"VIDEOVIGILANCIA"

PUNTO DE COLISIÓN ENTRE DERECHOS FUNDAMENTALES, SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

Ernesto IBARRA SÁNCHEZ[1]

Al "maestro y amigo", doctor Julio Téllez Valdes y su familia, con admiración, aprecio y profundo agradecimiento.

SUMARIO: I. *Nota introductoria.* II. *El Estado, derechos fundamentales y seguridad.* III. *El derecho a la protección de datos personales.* IV. *La vigilancia por medios tecnológicos "videovigilancia".* V. Regulación jurídica de la videovigilancia en México. VI. *Consideciones finales.* VII. *Fuentes de consulta.*

I. NOTA INTRODUCTORIA

Mucho se ha hablado sobre lo que es la "sociedad de la información y/o del conocimiento", del impacto de las tecnologías desde el un punto de vista de las transformaciones que se han provocado dentro del ámbito de la vida diaria de las personas y de la sociedad en su conjunto.

En esta oportunidad se pretende realizar un breve señalamiento sobre una fenomenología social que con el uso de tecnologías de la información, la vigilancia con empleo de videocámaras de distintas características, la llamada "videovigilanica" cuyo objetivo principal es el obtener cierto control sobre la integridad y el patrimonio, ya sea del Estado en la búsqueda de la seguridad pública y el orden, o de los particulares respecto de su integridad física, su patrimonio. Sin embargo, ante el control y la búsqueda de esa seguridad por parte del Estado mexicano y de los particulares se pueden ver conculcados derechos fundamentales, como la intimidad, la privacidad, la libertad y el ahora independiente derecho de protección de datos personales; por ello resulta importante establecer los procedimientos específicos para la

[1]Estudiante del Posgrado en Derecho en la UNAM, becario en el Instituto de Investigaciones Jurídicas de la UNAM y asociado investigador en el Instituto Jurídico Mexicano de Tecnologías de la Información A.C. *ibarra_e8@hotmail.com.*

instalación, pero, sobretodo, para el tratamiento de las imágenes de las personas, de tal modo que garanticen el mejor equilibrio entre dos derechos de suma importancia: el de la seguridad y el de los datos personales.

Es cada vez más notorio el incremento de la videovigilancia como fenómeno de reacción ante la creciente ola de inseguridad; esto ha desencadenado que cada día más localidades, ciudades, establecimientos públicos y privados, hogares e incluso trasportes públicos cuenten con sistemas de vigilancia que utilicen herramientas tecnológicas.

La seguridad pública es y ha sido un tema por demás relevante y delicado tanto en nuestro país como en el resto del mundo. La situación de inseguridad que impera en la sociedad mexicana es crítica y alarmante, muy a pesar de las notas periodísticas que los gobernantes hacen llegar a la sociedad. La delincuencia organizada ha sido, principalmente, el agente detentador del poder que pone a prueba y en predicamentos al sistema de gobierno del Estado mexicano.

Parece más fácil generar un esquema de terror y miedo, respecto de la difícil tarea de construir mediante la creatividad y el ingenio, aunado a las dificultades o resistencias que provoca la situación económica y otros factores como la corrupción. Ante el miedo generado y la constante búsqueda y necesidad del hombre por la certeza de sus actos y/o consecuencias, se ha buscado un mínimo de reglas de todo tipo para garantizar la tranquilidad, el orden y hacer posible con ello el ideal de la vida armónica de la sociedad misma. A esa búsqueda por parte del Estado y de los particulares, resulta valioso el echar mano de las distintas herramientas tecnológicas que están a disposición de la función de policía que realizan las autoridades o la simple vigilancia que ejercen los particulares para salvaguardar su integridad, su patrimonio y garantizar que se cumplen las funciones encomendadas a otra persona.

Pero ¿en qué momento surge una necesidad de implementar a gran escala y de manera consistente, los sistemas de videovigilancia?, ¿qué provocó que la industria de la videovigilancia se disparara?, ¿cuál ha sido la contracara de la instalación de tantas cámaras que vigilan los espacios donde las personas creen vivir libres?, ¿en realidad se vive libre y con privacidad en la era globalizada, donde cada persona es un conjunto de datos y esos datos un grupo de información de distinto valor económico? A todas las interrogantes anteriores sirve de base el desafortunado suceso del 11 de septiembre de 2001, donde el estado más poderoso del mundo, aquel que presume de mayor sistema de inteligencia y control en distintos aspectos, el estado que implementa la tecnología más sofisticada del orbe, fue atacado y recibió un golpe doloroso que dejó de manifiesto que el tema de la seguridad alcanzaba mayor trascendencia, se llevaba a niveles de terrorismo y se infundía el miedo hacia la sociedad y con ello la pérdida de

la vida libre, la tranquilidad y la paz interna, necesarias todas para una paz social como fin de los Estados democráticos.

> A partir de entonces, las mismas tecnologías serían utilizadas para un mayor nivel de control, aumentando los ojos vigilantes, la capacidad, potencia de visión, sumando desarrollo tecnológico para aplicarlo a medidas de seguridad, como detectores de metales, gases, sustancias peligrosas, enfermedades y conductas sospechosas, sistemas de medición y registro de morfología, lectura de iris, escaneo del rostro, de huellas digitales, de temperatura, de radiofrecuencias y todo tipo de mecanismo que ofrezca mayor control y seguimiento de cualquier persona, además de otros datos personales sean estos íntimos o no.

Aquel atentado dejó un impacto no sólo a los Estados Unidos de América, la preocupación de muchos otros gobiernos fue inmediata, buscaron mayores y más eficaces medios de control para prevenir algún acontecimiento parecido. La desconfianza y el temor se generalizaron, esto aunado a la crisis económica, la delincuencia organizada y la corrupción, entre los principales factores que propiciaron el acelerado desarrollo de sistemas de vigilancia por medios electrónicos. Ante dicho temor, Estados y particulares sintieron la necesidad de establecer sus propios mecanismos de protección de la integridad y el patrimonio.

El tema de la videovigilancia, como muchos otros, tiene en su expresión diversas aristas, caras encontradas que permiten el espacio para la reflexión, y en este caso, el detenernos a su estudio desde un punto de vista jurídico, por lo que analizando su regulación jurídica en nuestro país partiendo de lo delicado que es la situación respecto de su tratamiento, su manejo adecuado y las correspondientes sanciones ante su uso incorrecto que hagan de ellos las autoridades y los particulares mismos ante un mundo interconectado por la red de redes donde cualquier dato o información pierde absoluto control y puede causar algún perjuicio a su titular.

Para lo anterior realizaremos un breve señalamiento de los antecedentes de la seguridad pública, la evolución de la función de vigilancia, el surgimiento como derecho fundamental de la protección de datos personales, para revisar el marco normativo que rige en nuestro país.

Se pretende un acercamiento a algunas cuestiones que se encuentran involucradas a la situación del tema de la libertad, identidad, intimidad y privacidad ante el uso de tecnologías que procura una mayor seguridad pública y privada. Y un elemento de reflexión sobre si esta implementación de sistemas tecnológicos, como los documentos de identidad, el uso de los dispositivos de geolocalización, de radiofrecuencia, de dispositivos móviles y la cada vez mayor videovigilancia constituyen o no un atentado ante la esencia del ser humano.

Respecto de la videovigilancia, se pueden identificar un sinnúmero de campos de aplicación, aunque se pueden reducir a dos grandes grupos: el público y el privado, los cuales trataremos más adelante.

