo de los derechos constitucionales. Es decir, no propongo el retroceso tecnológico y la demolición de grandes avances que se han efectuado, pero sí un debido control de los mismos que garantice el cumplimiento de la Constitución Nacional, y dicho control deriva por lo menos en **dos mecanismos** que se potencian entre ambos.

El primero de ellos, es la necesidad de contar con una orden judicial para acceder a cualquier tipo de información personal que esté vinculada con la colocación de sistemas tecnológicos destinados a la seguridad, como lo son los seguimientos por cámaras a individuos, la fijación de las mismas a domicilios determinados, la solicitud de información a los "anillos digitales" y las comparaciones de rostro mediante un sistema de reconocimiento facial. Todas esas acciones del Estado son invasivas de la intimidad de los individuos afectando los arts. 18 y 19 de la CN por lo que es un Juez quien debe autorizar esa acción.

Con respecto a esto último, y como ya he mencionado en el capítulo sobre el derecho a la privacidad nuestros legisladores han optado por un sistema en que las intromisiones a la intimidad sean resueltas por los jueces dado que se encuentran en una posición más serena para resolver sobre ello. En tal sentido, de ello se

colige que si el personal policial actuara sin una orden judicial ese accionar debería como mínimo cumplir con los recaudos que demandan la existencia de motivos previos para actuar (art. 230bis y 284 del CPP). Es lógico, que exista una mayor exigencia para el personal policial para actuar sin orden judicial en materia de acciones que pueden resultar invasivas de la intimidad de las personas justamente porque el principio es que debe prevalecer la orden judicial, y la excepción actuar sin ella. De no ser así el personal policial carecería de motivación para conseguir una orden judicial dado que pensaría que es más lo que puede lograr sin ella.

Corresponde recordar las excepciones de los arts. 230bis y 284 del CPP que enunciare a continuación:

Art 230 bis. - Los funcionarios de la policía y fuerza de seguridad, sin orden judicial, podrán requisar a las personas e inspeccionar los efectos personales que lleven consigo, así como el interior de los vehículos, aeronaves y buques, de cualquier clase, con la finalidad de hallar la existencia de cosas probablemente provenientes o constitutivas de un delito o de elementos que pudieran ser utilizados para la comisión de un hecho delictivo de acuerdo a las circunstancias particulares de su hallazgo siempre que sean realizadas:

a) con la concurrencia de circunstancias previas o concomitantes que razonable y objetivamente permitan justificar dichas medidas respecto de persona o vehículo determinado; y,

b) en la vía pública o en lugares de acceso público.

Art. 284. - Los funcionarios y auxiliares de la policía tienen el deber de detener, aún sin orden judicial:

1º) Al que intentare un delito de acción pública reprimido con pena privativa de libertad, en el momento de disponerse a cometerlo.

2º) Al que fugare, estando legalmente detenido.

3º) Excepcionalmente a la persona contra la cual hubiere indicios vehementes de culpabilidad, y exista peligro inminente de fuga o de serio entorpecimiento de la investigación y al solo efecto de conducirlo ante el juez competente de inmediato para que resuelva su detención,

4º) A quien sea sorprendido en flagrancia en la comisión de un delito de acción pública reprimido con pena privativa de libertad.

Como es evidente la tecnología siempre avanza más rápido que la adaptación de la legislación vigente a la misma por lo que del mismo modo que nuestra Constitución Nacional no enumeraba a las comunicaciones telefónicas dentro del art. 18, hoy la videovigilancia no se encuentra regulada dentro de los códigos de procedimiento penal en cuanto a la necesidad de órdenes judiciales para estos supuestos. Debo hacer notar, que dicha inquietud ha sido observada por el legislador al momento de sancionar el nuevo Código Procesal Penal de la Nación (ley 27.063), suspendido por decreto PEN N° 257/15), el cual prevé en su art. 143 y ss, la necesidad de contar con orden judicial por ejemplo para la interceptación de correspondencia electrónica y para el registro de un sistema informático. Esas definiciones a la fecha siguen siendo limitadas para el gran alcance de nuestro art. 18 de la CN pero es un avance que no debemos dejar de mencionar.

Del mismo modo, en el mundo existe una tendencia para armonizar las normas procesales con el avance de la tecnología y la invasión de esta al derecho a la privacidad, pudiendo mencionar los siguientes ejemplos:

- Convenio sobre la Ciberdelincuencia de 2001 (STE N° 185), el cual dispone diversas normas procesales en materia de interceptación, tratamiento y almacenamiento de datos informáticos (art. 14 a 21).
- Código Procesal Penal Alemán, los §§ 94 y ss, establecen medidas probatorias para identificar a sospechosos de delitos graves sobre el entrecruzamiento de datos informáticos, y las cuales requieren autorización judicial (§ 98b). Asimismo, prevé medidas de seguimiento, registro fílmico y fotográfico del autor, todas las cuales deben ser homologadas por el juez (§100c y §100d)
- Ley de enjuiciamiento Criminal española, en su capítulo IV, del título VIII, establece las condiciones que se deben dar para disponer medidas limitativas de la privacidad de las personas como lo son interceptaciones telemáticas, y las cuales están sujetas a control judicial.