II. El Estado, derechos fundamentales y seguridad

1. *Visión general sobre los derechos fundamentales y el Estado*

En la actualidad, con la denominada "sociedad de la información" y/o del "conocimiento"[2] se presenta una generalizada transformación del modo de realizar un sinnúmero de actividades humanas, ya sea en forma individual, en grupo o en toda una sociedad o sociedades, que impliquen cosas banales, creativas, productivas, de ocio, de cualquier cosa, sea lo que sea, las actividades del ser humano, incluso las intangibles, como el pensamiento, se ven alcanzadas por el impacto de la tecnología en los distintos ámbitos. Ante esta situación y el constante desarrollo científico tecnológico, no todo resulta del lado claro de la luna, es decir, que aunado al gran avance para la humanidad y los incontables procesos a los que se ha favorecido con la tecnología, esta última ha servido para satisfacer los deseos de destrucción, daño o perjuicio de algunas personas hacia otras. La utilización negativa o perversa de las tecnologías de la información puede ocasionar un ataque en la integridad física o emocional de una persona y en su patrimonio.

Ante la situación ambivalente del impacto de las tecnologías de la información y comunicación, donde existe mucho riesgo de sufrir un menoscabo a nuestros derechos fundamentales.[3] Por lo que señalaremos groso modo algunos de los derechos que están en juego, como el de la seguridad pública y el derecho de protección de datos personales como un derecho fundamental.

Para hablar sobre el derecho de protección de datos común derecho fundamental, es importante hacer un señalamiento sobre la concepción de derecho fundamental, retomar cuáles han sido los documentos más importantes a nivel internacional de los que se construye la plataforma para los derechos del individuo y su carácter de fundamental, sin olvidar la importancia del derecho a la intimidad y a la vida privada.

---

[2] Véase, Rodolfo Suárez, *Sociedad del conocimiento, propuesta para una agenda conceptual,* UNAM, México, 2009.

[3] Se sugiere revisar las ponencias que conformarán la mesa 10. "La indivisibilidad de los derechos humanos", que se presentarán el miércoles 8 de diciembre de 2010, dentro del marco del VIII Congreso Mundial de la Asociación Internacional de Derecho Constitucional, mismas que estarán disponibles en la página del congreso en: *https://www.juridicas.unam.mx/wccl/* a partir de noviembre de 2010.

De manera indistinta se suelen utilizar las expresiones “derechos humanos” o “derechos fundamentales” para significar una misma realidad, los cuales se pueden resumir como los derechos que tiene atribuida la persona *per se*.[4]

En tal sentido, se puede utilizar la expresión “derechos humanos” a la argumentación filosófica de un derecho de personas, y emplear la expresión “derechos fundamentales” cuando se argumente desde un plano del derecho vigente del Estado mexicano en el caso particular.

Haremos un señalamiento del derecho de protección de datos personales como un derecho fundamental, a partir del marco teórico proporcionado por Robert Alexy,[5] en su teoría de los derechos fundamentales.

Al respecto, el propio Alexy establece que las “las normas de derecho fundamental son aquellas expresadas a través de normas iusfundamentales entendiéndose por estas exclusivamente enunciados contenidos en la ley fundamental.” Pero no todas las normas fundamentales se adscriben directamente en la constitución, por lo que las normas fundamentales pueden separarse en dos clases: las normas de derecho fundamental estatuida directamente por la constitución y las normas de derecho fundamental a ellas adscritas.

A nivel de documento histórico, como documento base para los sistemas políticos contemporáneos occidentales o Estados modernos, se puede señalar la Carta Libertatum de 1215, también conocida como *Carta de Juan sin tierra*, primer antecedente de lo que hoy en día es la Constitución de un Estado, garante de derechos y libertades de los habitantes del mismo, pues se establece una reducción de potestades del rey y creación de cuerpos civiles de control o contrapeso a las decisiones arbitrarias del soberano, además del comienzo de la separación entre el Estado y la Iglesia.

Los derechos fundamentales que se van adquiriendo con el devenir histórico, como el derecho a la intimidad o a la vida privada, con los cuales mantiene vinculación directa el de la protección de datos personales, han sido reconocidos por diferentes instrumentos y actos internacionales, como:

---

[4] En este sentido se ha manifestado García Belaunde, quien ha escrito que "los derechos fundamentales o derechos de la persona (llamados *libertades públicas* en la tradición jurídica sajona), son considerados como derechos fundamentales básicos, constitucionales o simplemente derechos humanos". García Belaunde, Domingo, *Derecho procesal constitucional*, Bogotá, Temis, 2001, p. 118.

[5] Alexy, Robert, *Teoría de los derecho fundamentales*, trad. de Ernesto Garzón Valdés, Madrid, Centro de Estudios Constitucionales, 1997.

- La Declaración de los Derechos del Hombre y del Ciudadano de 1789, en la que se establecían los derechos mínimos naturales e imprescriptibles del hombre, y en el artículo 12, los principales derechos, como son libertad, propiedad, resistencia a la opresión, igualdad y seguridad.
- La Declaración Universal de los Derechos Humanos, de 1948. En esta Declaración se consagra el derecho a la intimidad y merece por primera vez un reconocimiento internacional. El artículo 12 de esta Declaración dice que nadie podrá ser objeto de injerencias arbitrarias en su *vida privada*, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación.
- El Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950,[6] cuyo artículo 8° hace referencia al derecho a la vida privada y familiar, declarando que: "Toda persona tiene derecho a al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". Y que:

> No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté *prevista por la ley* y constituya una medida que, en una sociedad democrática, sea necesaria para la *seguridad* nacional, la *seguridad* pública, el *bienestar económico* del país, la *defensa del orden* y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás." (*las cursivas son nuestras)*.

- En el Consejo de Europa, en 1967, se crea la Comisión Consultiva para estudiar las tecnologías de la información y su potencial agresividad hacia los derechos de las personas, especialmente a la *vida privada*, derecho que se había ya recogido en la Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos de 1966.
- El Convenio 108/1981 del Consejo de Europa, relativo a la protección de las personas físicas en lo que respecta al tratamiento automático de datos personales.
- Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, "directrices de privacidad", fueron adoptadas como una recomendación del Consejo de la OCDE, apoyando los tres principios: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Se hicieron efectivas el 23 de septiembre de 1980. La recomendación sobre circulación internacional de datos

---

[6]El Convenio Europeo de los Derechos Humanos, Convenio de Roma 1950.

Véase en *http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf, consultado en agosto 2010.*

personales para la protección de la intimidad y la relativa a la seguridad de los sistemas de información.

- La Carta de Derechos Fundamentales de la Unión Europea, proclamada en Niza el 7 de diciembre de 2000, establece en su artículo 8°, dentro del capítulo relativo a las libertades, que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen".
- Los Estados, economías que forman parte de APEC, aprobaron en 2004, el marco de privacidad basado en principios APEC, como una herramienta importante para alentar el desarrollo de protecciones apropiadas a la privacidad de la información y para asegurar el libre flujo de información en la región Asia Pacífico, atendiendo los lineamientos de la OCDE.
- En la Conferencia Internacional de Autoridades de Protección de Datos, a la que me refería antes, desde la mesa del *presidium*, celebrada en Montreux, Suiza, del 13 al 15 de septiembre de 2005, se aprobó una declaración final sobre la protección de datos personales y la privacidad en un mundo globalizado.

Aunado al interés por la protección de este derecho, las autoridades garantes del mismo, distintos países se reúnen para discutir y proponer avances en su función protectora del derecho fundamental. El 6 de noviembre de 2009, más de 50 autoridades adoptaron la "Resolución de Madrid", de estándares internacionales de privacidad, la cual recoge experiencias y diversos enfoques para garantizar la protección de este derecho, integrando legislaciones de los cinco continentes. Esta resolución constituye la base para el desarrollo de un instrumento vinculante a escala internacional, que contribuya a una mayor protección de los derechos y libertades individuales.