Como vemos, existe una tendencia en el mundo y en nuestro país para tratar de corregir el desfasaje entre las normas procesales y el avancen tecnológico. Sin embargo, por mucho que se esfuerce el legislador vemos que las normas procesales siempre quedan limitadas a comparación de los descubrimientos tecnológicos. Por otra parte, lo cierto es que a la fecha ni siquiera se encuentra vigente en nuestro país el nuevo código procesal penal por lo que debemos regirnos por las limitadas definiciones de la normativa procesal vigente que no contempla ningún caso relacionado a los avances de la tecnología que venimos mencionado.

Es por ello, que considero que para lograr sortear dicha cuestión, al menos por el momento, es que las fuerzas de seguridad para actuar sin orden judicial respecto a los recursos de videovigilancia existentes deben darse por lo menos algunos de los supuestos enumerados como excepcionales en los arts. 230bis y 284 del CPP. De no ser así deberá requerirse orden judicial sin más en resguardo de las garantías constitucionales.

El segundo de los mecanismos para garantizar las garantías constitucionales es que las bases de datos que almacenan información como los son las grabaciones de las cámaras de seguridad, los registros de los vehículos que pasan por los anillos digitales o bases de datos que recopilen información personal mediante el uso de datos biométricos, se encuentren a resguardo de entes independientes de las fuerzas de seguridad para garantizar la solicitud de una orden judicial para acceder a las mismas. Algo similar ocurre con los registros telefónicos dado que la información es almacenada por entes privados y requieren de órdenes judiciales para aportar esa información.

Es evidente que el monitoreo de las cámaras en aras de prevenir delitos debe estar en manos de las fuerzas de seguridad. Del mismo modo, resulta lógico que si un vehículo con pedido de secuestro activo pasa por un anillo digital se dispare una alerta a la Policía. Sin embargo, el posterior almacenamiento de la totalidad de datos relacionados a la video vigilancia podría ser resguardado por un ente independiente para asegurar el sistema de órdenes judiciales.

El caso más preocupante, a nuestro entender, es el almacenamiento sistemático por los lectores de patentes instalados en la ciudad dado que registran el paso de la totalidad de automóviles, lo que implica, como ya sostuve una crónica de la vida de los individuos. A su vez, dicha base de datos se encuentra a cargo de las fuerzas de seguridad y pueden efectuar consultas sin necesidad de contar con una orden judicial. Por ello, nuevamente se observa que lo más conveniente es que las bases de datos que recopilan información de modo sistemático por el uso de medios tecnológicos aplicados a la seguridad sean resguardadas por entes distintos a las fuerzas de seguridad.

En tal sentido, el hecho de que la información sea almacenada por un tercero con capacidad de acceder a esa información no disminuye la razonabilidad de la confianza de los usuarios de la privacidad de sus datos personales. Este criterio fue

utilizado en el precedente "United States v. Ackermann"[26] de la Corte Suprema de Justicia de EEUU.

VI.- Almacenamiento y tratamiento de datos personales como resultado de la video vigilancia

Como se explicara anteriormente, la recopilación de modo automático de datos personales es un hecho sumamente invasivo hacia las personas por lo que su almacenamiento y posterior tratamiento reviste un carácter de suma importancia a la hora de aplicar la video vigilancia. Por ello, sugerí la posibilidad de que esas bases de datos sean controladas por empresas privadas que no posean un interés determinado en el control de las actividades individuales del individuo como si las tiene el Estado en su rol de vigilar a la población. Ello, robustecería el sistema de órdenes judiciales que consideraron pertinentes nuestros constituyentes en el art. 18 de la CN.

Dichos datos se encuentran protegidos por la ley 25.326 de protección de datos personales. Si bien la mencionada ley en su art. 2° define los datos personales como "*Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables*" por lo que no cabe duda que se encontrarían abarcados por dicha ley los datos objeto de análisis debe tenerse en cuenta también la disposición 10/2015 del de la Dirección Nacional de Protección de datos Personales en donde esclareció con mayor precisión esa cuestión y establece que

"Que una imagen o registro fílmico constituyen, a los efectos de la Ley N° 25.326, es un dato de carácter personal, en tanto que una persona pueda ser determinada o determinable. Que una imagen con formato digital permite su tratamiento a través de sistemas informáticos y conformar un sistema organizado de fácil consulta. Que en razón de lo expuesto, un conjunto organizado de material fotográfico o fílmico en el que sea posible la identificación de personas constituye una base de datos sujeta al régimen de la LEY DE PROTECCIÓN DE LOS DATOS PERSONALES. Que, en consecuencia, debe considerarse que las

[26] 831, F. 3d 1292 (2016). El mismo aborda la problemática de un algoritmo utilizado por la empresa de servicios e-mail "AOL" para detectar el envío de correos electrónicos cuyo contenido es de pornografía infantil, accediendo así al contenido de los mensajes que posean esa alerta. La Corte Suprema de Estados Unidos entendió que existe una expectativa de privacidad en un correo electrónico, al igual que lo es una carta manuscrita, dado que en la actualidad las comunicaciones se efectúan por medios tecnológicos en su mayoría. Asimismo, entendió que la capacidad de un proveedor externo de acceder a información no disminuye la razonabilidad de la confianza de los usuarios en la privacidad de sus correos.

actividades de video vigilancia, esto es el tratamiento de imágenes digitales de personas con fines de seguridad, se encuentran alcanzadas por esta categoría de base de datos."