Existen documentos de la sociedad civil que sirven de apoyo a estos documentos internacionales, como es el caso de la Declaración de México 2010, sobre la protección de datos personales, en la que se comprometen las autoridades y sus funcionarios a llevar la protección de ese derecho de manera responsable y bajo los principios adoptados a nivel internacional.[7]

En la fenomenología de la videovigilancia se pueden encontrar derechos fundamentales que sólo encuentren salida entre ellos por alguna causa justificada en el propio ordenamiento, como la colisión de derechos a la seguridad y el de la intimidad o la libertad, que, a su vez,

[7] Dicha Declaración, se llevó a cabo en el marco del VIIl Encuentro Iberoamericano de Protección de Datos Personales, en la ciudad de México, realizada por la Red Iberoamericana de Protección de Datos Personales. Las memorias y la propia declaración podrán ser consultadas en la página del Instituto Federal de Acceso a la Información y Protección de Datos, IFAI, en: *http://www.ifai.org.mx/* o en el sitio de la propia Ded en: *http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material.*

parece tener justificado deslinde cuando se trate del establecimiento del orden o la seguridad nacional, o cualquier riesgo sanitario, o ante el combate a la delincuencia organizada.

Respecto del impacto entre dos o más derechos fundamentales, se ha dicho en la doctrina[8], que la expresión de "punto de conflicto" de derechos fundamentales es donde surgen delicadas discusiones y la ponderación resulta por demás compleja, según una visión conflictivista, éstos "son realidades que eventualmente pueden entrar conflicto".[9] En el terreno de la vigilancia, esto es así en el caso del derecho a la seguridad y protección de nuestra integridad y patrimonio, puede colisionar con el derecho a la intimidad, la libertad de expresión, libre tránsito, manifestación y asociación de cualquier tipo, de la propia imagen, al honor y ahora al de la protección de nuestros datos personales.

Al existir un derecho fundamental, en su ejercicio puede coincidir en conflicto con otro derecho fundamental que esté siendo ejercido por otra persona. En caso de conflicto o de concurrencia de valores normativos, la ponderación ayuda a resolver en buna medida la colisión, sin que esto sea caso fácil, y por ello la propia Constitución debe establecer casos de excepción o facultar el procedimiento para crear las causas justas en que pueda uno prevalecer sobre otro.

Por tanto, se establecen "como las fronteras que definen los derechos son imprecisas, los conflictos devienen inevitables y problemáticos".[10]Y en el caso de la aplicación de las tecnologías de la información y específicamente sobre muchas de las conductas que se llevan a cabo por Internet surge puntos de colisión entre derechos fundamentales.

En México contamos con un derecho fundamental a la privacidad, que para que sea plenamente ejercido y garantizado debe ser reconocido por el Estado. En la Constitución Política de los Estados Unidos Mexicanos se establece el derecho a la vida privada, como límite a la intromisión del Estado en el ámbito de la persona.

---

[8]Véase Rodríguez Molinero, Marcelino, "Colisión de derechos fundamentales y garantías jurisdiccionales", Prieto Sanchís, Luis, *Estudios sobre derechos fundamentales*, Madrid, Debate, 1992.

[9] Bleckmann agrupa bajo el concepto genérico "conflicto de derechos fundamentales" o "tensión de derechos fundamentales". Bleckmann, Albert, *Staatsrecht IIDie Grundrechte*, 4a. ed., Berlín, Karl Heymanns, 1997, p. 473. El mismo autor continúa diciendo... "el concepto de colisión de derechos fundamentales no abarca el caso de la colisión de derechos fundamentales con otros bienes constitucionales. Existe colisión de derechos fundamentales cuando el titular de un derecho fundamental a causa de una actividad estatal obtiene una ventaja pero afectando al mismo tiempo el derecho fundamental de otro titular. Se da por otra parte cuando se está frente a la mediata o inmediata *producción de efectos colaterales* de los derechos privados, sin que el Estado participe directamente. Y finalmente se da cuando es tenido en cuenta un mismo derecho fundamental de diferentes titulares". *Ibidem*, pp. 473 y 474.

[10] García-Pablos, Antonio, "La protección penal del honor y la intimidad como límite al ejercicio del derecho a la libre expresión", en varios autores, *Libertad de expresión y derecho penal*, Madrid, Edersa, 1985, p. 205.

El artículo 16 de nuestra carta magna señala que: "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".

Dentro de los derechos fundamentales que están involucrados con el de la protección de los datos personales, podemos decir que el de la seguridad es uno de los más importantes para el tema de la videovigilancia en razón de parecer la contracara primordial y principal fin del uso de tecnologías para auxiliar la protección del patrimonio y la integridad; por ello dedicaremos un par de cuartillas a desarrollar algunas ideas sobre la seguridad pública y privada.

2. Estado y seguridad

Uno de los fines primordiales del Estado es el orden y la paz social para alcanzar la convivencia armónica de sus habitantes. Pero no siempre el Estado ha sido el mismo, y corresponden diferentes concepciones de ejercicio de poder y con ello de protección o seguridad hacia sus habitantes. Así, el pensamiento político moderno, desde Maquiavelo, Hoobes, Bodin, Hegel, Weber, Kelsen y Bobbio, ha establecido la primacía del poder político por sobre otros poderes como fundamento del Estado moderno.[11]

El fundamento del poder político se puede entender como el uso de la fuerza o coacción física, ya sea mediante la violencia física o moral ejercida por el gobernante de un Estado. A lo anterior tenemos algunas expresiones, como la de Max Weber, quien refiere: "…el Estado como detentador del monopolio de la coacción física legítima". Esto parece el fundamento de las medidas de control y vigilancia establecida por el Estado de manera legítima sobre la base de la importancia de la seguridad pública de la sociedad.

Con la propia evolución de la configuración del Estado, desde el Estado preabsolutista, el absolutista, el Estado moderno o democrático, en fin cualquiera que sea la concepción de *Estado,* a través del desarrollo de la sociedad organizada bajo una autoridad y un conjunto de religaciones particulares de carácter normativo o de costumbre, el término "seguridad" implica, por lo tanto, diferentes percepciones; con ello, la percepción de seguridad pública como derecho ha sido consecuencia de la evolución particular de cada Estado y sistema de gobierno.

Para referirnos a la "seguridad pública", sigo la división del Estado, en preabsolutista, absolutista y moderno (aunque el término "moderno", hace referencia a "modernidad" y

---

[11] Samuel González Ruiz *et al,* Seguridad pública en México, problemas, perspectivas y propuestas, México, UNAM.

respecto de ello no es fácil determinar una fecha exacta, ni siquiera una etapa determinada). Estas son algunas de las características de la configuración de Estado con relación a la seguridad y otros derechos:

- En los siglos XI-XV, la acumulación de poder en monopolio,
- En los siglos XV y XVI, incipiente protección que los príncipes debían dar a sus súbditos. A cambio de no portar armas, de aportar a la defensa del reino, dar alimentos y entretenimiento, el rey les daba protección y cierta seguridad, aunque a manera totalmente discrecional,
- Estado medieval: se regía por *pactos o cartas reales* que podía desconocer el rey. Había cierta limitación al poder del soberano y obediencias condicionadas (negociación entre el príncipe y el pueblo "comunas, aldeas o ciudades").
- Monarcas europeos (siglos XVI y XVIII). Monopolios de violencia física. Necesarios para entender la conformación de la sociedad actual,
- Fue hasta 1829, cuando algunos gobiernos medievales desarrollan la función de "policía" a través de un aparato o cuerpo policiaco.
- El Estado absolutista acabó con el orden político medieval y con ello descuidó la seguridad pública al asumir el monopolio total del gobierno,
- El pilar del Estado absolutista y del dominio del poder estuvo basado en el control de la seguridad y las mercancías desde el siglo XV hasta la conformación del Estado moderno.
- Estado absolutista, su fin principal era garantizar a su pueblo el mayor bienestar y seguridad. Pero el gobernante decidía discrecionalmente la forma de proveer todo ello. Surge el aparato burocrático. La administración pública y con ello los cuerpos de policía, casi como hoy los conocemos,
- En el siglo XVII surge por primera vez la idea de un Estado con "policía".
- Luis XV, crea la institución de policía, con el fin de vigilar un sinnúmero de asuntos.
- La Ilustración, como fundamento ideológico de la modernidad, misma que está ligada a la concepción idealizada de un Estado liberal, donde priven las leyes que garantizan la seguridad, y brinde con ello la libertad y tranquilidad así, la seguridad nacional.
- El marqués de Beccaria habla sobre distintos mecanismos para obtener la tranquilidad pública, mediante iluminación de callejones, guardias y autoridades públicas y protegiendo templos importantes. Referencia directa de la política de prevención y la figura del policía.
- Joseph von Sonnenfels definió la ciencia de la policía como: aquella destinada a instituir y mantener la seguridad interna del Estado,

- Policía, del griego *politeia,* gobierno de la ciudad. Incluyó la protección de los bienes y las personas.
- Policía: mantener el orden y vigilar sobre las necesidades comunes de los ciudadanos.
- Siglo XVIII, surge la acepción restringida de policía. Encargada de la "seguridad pública".