Asimismo, el decreto 1766/11 del Ministerio de Seguridad que crea el sistema SIBIOS sostiene que:

"Que valorando la importancia de todo dato biométrico y su equiparación en términos legales a los datos personales amparados por la Ley Nº 25.326, el funcionamiento del sistema integral propuesto respeta las pautas normativas en materia de procedimiento, tratamiento compatible, confidencialidad, protección y resguardo de información y cumplimiento exclusivo de la finalidad específica de su creación."

Del mismo modo, el art. 1 del reglamento complementario de la disposición 10/2015 sostiene que la recolección de imágenes digitales de las personas a través de cámaras de seguridad será licita en la medida que cuente con el consentimiento previo del titular del dato en los términos de los arts. 5 y 6 de la ley 25.326. Sin embargo, ese mismo artículo establece las siguientes excepciones:

Siempre y cuando la recolección de las imágenes personales no implique una intromisión desproporcionada en su privacidad, no será necesario requerir el consentimiento previo del titular del dato en los siguientes casos:

a) los datos se recolecten con motivo de la realización de un evento privado (se realice o no en espacio público) en el que la recolección de los datos sea efectuada por parte del organizador o responsable del evento;
b) la recolección de los datos la realice el Estado en el ejercicio de sus funciones, siendo en principio suficiente notificación de los requisitos del artículo 6° de la Ley N° 25.326 su publicación en el Boletín Oficial (conforme artículo 22 de la Ley N° 25.326); sin perjuicio de ello, en las oficinas y/o establecimientos públicos deberá hacerse saber dicha recolección conforme lo dispuesto en el segundo párrafo del presente artículo;
c) los datos se recolecten dentro de un predio de uso propio (por ejemplo: ser propiedad privada, alquilado, concesión pública, etc.) y/o su perímetro sin invadir el espacio de uso público o de terceros, salvo en aquello que resulte una consecuencia inevitable, debiendo restringirlo al mínimo necesario y previendo mecanismos razonables

> para que el público y/o los terceros se informen de una eventual recolección de su información personal en tales circunstancias.

Como vemos en el punto "b" se sostiene la excepción en cuanto a que el titular de un dato no debe prestar consentimiento en su recolección cuando la misma es efectuada por el Estado en ejercicio de sus funciones. Sin embargo, no menos cierto es que ello es así siempre y cuando no impliquen una intromisión desproporcionada en la privacidad de los individuos.

Como ya quedara asentado, considero que la recolección de datos de modo compulsivo mediante los distintos mecanismos de videovigilancia significa una intromisión a la privacidad en los términos del art. 18 de la CN.

Sin embargo, el modo recopilación sistemático y automatizado impediría la posibilidad de contar con un consentimiento expreso de los individuos sobre su recopilación por cuestiones prácticas. Por ello, podría sostenerse que sí existe un consentimiento implícito de quien pasa con su vehículo por un anillo digital, quedando registrada y almacenada en una base de datos esa información.

Ello, de modo alguno autoriza a compulsar esa información por parte del Estado, sino que deberán ser los jueces mediante órdenes judiciales quienes deberán, como explicara en el capítulo anterior, autorizar dicha intromisión en la vida privada de las personas. Pues los individuos si bien prestamos, quizás, ese consentimiento implícito debemos tener la seguridad de depositar la confianza de que esos datos se encuentran resguardados bajo los supuestos de la ley de protección de datos personales.

Lo que preocupa a mi entender no es tanto la recopilación de dichos datos sino el tratamiento de los mismos. Por eso, un sistema de contra pesos en donde el ente que recopile los datos no sea el mismo que aplique su debido tratamiento y compulsa aseguraría el sistema de solicitud de órdenes judiciales para obtenerlos como lo son los casos de las empresas telefónicas que recopilan ciertos registros y solo se otorgan a la autoridad competente por medio de una orden judicial.

En la actualidad véase que las fuerzas de seguridad además de su deber en cuanto a la prevención y represión de ilícitos se encargan de recopilar y el posterior tratamiento de datos relacionados a la videovigilancia. Pareciera que ello, puede ser algo positivo dado que dota de mayores herramientas a las fuerzas de seguridad para lograr su fin, sin perjuicio de lo cual la contra cara es una amenaza al sistema de órdenes judiciales, pues se podría caer en el error de pensar que no son

necesarias y es solo un trámite burocrático, pues no existe incentivo alguno de solicitarla cuando esa base de datos se encuentra en manos de la misma fuerza.