Así, tras el paso del tiempo, largos esfuerzos y constantes luchas, aparece en el orbe la idea de la seguridad y la paz social en estrecha vinculación con el orden y la seguridad. Dejando la etapa de acudir al rey para solicitar intervención y establecimiento de la paz y el orden público, entendiendo así el surgimiento del Estado moderno, en cuanto organización garantizadora de seguridad, de orden y de tranquilidad.

La "seguridad", junto con la propiedad pública y privada, se convierte en el bien primario y vinculado fuertemente con las principales tareas del gobierno.

Para el análisis del tema de la seguridad pública, dentro de la concepción del Estado moderno, cuyos pensamientos filosófico-políticos liberal, se encuentra la idea de la soberanía y legitimidad del poder público, pero sobre todo el de la división de funciones, la libertad, igualdad y, en general, los derechos del hombre. Por ejemplo, la Declaración de los Derechos del Hombre y del Ciudadano de 1789, en la que se establecían los derechos mínimos naturales e imprescriptibles del hombre, y en el artículo 12, en donde se mencionan los principales derechos, como son: libertad, propiedad, resistencia a la opresión, igualdad y "seguridad".

Antes del Estado moderno al que se hace referencia, encontramos un esquema de Estado en el que la seguridad pública existía exclusivamente del lado del soberano, para que éste pudiese establecer su dominio y hegemonía en su territorio, donde los súbditos recibían protección a cambio de dejarlos permanecer en el territorio; era un medio de ejercer el poder mediante la fuerza del cuerpo que protegía al soberano y a su vez intimidar al pueblo.

Ya en la Declaración de los Derechos de los Norteamericanos de Virginia, en 1776, se señalaba que el gobierno debía ser instituido para la utilidad pública, la protección y la "seguridad" del pueblo.

En la Declaración francesa de 1793, en el artículo 8 se señala que la "seguridad" *consiste en "la protección otorgada por la sociedad por la sociedad a cada uno de sus miembros para la conservación de su persona, de sus derechos y de sus propiedades".*

Con lo anterior, el concepto de "seguridad" es trasladado en la actualidad como un "derecho", pero también como una obligación para el Estado.

Para el siglo XVIII, Montesquieu declara: "la libertad política está garantizada por la libertad de hacer lo que las leyes permiten y por la limitación y división del poder del Estado". Pero también señala que "La libertad política del ciudadano depende de la libertad de espíritu que nace de la opinión que cada uno tiene de su seguridad y para que exista la libertad es necesario que el gobierno sea tal que ningún ciudadano pueda temer nada de otro".[12]

El Estado moderno quiso entregar la fuerza pública a los ciudadanos garantizando el respeto y cumplimiento de las libertades y derechos ante los órganos de gobierno. Así pues, la vigencia del Estado de derecho implica la garantía de la seguridad pública, es decir, la defensa de las libertades y derechos del ciudadano; esto significa que el ciudadano sea copartícipe en los fines de la política de un Estado democrático.

3. Concepto de "seguridad pública"

El *Diccionario de la Real Academia*[13], define "seguridad" como "calidad de seguro", y "seguro" es definido como "libre de todo peligro, daño o riesgo". De la noción anterior podemos destacar dos elementos: uno de carácter subjetivo (la percepción de una persona respecto de sentir miedo o peligro) y el otro de carácter objetivo (el hecho concreto de no existir riesgo alguno).

Así como se ha mencionado antes, la seguridad pública está referida a la capacidad de tranquilidad, confianza y orden público.

La seguridad pública desde el punto de vista objetivo se define como "El conjunto de políticas públicas y acciones coherentes y articuladas, que tienden a garantizar la paz pública a través de la prevención y represión de los delitos y de las faltas contra el orden público mediante el sistema de control penal y el de policía administrativa."[14]

---

[12] Montesquieu, *Del espíritu de las leyes*, Madrid, Tecnos, 1987, pp. 106 y 107.

[13] *Diccionario de la lengua española*, 22ª. Ed., versión en línea, consultada en octubre 2010, en: *http://www.ifai.org.mx/.*

[14] Gonzalez Ruiz, Samuel, *et al., Seguridad pública en México. Problemas, Perspectivas y Propuestas,* México, UNAM. p. 43.

La seguridad pública comprende la tranquilidad que debe gozar toda persona ante toda clase de riesgos, ya sean provocados por la naturaleza o por el propio ser humano, así como la prevención, y evitar con ello cualquier desgracia o resquebrajamiento del orden y la paz social.

Como hemos visto, la "seguridad" es un derecho inalienable que el Estado debe garantizar, por otro lado debe actuar de manera que no invada la esfera de la vida privada de los gobernados; situación que merece de reflexión la consideración a la luz del surgimiento de la tecnología que ahora se emplea como medida de protección ante verse rebasado por la ola creciente de inseguridad en el país.

Siguiendo a Samuel González,[15] dentro de los principales objetivos de la seguridad pública se encuentran:

- Mantener el orden público.
- Proteger la integridad física de las personas, así como de los bienes.
- Prevenir la comisión de delitos e infracciones administrativos.
- Colaborar en la investigación y persecución de los delitos.
- Auxiliar a la población en caso de siniestros y desastres.
- Aportar elementos probatorios en el desarrollo de algún proceso jurisdiccional, a lo que puede valerse de los documentos digitales.

Para todo lo anterior es importante destacar la figura de la "policía" como institución encargada de los principales actos de seguridad pública que el Estado debe ofrecer a la población; sin embargo, el surgimiento de esta institución como conocemos ahora en respecto de un ámbito estricto de la *seguridad pública* se da con el surgimiento del Estado moderno.

Si bien, la institución de la policía es quien presta el auxilio y brinda la protección a las personas y sus bienes, ha llegado un punto en el que la capacidad humana de protección y, sobre todo, de *vigilancia* se vuelve muy complicada debido a un sinnúmero de causas que pudieran ser perjudiciales para el mantenimiento del orden y armonía social.

De lo anterior podemos advertir cómo el surgimiento de las tecnologías de vigilancia llegaron como una herramienta muy importante para el auxilio de las funciones de vigilancia, protección de las personas y sus bienes, pero más aún de la prevención del delito, fenómenos naturales que provoquen daños y otras eventualidades desafortunadas; por eso el desarrollo tecnológico es aprovechado por la policía.

---

[15] *Ibidem,* p. 43.

4. Vigilancia

Para avanzar al respecto, es importante encontrar la noción sobre el significado de "vigilancia", vocablo que proviene de latín *vigilare*, que significa "velar sobre alguien o algo", o "atender exacta y cuidadosamente a él o a ello".[16]

De lo anterior podemos mencionar que los términos vigilar y seguridad pública tienen un vínculo inseparable, pues no podemos concebir que un cuerpo de seguridad, llamémosle "policía", pueda desarrollar funciones de prevención, protección y auxilio sin contar con métodos y mecanismos de vigilancia adecuados.

A razón de lo importante que resulta la acción de vigilar, es que el propio gobierno a través de los cuerpos policiacos ha desarrollado sistemas de vigilancia humanos con auxilio de herramientas tecnológicas cada vez más caras y que permiten una mayor probabilidad de captar los acontecimientos.

A tal punto, resulta que se ha encontrado en los dispositivos tecnológicos una herramienta indispensable hoy en día para desarrollar la función de policía, surgiendo con ello la *"videovigilancia"*.

III. El derecho de protección de datos personales y la videovigilancia

A nivel Internacional, un esfuerzo importante que reúne a casi todos los países del mundo, es la Agenda de Tunez para la sociedad de la información, en el punto 39 del apartado de la gobernanza en Internet, la Asamblea General de las Naciones Unidas solicita a las naciones un incremento de la cooperación internacional para fortalecer la seguridad, mejorando al mismo tiempo la protección de la información, privacidad y datos personales.

Para entrar al tema del derecho de *protección de datos perosonles*, nos parece importante recalcar el punto de encuentro entre este derecho y la videovigilancia. Cuando hablamos de datos personales nos hace pensar de manera inmediata en información, y la videovigilancia es un dato personal en tanto la imagen constituye un medio de identificar a una persona. Para ello se debe precisar el concepto de "datos personales".

---

[16] *Diccionario de la lengua española*, 22ª. ed., consultada en línea en *http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=seguridad* octubre 2010.

La importancia de los datos personales radica en el valor económico que ahora tienen en la era de la información dentro de la sociedad globalizada, en la que casi todo se está volviendo un proceso automatizado y el plus de las actividades es el conocimiento completo y exacto sobre las cosas o las personas. Siguiendo al doctor Julio Téllez: "la importancia de la información no esta puesta en duda y es un verdadero bien susceptible de apoderamiento con un innegable valor patrimonial o contenido económico inherente o intrínseco, que radica en su destino y utilidad".[17]

En el entendido de que los datos personales pueden ser suficientes para unos fines y para otros no, en cuanto a la identificación, deberá tenerse en cuenta que los datos acumulados constituyen un mayor valor para la identificación, la información y la toma de decisiones y en esa medida el derecho debe distinguir y definir.

1. Concepto

Antes de dar alguna definición de "datos personales" hay que mencionar el fundamento constitucional que México tiene para que tal figura sea un derecho fundamental.

Nuestra Carta Magna establece en su artículo 6°, segunda fracción, que: "La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes". Aunado a lo dispuesto en el artículo 73, fracción XXIX-O, respecto a la facultad expresas del Congreso de la Unión para legislar en materia de datos personales en posesión de particulares. Por otra parte, el artículo 16, segundo párrafo, establece de manera tajante al derecho de protección de datos personales como un verdadero derecho fundamental en el marco jurídico mexicano, en los siguientes términos.

> Artículo 16. Nadie puede ser molestado en su persona,...
> ...
> Toda persona tiene *derecho a la protección de sus datos personales*, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Las cursivas son nuestras).

[17] Téllez Valdés, Julio, Derecho informático, 4ta ed., México, Mc Graw Hill, 2009, p. 69.

Con las reformas mencionadas, se concibe finalmente el marco jurídico constitucional para que, tras largos años y numerosas iniciativas de ley al respecto, sea publicada el 5 de julio del 2010 la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.[18]

Ya en materia de la ley específica, reglamentaria del segundo párrafo del artículo 16, en su artículo tercero establece un conjunto de definiciones, de entre los cuales obtenemos que:

> Artículo 3°.
> V. "Se entenderá por datos personales: Cualquier información concerniente a una persona física *identificada* o *identificable*".

El mismo artículo ofrece una división entre datos sensibles y no sensibles al señalar que se entenderá por:

> VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran *sensibles* aquellos que puedan revelar aspectos como *origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.* (Las cursivas son nuestras).

Podemos observar que existe una clasificación según lo delicado de la información con relación al grado de afectación que pueda resultar para el titular de los datos, por lo que en el *tratamiento* de la información se encuentra el principal punto de regulación, para así proteger la violación a los preceptos de la ley específica y los demás que sean correlativos a este derecho fundamental.

En tal sentido, la misma ley federal, en el mismo artículo 3°, pero en su fracción XVIII, define el tratamiento como: "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales".

Ahora bien, para el correcto goce de este derecho se han establecido principios rectores de mismo con la finalidad de dar garantía estricta a las libertades y facultades de las personas y

---

[18]Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Del 5 de julio de 2010.

delimitar las atribuciones de las personas responsables y de los titulares de las bases de datos y la obligación de la autoridad que el Estado encomienda para su control y cumplimiento.[19]

2. Principios

En opinión de José Luis Piñar Mañas, los principios que rigen el derecho de protección de datos personales pueden reducirse en consentimiento, información, finalidad, calidad de los datos con especial referencia a la proporcionalidad, seguridad y el que denominaría quizá el principio del control independiente.

Estos principios rectores se encuentran señalados en la propia ley específica, en su artículo 6°, en el cual se establece que "los responsables en el tratamiento de datos personales, deberán observar los principios de *licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad,* previstos en la ley".

Son éstos los que determinarán el margen de aplicación de los derechos que a su vez integran el derecho fundamental que estamos tratando. Ahora bien, para atender estos principios, la propia ley establece en el capítulo segundo "De los principios de protección de datos personales", de donde podemos desprender la siguiente agrupación:

Licitud

- Al *recabarse*: la obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos y;
- Al *tratarse*: con la debida confidencialidad y privacidad, entendida como la confianza que deposita cualquier persona en otra (lealtad), respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes (finalidad) de manera lícita, en cumplimiento del marco jurídico específico y correlativo.

Consentimiento

- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley,

---

[19] *Idem*, en el caso del Estado mexicano, el mismo decreto establece que será el IFAI, ahora Instituto Federal de Acceso a la Información y Datos Personales, el encargado de este control y protección. A lo que surge la duda de ¿qué hay respecto a la información privada y personal que está en manos del gobierno? ¿porqué no se integró una misma ley lo público y lo privado?, ¿porqué se excluyó a las entidades de servicios financieros, y porque la ley no habla sobre datos de personas jurídicas?

- El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito o por medios electrónicos,
- Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Este principio merece especial atención, pues hay muchos casos que por ser delicados deberían exigir para su tratamiento el consentimiento expreso, como en el caso de los datos personales sensibles.

- El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos.

Información

- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.
- El aviso de privacidad deberá contener, al menos, la siguiente información:
    - La identidad y domicilio del responsable que los recaba;
    - Las finalidades del tratamiento de datos;
    - Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
    - Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
    - En su caso, las transferencias de datos que se efectúen, y
    - El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.
- Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.

Calidad

- Que los datos sean pertinentes, correctos, actualizados, sean lo más exactos y completos en relación a la finalidad.

Finalidad

- El responsable de la base de datos cuidará que los datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.
-

Lealtad

- Entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes.

Proporcionalidad,

- *En su doble aspecto de idoneidad y de intervención mínima:*
    - Idoneidad: sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta y relevante en relación con las finalidades previstas en el aviso de privacidad.
    - Intervención mínima: la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho a la intimidad de las personas, al honor y a la propia imagen.

- En tratándose de datos sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Responsabilidad

- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aun cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.
- Como principio de *seguridad*: todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar *confidencialidad* respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Este conjunto de principios serán el eje principal para la aplicación de criterios por parte de los tribunales, y los rectores para los particulares y la propia autoridad encargada de su cumplimiento.

3. Derechos

Es importante ahora hablar de cuáles serán los derechos en los que se reflejan los principios y el procedimiento para hacer valer el cumplimiento de aquéllos. Para ello atenderemos de igual forma a los adoptados por la doctrina y la legislación internacional.