Un avance en este sentido, respecto a otros países del mundo, es el caso italiano en donde se sancionó la ley 675/1996, la cual procuró un punto de equilibrio entre la privacidad y el uso de dispositivos de videovigilancia al crear una autoridad independiente a modo de inspección, denuncia y comunicación en materia de protección de datos[27].

VII.- Las cámaras de reconocimiento facial y el derecho penal del enemigo

Podríamos sostener que el actual derecho penal del enemigo tiene sus orígenes en el especialista en derecho penal Franz Von Liszt, quien ha dejado una herencia que quizá nunca ni él hubiese imaginado.

Dicho jurista recibió diversas críticas por la cierta contradicción en sus teorías de política criminal y dogmática penal. Por un lado, promovió remplazar el derecho penal retribucionista por una concepción preventiva orientada a la idea del fin de la pena, la cual correspondía aplicar solo cuando era necesaria. Así, propuso la eliminación de penas privativas de la libertad de corta duración, la condena condicional, y la ampliación de penas de multa, orientadas a la recuperación del autor[28].

Pero, como contracara de ello, von Liszt, propuso una pena de tiempo indeterminado que tenía como fin la "neutralización" de los "incorregibles"[29].

Asimismo, sostuvo que la pena privativa de la libertad tenía una triple función: a) mejoramiento de los delincuentes necesitados de recuperación y susceptibles de lograrla, b) mera disuasión de los que no necesitan ser corregidos, c) neutralización de los delincuentes irrecuperables.

---

[27] Martínez Martínez, R, *Los ficheros de datos y archivo de imágenes policiales en la legislación italiana. Análisis de resoluciones dictadas por el garante italiano para la protección de datos personales*. Revista Española de derecho Constitucional, Año 20, Núm. 60, sept.-dic de 2000, pp. 179 y ss.

[28] Véase von Liszt, "Kriminalpolitische Aufgabe", en *Strafrechtliche Vorträge*,, pp. 290 ss.; *idem*, "Die Reform der Freiheitsstrafe", en *Strafrechtliche Vorträge*, pp. 511 ss.

[29] Esto fue expuesto en el denominado "Programa de Marburgo", véase Von Liszt, "Der Zweckgedanke im Strafrecht", en *Strafrechtliche Vorträge*, pp. 166 ss. Traducción al español de Enrique Aimone Gibson, con prólogo de Manuel de Rivacoba, Valparaíso, Chile, 1984, bajo el título *La idea de fin en el Derecho Penal.*

Así en el Programa de Marburgo de 1882, von Liszt sostuvo que *"La lucha contra la criminalidad consuetudinaria presupone conocimientos precisos acerca de la misma. Hoy todavía carecemos de ellos. Se trata de un eslabón, ciertamente del más significativo y peligroso, en aquella cadena de fenómenos sociales patológicos que acostumbramos resumir con el denominador común de proletariado. Mendigos y vagabundos, prostituidos de ambos sexos y alcohólicos, rufianes y personas de los bajos fondos en sentido amplio, degenerados física y psíquicamente; todos ellos constituyen el ejército de los enemigos principales del orden social, cuyo Estado mayor está constituido por los delincuentes habituales*[30]*."*

Incluso el citado jurista llego a sostener que "la pena de muerte me resulta superflua, tan pronto como los incorregibles sean neutralizados[31]".

Como vemos, la idea de la existencia de un derecho penal con todas las garantías del Estado de Derecho para el ciudadano "normal" y otro derecho penal sin límites ni garantías para el "incorregible", no es nueva y data por lo menos de hace cien años. Esta deformación del derecho penal ha generado consecuencias desastrosas que son mundialmente conocidas[32].

Asimismo, y pese a ello, este concepto fue reeditado por Gunter Jakobs, en lo que llamó *el derecho penal del enemigo* y establece que el Estado no dialoga con sus ciudadanos, sino que amenaza a sus enemigos, imponiendo penas desproporcionadas y especialmente recortando las garantías constitucionales[33].

Así Jakobs sostiene que "*el enemigo es un individuo que no solo de manera incidental, en su comportamiento (delitos sexuales) o en su ocupación profesional (delincuencia económica) , o principalmente a través de una organización (terrorismo delincuencia organizada, tráfico de drogas), es decir en cualquier caso, de una forma presuntamente duradera, ha abandonado el*

[30] Von Liszt, *op. cit.*, p. 167.

[31] Von Liszt, *op. cit.*, p. 173.

[32] Se advierte en Agamben, *Homo sacer, El poder soberano y la nuda vida*, Valencia, 2003, 217, que a la vista de los horrores sucedidos en los campos de concentración durante el Nacionalsocialismo, "la pregunta correcta no es requerir hipócritamente cómo fue posible cometer en ellos delitos tan atroces respecto a seres humanos; sería más honesto, y, sobre todo, más útil, indagar atentamente indagar sobre los procedimientos jurídicos y los dispositivos políticos que hicieron posible llegar a privar tan completamente de sus derechos y prerrogativas a unos seres humanos hasta el punto de que realizar cualquier tipo de acción contra ellos no se considerara ya como un delito".

[33] Jakobs, "*La ciencia penal ante los retos del futuro*", trad. De Teresa Manso en Eser/Hassemer/Burkhardt, *La ciencia del derecho penal ante el cambio de milenio*", Francisco Muñoz Conde (coord.), Valencia 2004, p. 53 y ss.

derecho y, por lo tanto, no garantiza el mínimo cognitivo de seguridad del comportamiento personal y demuestra este déficit a través de su comportamiento."[34]

Un claro ejemplo de este derecho penal del enemigo ocurrido en este siglo, en relación a la disminución de derechos fundamentales, fue la sanción de la Patriot Act en Estados Unidos como respuesta a los atentados terroristas del año 2001. En la misma, su art. 215 autorizaba al FBI a interceptar comunicaciones de cualquier naturaleza y realizar el monitoreo de eventuales grupos terroristas. En la actualidad ese apartado fue modificado por la Freedom Act[35].

La existencia de un derecho penal del enemigo en el mundo aún en la actualidad, es algo innegable y muestra tangible de ello lo son los centros de detención (sin orden judicial) con base en Guantánamo, incluso pese a los derechos de guerra establecidos en la Convención de Ginebra.

En tal sentido, el penalista alemán Mezger en el año 1943 sostuvo que "*en el futuro habrá dos o más derechos penales. Un derecho penal para la generalidad y un derecho penal (completamente diferente) para grupos especiales de determinadas personas como, por ejemplo, los delincuentes por tendencia.* Lo decisivo es en qué grupo debe incluirse a la persona en cuestión…*Una vez que se realice la inclusión, el "derecho especial" (es decir, la reclusión por tiempo indefinido) deberá aplicarse sin límites. Y desde ese momento carecen de objeto todas las diferenciaciones jurídicas…Esta separación entre diversos grupos de personas me parece realmente novedosa (estar en el nuevo orden; en el radica "nuevo comienzo").*[36]

Como vemos, este concepto de dos derechos penales aplicables según la clase de ciudadano no es nueva, independientemente de que se los clasifique como "incorregibles" (von Liszt), "extraños a la comunidad" (Mezger) o "enemigos" (Jakobs).

Así, sintéticamente podríamos definir, según esta teoría, que existe para el Estado un sistema de "*amigo/enemigo*" para diferenciar los derechos que a cada uno le corresponden.

---

[34] Ob. cit, pg. 59

[35] United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA Freedom), Act of 2015, publ. L. N° 114-23, 129 Stat. 268 (50 U.S.C. §§ 1872-1874, 2012, y 18 U.S.C. §§ 2280-2281, 2332, 2012. En la actualidad el art. 215 ha sido modificado por la USA FREEDOM ACT que dispone un límite de 180 días de vigilancia luego de lo cual es necesario la autorización judicial.

[36] Muñoz Conde, *Edmund Mezger y el derecho penal de su tiempo*, cit., p. 236.

Ahora bien, no consiste materia de este trabajo analizar si es adecuada o no la aplicación del derecho penal del enemigo[37] para aquellos sujetos que Jakobs menciona como enemigos (como por ejemplo los grupos terroristas) sino que tomando el sistema de "amigo/enemigo" antes mencionado preocupa que (salvando las distancias) el avance de la tecnología aplicada a la seguridad haya convertido este sistema en un "*enemigo/enemigo*" a fin de prevalecer la presencia de un "Súper Estado".

Como vimos anteriormente, uno de los conceptos centrales del derecho penal del enemigo es disminuir garantías constitucionales a aquellos quienes el estado considera "enemigo". Así, en el caso puntual de las cámaras de reconocimiento facial podemos observar que el Estado escanea los rostros de un sinfín de individuos sin hacer diferenciación alguna. Es decir, que invade la privacidad de aquellos que serían "amigos" (aquellos que no trasgreden el orden jurídico vigente) y de aquellos que serían "enemigos" del Estado dado que cometieron infracciones, irrumpiendo el orden social.

En definitiva, este avasallamiento del Estado, para ambos grupos, se convierte en realidad en un sistema "enemigo/enemigo", dado que en definitiva todos los ciudadanos recibimos el trato de enemigos, disminuyendo así injustificadamente nuestras garantías constitucionales y principalmente nuestro derecho a la privacidad consagrado en el art. 18 de la CN.

Si bien es cierto que este avance del Estado sobre nuestras garantías constitucionales no parece tan relevante en comparación con otras acciones cometidas por Estados Totalitarios, en otros momentos de la historia, lo cierto es que es en estos pequeños avances el momento de ponernos en estado de alerta y defender nuestras garantías constitucionales.