Principalmente son los llamados derechos de *acceso*, *rectificación*, *cancelación* y *oposición* (ARCO), puede además considerarse a manera doctrinal puede considerarse el "derecho a la no interconexión de archivos".[20]

Acceso. Es el derecho que tiene el titular de los datos de acceder a su propia información, a partir de que forman parte de una base de datos, ya sea en papel o en archivo electrónico, y a recibir el aviso de privacidad al que está sujeto el tratamiento.

Rectificación. Es el derecho que le asiste al titular para poder realizar alguna modificación en los datos que forman parte de la base de datos, cuando sean inexactos, incompletos.

Cancelación. Es la facultad del titular de los datos para que los mismos sean dados de baja de la base de datos, ya sea en parte o de manera completa.

Oposición. Este le asiste al titular para estar en contra de que existan datos suyos en una base de datos, por si fueron obtenidos fraudulentamente o sin su consentimiento.

En la multicitada ley se contempla su descripción en los artículos del 22 al 27, y en el capítulo posterior establece el procedimiento para hacerlos valer.

---

[20] Téllez Valdés Julio, *op.* Cit., p. 72.

Así, en su artículo 22 dice:

> Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de *acceso*, *rectificación, cancelación* y *oposición* previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Para lo anterior será necesario cumplir con la formalidad y requisitos de la solicitud, la cual, según el artículo 23, debe contener lo siguiente:

> Artículo 23, La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:
>
> I. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
>
> II. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
>
> III. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y;
>
> IV. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Todo ello, debemos recordar, aun no tiene vigencia, pues un transitorio dio una *vacatio legis* en el siguiente sentido:

> CUARTO. Los titulares podrán ejercer ante los responsables sus derechos de *acceso, rectificación, cancelación y oposición* contemplados en el Capítulo IV de la Ley; así como dar inicio, en su caso, al procedimiento de protección de derechos establecido en el Capítulo VII de la misma, **dieciocho meses** *después* de la entrada en vigor de la Ley.

De la misma manera resulta importante establecer las excepciones que regula la ley multicitada, en su artículo 4°, que establece que:..."los principios y derechos previstos en esta ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la *seguridad* nacional, el orden, la *seguridad* y la salud públicos, así como los derechos de terceros".

La disposición anterior deja de lado, como podemos observar, toda base de datos, y el tratamiento de la información en ellas contenidas y, por tanto, sin ejercicio de derechos de los particulares al tema de la videovigilancia, como mecanismo de captación, almacenamiento y

tratamiento en general de datos personales, constituidos por la propia imagen (derecho que por cierto se encuentra reconocido no en la ley, sino en criterios de la Suprema Corte de Justicia de la Nación); todo ello por la causa excluyente de observancia, consistente en la "seguridad nacional y pública", tema que motiva y justifica en nuestro marco jurídico, la existencia de la videovigilancia.[21]

Retomando la segunda fracción del propio artículo 2°, podemos dar cabida a la videovigilancia llevada por particulares, físicos o morales, siempre y cuando no tenga fines de divulgación o comercial, empero si se trata de nuestra seguridad privada o la de nuestra familia o patrimonio se ve justificada, ello no quita que dejemos de cumplir con las disposiciones de nuestro marco jurídico leído en forma armónica, y nos remitiría al ámbito de la seguridad pública. En el Distrito Federal ese permite la interconexión de sistemas privados a los que opera la secretaría correspondiente, en el caso concreto de la ley aplicable al Distrito Federal.

Todas estas causas hacen que la videovigilancia, ya sea para protección de seguridad nacional o pública diferenciándola de la seguridad privada, cobre importancia su estudio simultáneo entre dos derechos fundamentales, que en ciertos puntos colisionan, el de la protección de datos y la seguridad pública o viceversa. ¿la posible invasión a la privacidad o libertades, se ve justificada por brindar más protección y seguridad pública, misma que el Estado mexicano ha propiciado con la ausencia de políticas de responsabilidad, social y un adecuado manejo y distribución del capital, aunado a la corresponsabilidad de la sociedad misma.

IV. La vigilancia por medios tecnológicos: "videovigilancia"

1. La videovigilancia

Veamos ahora el tema de la videovigilancia como fenómeno que ya existe como parte del auxilio de las agrupaciones de seguridad pública, inteligencia y otras, tanto la que surge a manos de los particulares, sus distintos fines, algunas características técnicas y su regulación jurídica, si la hay, en México.

---

[21] A este respecto cabe señalar que la misma ley establece en su artículo 2° que son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales…

Y excluye de su observancia a:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la **recolección y almacenamiento de datos personales**, que sea para uso exclusivamente personal y sin fines de divulgación o utilización comercial.

A. Concepto de videovigilancia

Ahora bien, este sistema de vigilancia tecnológica o *videovigilancia* se ha vuelto un fenómeno cada vez más frecuente, sobre todo desde aquel desafortunado acontecimiento de las torres gemelas en los Estados Unidos. No podemos ocultar cómo la política de seguridad nacional del país vecino ha tenido eco en las políticas de seguridad interna en nuestro país y muchas de las implementaciones son consecuencia de las duras medidas de control y seguridad del vecino del Norte. Aunado al terrorismo, la ola creciente de delincuencia, el vandalismo, y la descomposición social se han producido entierre en nuestra sociedad. Resulta entonces importante saber sobre la definición de "videovigilancia".

La videovigilancia ha tenido una evolución acelerada en la última década, impulsada por los avances tecnológicos y una preocupación creciente por la seguridad pública y privada. Partiendo de su concepto más general, según la Real Academia de la Lengua Española, la videovigilancia se define como "vigilancia a través de un sistema de cámaras, fijas o móviles".

Para nosotros, la videovigilancia es todo conjunto de tecnologías y productos de su desarrollo, que permiten llevar a cabo la función de vigilancia en condiciones que antes el hombre, por sus limitantes naturales, no podía. Es un sistema que permite captar imágenes fijas o en movimiento con mayor alcance, visión, resolución, posibilita su almacenamiento, consulta y tratamiento, y que se encuentra en constante incremento de capacidades, según el estado actual de la propia tecnología.

Sus comienzos se remontan al surgimiento de una nueva forma de vigilar, pasar de la vigilancia sensorial a la del auxilio de las herramientas y dispositivos electrónicos, desde el video análogo. Ahora los avances han permitido la combinación entre aquellos y los digitales hasta llegar a un entorno completamente digital y que sigue desarrollándose en el camino del *software* y del *hardware*, buscando tener un sistema de vigilancia cada vez más inteligente, lo que conlleva a poseer una amplia cantidad de funciones que son posibles gracias a la tecnología avanzada.

Como punto de partida diremos que el término "videovigilancia" refiere a la vigilancia que se lleva a cabo a través de un sistema de cámaras, ya sean fijas, móviles, a distancia, inalámbricas, de conexión a Internet, etcétera.

La videovigilancia es, también, cualquier dispositivo tecnológico que permita la captación y/o almacenamiento de las imágenes de video u otro formato de imagen en

movimiento. Aunque hay que decir que para contar con un sistema integral de vigilancia tecnológica se requiere de todo un conjunto de herramientas y dispositivos electrónicos (computadoras, consolas de tratamiento de video, equipo de almacenamiento controles de las cámaras, *software* de gestión y administración de las mismas, entre otros).

Ya para el ámbito de la videovigilancia pública, desde luego, es necesario el personal capacitado para ello, sobretodo en caso de la seguridad pública y nacional.

Aunado a la creciente inseguridad que provoca la delincuencia, el sistema de videovigilancia no debería aumentar la preocupación de que su empleo provoque algún menoscabo a las libertades y derechos de las personas. Para hacer alguna identificación sobre ese punto de colisión, es importante ubicar y distinguir cuáles podrían ser sus aplicaciones.