En este sentido, y de igual modo que en criminología se utilizó la teoría de las *ventanas rotas*[38] para asegurar un menor índice de crimen y vandalismo podríamos sostener, utilizando esa misma teoría, que un freno a tiempo por parte de los

[37] Ese interrogante lo respondió la doctrina al sostener que "*la razón jurídica del estado de derecho, en efecto, no conoce enemigos y amigos, sino solo culpables e inocentes*". Ferrajoli, *Derecho y razón*, p. 830.

[38] James Q. Wilson and George L. Kelling. "*BROKEN WINDOWS: The police and neighborhood safety*". Este concepto fue introducido en dicho artículo como estrategia para eliminar o contener el crimen y se utilizó el siguiente ejemplo: "Consideren un edificio con una ventana rota. Si la ventana no se repara, los vándalos tenderán a romper unas cuantas más. Finalmente, quizás hasta irrumpan en el edificio; y, si está abandonado, es posible que lo ocupen ellos y que prendan fuego dentro."

ciudadanos sobre los avances del Estado hacia nuestra intimidad impide un avasallamiento absoluto por parte de éste sobre nuestros derechos esenciales; es decir no colocar ese freno a tiempo sería como dejarnos en un estado de abandono librados a merced del Súper Estado.

En definitiva, podríamos concluir en que existe una lucha entre la política criminal y la dogmática penal, de modo tal que la segunda de ellas debería funcionar como un freno a la primera y que el avance de ésta (política criminal) sea en el marco de un Estado de derecho. Sin embargo, como vimos a lo largo del trabajo no pareciera que esto funcionara de ese modo, sino más bien a la inversa.

Corresponde finalizar este capítulo con una cita de doctrina muy acertada que ilustra lo manifestado en el párrafo anterior y advierte sobre el cuidado que debemos tener a la hora de advertir avasallamientos por parte del Estado. En tal sentido, en un trabajo titulado "la herencia de Franz von Liszt" se sostuvo que "*…Pero si se reconoce y admite que también en las sociedades actuales, junto con un Derecho Penal que observe las garantías y límites del poder penal en el Estado de Derecho, debe existir todavía otro Derecho Penal, un "Derecho Penal del enemigo", mediante el cual el Estado debe reaccionar más combativamente respecto de determinados sujetos que atacan grave y reiteradamente normas sociales fundamentales, sin tener que respetar las garantía y principios del Estado de Derecho, entonces el regreso de aquello que antes hemos señalado como lado negativo de von Liszt no es para celebrar, sino más bien para llorar;* ***el Derecho Penal no es entonces ninguna "barrera insuperable" de una Política criminal que no respeta los límites y principios del Estado de Derecho, sino que se convierte en un instrumento para su realización***[39]."

VIII.- Conclusiones

De lo expuesto resulta necesario efectuar una serie de consideraciones finales respecto a los conceptos analizados a lo largo del trabajo.

- Es evidente que existe una la relación de tensión entre el derecho a la privacidad personal y el avance de la tecnología en materia de cibervigilancia en la vía pública, posibilidad técnica que permite el almacenamiento, registro y tratamiento de datos, en especial de la imagen

[39] Titulo original: "*Das Erbe Franz von Liszt*", publicado en alemán en *Festschrift für Winfried Hassemer zum 70. Geburtstag am 17.vFebruar 2010*, editado por Felix Herzog y Ulfrid Neumann, pg. 70, en colaboración con Jong-Dae Bae, Andreas von Hirsch, Shozo Horiouchi,*v*Francisco Muñoz Conde y Juárez Tavares, Heidelberg (u.a.), Múnich, 2010, pp. 535-558. Traducción al español de Alberto Nanzer (UBA) revisada por el autor.

de los individuos y el seguimiento de sus movimientos de modo sistemático y sin posibilidad de control sobre los datos almacenados. Dicha circunstancia es un fenómeno mundial como consecuencia del avance del crimen organizado, y en donde los Estados en su misión de mantener la Seguridad Interior han avanzado paulatinamente e imperceptiblemente sobre libertades individuales.

- Nuestros constituyentes plasmaron su intención de que las decisiones relacionadas a las invasiones a la intimidad queden en la órbita de los jueces. La función de control a cargo de los jueces es un resguardo contra la arbitrariedad estatal y ellos son los que se encuentran en una situación de mayor serenidad y objetividad para resolver sobre cuestiones atinentes a la limitación de derechos individuales.
- El inconmensurable avance tecnológico aplicado a la Seguridad de la Nación obliga a efectuar una interpretación dinámica de nuestro art. 18 y 19 de la CN a fin de que dicho articulado se adapte rápidamente a los cambios tecnológicos y de este modo resguardar adecuadamente el derecho a la privacidad de los individuos.
- La doctrina y la jurisprudencia acudió al criterio de *expectativa razonable de privacidad* para zanjar la cuestión de la relación de tensión entre la injerencia razonable y el derecho a la privacidad. Para ello fueron elaborados dos criterios para definir el concepto de "expectativa razonable de privacidad": 1) que el individuo haya actuado de manera tal de exhibir un interés de mantenerlo, y 2) dicha expectativa de privacidad deberá ser soportada por el Estado como razonable. En el antecedente "Katz v. United States" fue receptado este concepto para remarcar la inviolabilidad de las comunicaciones telefónicas.
- El carácter Republicano de nuestro país, con una división de poderes a tal efecto, toma un papel preponderante en la relación de tensión entre la injerencia estatal y el derecho a la privacidad, dado que el Poder Ejecutivo como cabeza de las fuerzas de seguridad vela por cumplir con la ley de Seguridad Interior a fin de garantizar el bienestar general pero cuando alguna medida implique la disminución de garantías constitucionales deberá ser el Poder Judicial (interpretador nato de nuestra Carta Magna), quien así lo disponga mediante una ORDEN JUDICIAL que analizará la proporcionalidad de la misma.
- Es necesario contar con una orden judicial para acceder a cualquier tipo de información personal que esté vinculada con sistemas tecnológicos destinados a la seguridad, como lo son los seguimientos por cámaras a

individuos, la fijación de las mismas a domicilios determinados, la solicitud de información a los "anillos digitales" y las comparaciones de rostro mediante un sistema de reconocimiento facial. Todas esas acciones del Estado son invasivas de la intimidad de los individuos afectando los arts. 18 y 19 de la CN por lo que es un Juez quien debe autorizarlo mediante la orden correspondiente.

- Las bases de datos que recopilen información personal de modo sistemático por medio de cualquier tecnología o mediante el uso de datos biométricos, deben encontrarse a resguardo de entes independientes de las fuerzas de seguridad para garantizar y fomentar la solicitud de una orden judicial para acceder a las mismas como así también para garantizar el respeto a la ley de Datos Personales.
- El sistema de video vigilancia de reconocimiento facial constituye, en algún punto, un derecho penal del enemigo convirtiendo el clásico sistema de "amigo/enemigo" en "enemigo/enemigo" dado que se disminuyen las garantías constitucionales de la totalidad de individuos, que participan de la sociedad, sin efectuar distinción alguna entre ellos.
- El Derecho Penal debe ser la barrera insuperable de la Política Criminal y no una herramienta de ésta última para lograr sus fines.

Sentadas esas consideraciones, podríamos decir que una de las mayores preocupaciones relacionadas a la tensión que existe entre el avance de la tecnología y el derecho a la privacidad no es la recopilación de datos personales en pos de la existencia de un bien superior (Seguridad Nacional) sino más bien el posterior tratamiento de los mismos, pues es necesario que los ciudadanos tengamos plena confianza de que esos datos son resguardados de modo seguro e inquebrantable y que solo un Juez (encargado de velar por las garantías constitucionales) será quien quiebre ese pacto.

No nos oponemos a la recopilación de datos porque ello significaría ir a contramarcha del avance de la tecnología y el progreso de la propia humanidad. Como se sostuvo, en el caso "Carpenter vs. United States", un teléfono celular inteligente es hoy en día casi un requisito obligatorio para participar de la sociedad moderna y a su vez ello conlleva la recopilación de un montón de datos personales por parte de las empresas proveedoras del servicio telefónico. En tan sentido, el ciudadano se encontraría en la encrucijada de utilizar un teléfono inteligente para participar de la sociedad moderna o marginarse de la misma, sin utilizar un

teléfono de esas características, para preservar el derecho a la privacidad[40]. Ello, no es viable por lo que el único mecanismo que se presenta es aceptar, al menos de modo implícito, que esa recopilación de datos existe pero que será guardada en un cofre bajo llave que solo un Juez competente podrá abrir.

En definitiva, y como observamos a lo largo del trabajo, debemos ser muy cautelosos a la hora de aplicar avances tecnológicos a fin de garantizar el derecho a la privacidad y en ese sentido debemos entender que el derecho penal debe ser la barrera insuperable de la política criminal y no la herramienta para lograr sus fines. Incluso muestra de esa relación de tensión entre el derecho penal y la política criminal, lo es la ley 27.319, que incluye novedosos métodos de investigación en delitos complejos y que han sido materia de numerosas críticas respecto a su falta de armonía con la Constitución Nacional. Así, la utilización del agente encubierto que introduce esta ley ha sido tachada de inconstitucional en la creencia de que el Estado no puede valerse de un método engañoso para la obtención de prueba, pues no resulta ético, y además puede repercutir en una violación al principio de autoincriminación establecido en el art. 18 de la CN. Así, el ámbito de privacidad comienza a ser cada vez más difuso en atención a la injerencia estatal constante.