B. Elementos técnicos de la videovigilancia

El surgimiento de este sistema se ubica en la década de los ochenta con los circuitos de seguridad de circuito cerrado de televisión o CCTV, que en principio permitía la captación del video y se transmitía en un monitor a blanco y negro contando con un sistema completamente analógico. Dicha evolución va de lo completamente análogo, pasando por las combinaciones hasta llegar a un entorno digital de red y uso de equipos IP[22] (Internet protocol, por sus siglas en ingles) con *software* especializado en todo el proceso de la videovigilancia.

Cabe mencionar que cada vez son más los sistemas automatizados. La dependencia de éstos a las tareas que realiza la sociedad y el tratamiento de los datos que se recopilan y tratan cada vez con mayor frecuencia ha producido un sinnúmero de impactos importantes, que para el caso del derecho no es diferente. Claro ejemplo del uso de sistemas automatizados, es el caso de imágenes o videos utilizados como medio de prueba o evidencia electrónica en un procedimiento jurisdiccional, cuyo valor probatorio depende en gran medida, de la capacidad de identificar con claridad los datos que hacen identificables a las personas o las cosas, es decir, hay una relación directa con la resolución tecnológica que ofrecen hoy día los sistemas de videovigilancia, mismos que están en una carrera de desarrollo entre competidores del sector por satisfacer las necesidades que exigen los preocupados por la seguridad y los más preocupados por ello buscan el equilibrio entre la mejor vigilancia y la no vulnerabilidad de los derechos fundamentales que están en juego.

[22] IP, refiere a un protocolo de internet, es decir a todos aquellos equipos que cuentan con la posibilidad de conectarse a internet.

C. Evolución de los sistemas de videovigilancia

A continuación se presenta la evolución del sistema o función de videovigilancia en razón del avance tecnológico: [23]

a) Sistemas de circuito cerrado de TV analógicos usando VCR

Un sistema de circuito cerrado de TV (CCTV) analógico que utilice un VCR (grabador de vídeo) representa un sistema completamente analógico formado por cámaras analógicas con salida coaxial, conectadas al VCR para grabar.

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El vídeo no se comprime, y si se graba a una velocidad de imagen completa, una cinta durará como máximo 8 horas. En sistemas mayores se puede conectar un *quad* o un *multiplexor* entre la cámara y el VCR. El *quad/multiplexor* permite grabar el vídeo procedente de varias cámaras en un solo grabador, pero con el inconveniente que tiene una menor vel66ocidad de imagen. Para monitorizar el vídeo, es necesario un monitor analógico.

b) Sistemas de circuito cerrado de TV analógicos usando DVR

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR (grabador de vídeo digital) es un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de los DVR cuentan con varias entradas de vídeo, normalmente 4, 9 ó 16, lo que significa que también incluyen la funcionalidad de los *quads* y *multiplexores.*

El sistema DVR añade las siguientes ventajas:

- ✓ No es necesario cambiar las cintas.

---

[23] Véase la página de AXIS, en línea, consultada en septiembre 2010 en: *http://www.axis.com/es/products/video/about_networkvideo/evolution.htm#vidoeservers.*

- ✓ Calidad de imagen constante.

c) Sistemas de circuito cerrado de TV analógicos usando DVR de red

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR IP es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el vídeo se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitorice en un PC en una ubicación remota.

El sistema DVR IP añade las siguientes ventajas:

- ✓ Monitorización remota de vídeo a través de una computadora o PC.
- ✓ Funcionamiento remoto del sistema.

d) *Sistemas de vídeo IP que utilizan servidores de vídeo*

Un sistema de vídeo IP que utiliza servidores de vídeo incluye un servidor de vídeo, un conmutador de red y un PC con *software* de gestión de vídeo. La cámara analógica se conecta al servidor de vídeo, el cual digitaliza y comprime el vídeo. A continuación, el servidor de vídeo se conecta a una red y transmite el vídeo a través de un conmutador de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de vídeo IP.

Un sistema de vídeo IP que utiliza servidores de vídeo añade las ventajas siguientes:

- ✓ Utilización de red estándar y *hardware* de servidor de PC para la grabación y gestión de vídeo.
- ✓ El sistema es escalable en ampliaciones de una cámara cada vez.
- ✓ Es posible la grabación fuera de las instalaciones.
- ✓ Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP.

e) Sistemas de vídeo IP que utilizan cámaras IP

Una cámara IP combina una cámara y un ordenador en una unidad, lo que incluye la digitalización y la compresión del vídeo, así como un conector de red. El vídeo se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con *software* de gestión de vídeo. Esto representa un verdadero sistema de vídeo IP donde no se utilizan componentes analógicos.

Un sistema de vídeo IP que utiliza cámaras IP añade las ventajas siguientes:

- ✓ Cámaras de alta resolución (mega pixel).
- ✓ Calidad de imagen constante.
- ✓ Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica.
- ✓ Funciones de *Pan/tilt/zoom*, audio, entradas y salidas digitales a través de IP, junto con el vídeo.
- ✓ Flexibilidad y escalabilidad completas.

Este sistema saca el máximo partido de la tecnología digital y proporciona una calidad de imagen constante desde la cámara hasta el visualizador, dondequiera que estén.

Desde los sistemas análogos, de una cinta magnética, pasando por los formatos de video, y ahora con el uso de la tecnología digital es posible que gran cantidad de video o imágenes sean almacenados en medios electrónicos, como discos duros, DVR, etcétera. Ahora en la llamada información en la nube[24] se presentan nuevos retos tecnológicos y de operación, pero ante la inseguridad informática y su gestión traen también implicaciones con el derecho de protección de datos personales, la intimidad, la privacidad y la tranquilidad de los titulares de la información, sobretodo porque en el entorno completamente virtual se elimina la posibilidad de control a través de medios físicos (*hardware*) y lógicos (*software*) y el control de la información está en manos de terceros, que además al tener información de otros, cobra gran valor, por lo que resulta de vital importancia establecer normas pertinentes que garanticen la confidencialidad, integridad, seguridad y funcionalidad de la información contenida en la aún poco conocida c*loud computing.*

El sistema de vigilancia tecnológica también representa un incremento en la capacidad de operación, pues incrementa el número de ojos y la capacidad de la visión, de acción incansable de 24 horas x 365 días, sin embargo se debe buscar el justo equilibrio para que no resulte excesivo ni en el ámbito privado ni en el de la seguridad pública.

D. Clasificación

[24] Para mayor abundamiento, véase Gilje Jaatun, Martin Springer, *Cloud computing: First International Conference, CloudCom 2009*, China, Beijing, 1-4 de diciembre, de 2009.

Se puede dar en atención de diversos factores, su fin, al sujeto, a la tecnología utilizad, etcétera. Sin embargo, para atender el fenómeno, podemos clasificarla como:

a. Videovigilancia pública, en tanto se trata de información de carácter pública por la finalidad de su captación, y el operador que la obtiene almacena y hace tratamiento de ella, de lo que se puede mencionar los siguientes campos de aplicación:

- Seguridad pública: en hospitales, edificios y oficinas públicas, parques, jardines, plazas y cualquier otro espacio abierto al público, así como museos, trasportes públicos, avenidas y cruces principales, y cualquier otro señalado como de alto riesgo para la seguridad de las personas y de alto índice delictivo.
- Combate a la corrupción.
- Con fines de investigación policiaca.
- Como evidencia para procesos jurisdiccionales.
- Control de vialidad y tránsito.
- Prevención de emergencias y riesgos naturales.
- Atención a urgencias y emisión de alarmas.
- Auxilio del servicios de protección civil.
- Trabajos de inteligencia por parte de autoridades.
- Persuasión de actos ilícitos en cualquier ámbito.

b. Videovigilancia privada, es la información que se recoge y puede tratar un particular como responsable, de entre lo cual se encuentran aplicaciones como:

- Seguridad privada: en el hogar, la oficina, de manera portátil, en el auto o trasporte privado, en cualquier establecimiento privado.
- Con fines laborales y de producción, para ver que se cumplan con los términos pactados entre trabajador y empleado.
- En los centros educativos, guarderías y otros centros educativos.
- Con fines de diversión o a nivel personal.