En ese contexto la doctrina sostuvo de modo muy acertado que *"A su vez, el rampante proceso de inclusión de esos medios de investigación encubiertos para delitos complejos provoca de manera directa una restricción a la garantía de defensa en juicio, ya que en la práctica ello conduce a exacerbar las funciones preventivas del Estado en la lucha contra la criminalidad organizada, aceptándose como necesario para satisfacer esos fines político criminales subordinar la vigencia plena de los derechos humanos. De forma paulatina se empieza a aceptar una intervención temprana o meramente preventiva de las autoridades públicas encargadas en la represión de esos delitos organizados, en cuyo caso las posibilidades de reacción por parte del acusado se estrechan de manera gradual en relación con el ámbito de privacidad. Ese ámbito de privacidad y su correlativa expectativa de confidencialidad de las formas de comunicación, en especial mediante el ingreso de los medios tecnológicos aplicados a las comunicaciones intersubjetivas y la información, son erosionados de manera constante a través de las modernas formas de injerencia en el domicilio y de interceptación de las comunicaciones. La renuncia por parte de la sociedad a una expectativa amplia de confidencialidad es aceptada como un mal necesario atado al carruaje de los sucesivos requerimientos formulados por una política criminal*

[40] En el artículo "*En búsqueda de la privacidad perdida*", Juan Antonio Traverso, La Ley, Ar/DOC/403/2019, el autor sostuvo que "Lo cierto es que el teléfono celular sigue con precisión al dueño. Se trata de una vigilancia perfecta; tal como si se hubiera conectado una tobillera electrónica al usuario del teléfono; verdaderamente un localizador personal preciso".

que propone un Derecho penal expansivo que se traduce en los hechos en una mayor presencia del Estado en el control de la criminalidad ordinaria y la organizada"[41]

Finalmente, habré de concluir que de no poner un freno a tiempo, pareciera ser que cada vez nos encontramos más cerca del Superestado que menciona George Orwell en la novela "1984" y donde su protagonista Winston Smith se ve acosado por el "Gran Hermano" que todo lo vigila. No creo que George Orwell haya siquiera imaginado que su novela de ficción, escrita en 1949, podría parecerse mucho a la realidad del siglo XXI.

IX.- Referencias bibliográficas

- ABOSO Eduardo Gustavo, *Técnicas de Investigación y Vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información*, Publicado el 30/05/2017, elDial.com – DC2325.
- ABOSO Gustavo Eduardo, *La regulación de medios de investigación encubierta en la lucha contra la criminalidad organizada: Agente encubierto, agente revelador, informante y entrega vigilada*, Publicado el 19-6-2018, elDial.com - DC255D.-
- AGAMBEN Giorgio, Homo sacer, *El poder soberano y la nuda vida*, Valencia, 2003, 217.
- CARRIO Alejandro D., *Garantías Constitucionales en el Proceso Penal*, 5.a. ed., Editorial Hammurabi, Buenos Aires, Argentina, Año 2012.
- CHAIA Rubén A., *Litigación penal II. Tecnología v. Garantías. Evidencia digital. Intimidad, privacidad y comunicaciones. Regulación procesal en la provincia de Entre Ríos y evolución de la Jurisprudencia del Tribunal Europeo de Derechos Humanos y la Corte Suprema de Estados Unidos***,** Publicado el 5/6/2019**,** elDial.com- DC275B.
- FERRAJOLI Luigi, *Derecho y razón, Teoría del Garantismo Penal*, editorial Trotta.
- JAKOBS Gunter, "*La ciencia penal ante los retos del futuro*", trad. De Teresa Manso en Eser/Hassemer/Burkhardt, *La ciencia del derecho penal*

[41] *La regulación de medios de investigación encubierta en la lucha contra la criminalidad organizada: Agente encubierto, agente revelador, informante y entrega vigilada*, Gustavo Eduardo Aboso, 19-6-2018, elDial.com - DC255D.-

ante el cambio de milenio", Francisco Muñoz Conde (coord.), Valencia 2004.

- MARTINEZ MARTINEZ, R, *Los ficheros de datos y archivo de imágenes policiales en la legislación italiana*. Análisis de resoluciones dictadas por el garante italiano para la protección de datos personales. Revista Española de derecho Constitucional, Año 20, Núm. 60, sept.-dic de 2000.
- MUÑOZ CONDE Francisco, *La herencia de Franz von Liszt*, Universidad Pablo de Olavide, Sevilla, España, Revista Penal Mexico, núm. 2, Julio-diciembre de 2011.
- MUÑOZ CONDE, *Edmund Mezger y el derecho penal de su tiempo, Estudios del Derecho Penal en el Nacional Socialismo*, cuarta edición, Editorial Tirant lo Blanch, año 2003.-
- TRAVERSO Juan Antonio, "*En búsqueda de la privacidad perdida*", La Ley, Ar/DOC/403/2019.
- VELEZ MARICONDE Alfredo, *Derecho Procesal Penal*, 3 ed., vol. II. Año 1986, Editora Córdoba.
- VON LISZT, "*Kriminalpolitische Aufgabe", en Strafrechtliche Vorträge*, Traducción al español de Enrique Aimone Gibson, con prólogo de Manuel de Rivacoba, Valparaíso, Chile, 1984, bajo el título *La idea de fin en el Derecho Penal.*
- WILSON James Q., "*BROKEN WINDOWS: The police and neighborhood safety*", artículo publicado en la revista The Atlantic Monthly en marzo de 1982.