De las finalidades anteriores, podemos observar que el tema de seguridad, es el principal motivo por el cual se realiza, con mayor frecuencia, la instalación de sistemas de videovigilancia. De las anteriores finalidades, pueden ser cubiertas de distinta manera, según las distintas posibilidades que ofrece la tecnologías, es decir, la amplia gama de equipos que existen en el mercado de la videovigilancia, pues en su variedad ofrece mayor o menor grado de calidad y capacidad en la captación y tratamiento y serán más oportunas según la finalidad específica

que se persiga. Pero lo anterior puede también ser excesivo y conculcador de derechos, en tanto no se cumpla con principios definidos y adoptados ya a nivel internacional.

2. Videovigilancia y el *cloud computing*

En el tema de la videovigilancia no debemos olvidar que el avance tecnológico ofrece de manera constante nuevas oportunidades y nuevos retos, es así como dentro del proceso que implica la videovigilancia se encuentra el acceso, almacenamiento y disposición, entre otros, y en estos tres se puede llevar ahora de manera virtual gracias al denominado *cloud compiuting*, o computación en la nube, porque las imágenes o fotografías que conforman el sistema de videovigilancia en cuanto a formatos, pueden ser almacenados como mera información y para ello resulta o puede resultar muy atractivo el conjunto de servicios que ofrece esta nueva presentación de esquema en la nube.

Con el sistema mencionado, es cierto que surgen nuevos retos a la administración de negocios, a la seguridad informática y desde luego que al derecho en tanto la información se convierte en un bien intangible de gran valor para su titular y como en el caso de datos personales, las imágenes o videos también son susceptibles de ser mal utilizados o con fines perjudiciales, significando una alerta para regular incluyendo los sistemas de información en materia de videovigilancia en la nube.

El uso de computación en la nube pareciera tener recién aparición, sin embargo ha sido el mecanismo empleado por las cuentas de correo, "*hotmail*, *yahoo*, *gmail*, etcétera." Pues la información se queda almacenada en un espacio inmaterial, que sin necesidad de gran estructura en la computadora puede ser accesible, tratada y transferible mediante el mismo canal y en el mismo entorno virtual que proveen las redes, principalmente Internet.

De manera que podemos definir el *cloud computing* o computación en la nube como un nuevo esquema de prestación de servicios de tecnologías de la información y comunicación, que permite el acceso a una gama de servicios uniformes sobre la plataforma de un entorno virtual (como acceso y tratamiento de la información, con mayor capacidad de almacenamiento y facilidad para su transferencia), siempre y cuando se trabaje dentro de una red.

Tipos de nubes

Las nubes podrían ser de distintos tipos, esto depende de varios criterios:

a) Cuántos y quiénes usan la nube, si una sola persona, (privada) o más de una (pública).

b) Según el carácter del titular de la nube, en públicas (de gobierno u órgano del Estado), privadas (de particulares) o híbridas (como nube paraestatal o compartida entre ambos sectores).

c) Según el tipo de red que se utilice, abiertas (como la nube basada en Internet) o cerradas (basada en intranets),

d) Según el carácter o clasificación de la información, en públicas (gubernamental) o privadas (civiles o particulares).

Respecto a las nubes y su seguridad ante la privacidad de la información, se pueden señalar:

1) Las *nubes privadas*, representan un conjunto de elementos e infraestructura tecnológica que puede garantizar un mayor almacenamiento y mejor funcionalidad en el manejo de la información, pero sobretodo puede aportar alto grado de seguridad en tanto el acceso está restringido. Las nubes privadas están en una infraestructura *on-demand,* manejada por un solo cliente, que controla qué aplicaciones utiliza, cómo las clasifica, el perfil de acceso, cuáles deben correr, dónde, en qué momento y puede llevar en sí misma una bitácora de uso y otros mecanismos de seguridad de la información, aunados a la seguridad física.
2) Las *nubes públicas* se manejan por terceras personas, en ellas la información de miles de usuarios pueden estar alojados en los mismos servidores, sistemas de almacenamiento y otras partes dentro del sistema *cloud compiuting* y depende de los mecanismos de seguridad que utilice el tercero.
3) Las *nubes híbridas* combinan los modelos de nubes públicas y privadas. El usuario es propietario de unas partes y comparte otras, aunque de una manera controlada. Las nubes híbridas ofrecen la promesa del escalado aprovisionada externamente, *on-demand*, pero añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Esta resulta preferible si entre ambas partes existen mecanismos y políticas adecuadas de seguridad de la información.

Algunos puntos a favor son:

- ✓ Acceso a la información y los servicios desde cualquier lugar del mundo, por su presencia siempre al cien por ciento en Internet,
- ✓ Servicios gratuitos o de pago según la contratación y finalidad del titular.
- ✓ Puede disminuir en gran medida los costos.
- ✓ Mayor capacidad de procesamiento y transferencia de archivos en relación con la conectividad o ancho de banda.
- ✓ Almacenar la información sin necesidad de contar con equipos de cómputo fijos o algún *software* especial que puede ser muy costoso.
- ✓ Disminución en el espacio que se destinaria a servidores y equipos.

Como desventaja tenemos:

- La dependencia de los servicios en línea o del funcionamiento de otra persona u empresa.
- Posibilita el acceso de toda la información a terceras personas.
- Posibles inconvenientes técnicos de conectividad a Internet (conexión, velocidad y disponibilidad).

V. Regulación jurídica de la videovigilancia en México

En la seguridad privada o pública se da el principal campo de aplicación de los sistemas tecnológicos de vigilancia, por lo cual analizaremos el marco regulatorio de este ámbito de aplicación en el Estado mexicano. Para ello resulta menester referirnos primero al derecho fundamental a la seguridad, que es al mismo tiempo una obligación del propio Estado a través del gobierno y la entidad correspondiente; analizaremos lo que, al respecto, establece la Constitución federal, la Ley Federal de Seguridad Pública y la Ley que Regula el uso de Tecnología para la Seguridad Pública del Distrito Federal.

Ya hemos señalado algunos artículos constitucionales sobre el derecho de protección de datos personales, como es el caso del 6°, fracción II, el 16, segundo párrafo, el 73, fracción XXIX-O, su vínculo estrecho con otros derechos fundamentales que pueden estar en juego con el fenómenos de la vigilancia, como el caso de la libertad de expresión, de asociación, de libre tránsito, entre otros, pero ahora toca turno a señalar el marco del derecho fundamental de la seguridad pública, pero en relación con la videovigilancia.

En nuestra carta magna se establece respecto de la "seguridad" los siguientes artículos:

> Artículo 21. La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.
>
> …
>
> La seguridad pública es una función a cargo de la Federación, el Distrito Federal, los Estados y los Municipios, que comprende la prevención de los delitos; la investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución.

…

Las instituciones de seguridad pública serán de carácter civil, disciplinado y profesional. El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno deberán coordinarse entre sí para cumplir los objetivos de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública, el cual comprende la que estará sujeto a las siguientes bases mínimas:

…

Del artículo antes citado podemos ver claramente cómo el derecho de la seguridad, además de ser un derecho para los habitantes, es también una obligación para los distintos órdenes de gobierno, mismos que estarán coordinados bajo el sistema nacional de seguridad pública, como funciones de policía *latu sensu*, es decir, a quien da cumplimiento al derecho a la seguridad que tienen los habitantes en ámbito de la investigación de los delitos, la protección de la sociedad y el restablecimiento del orden y la paz social.

Artículo 25. Corresponde al Estado la rectoría del desarrollo nacional para garantizar que éste sea integral y sustentable, que fortalezca la Soberanía de la Nación y su régimen democrático y que, mediante el fomento del crecimiento económico y el empleo y una más justa distribución del ingreso y la riqueza, permita el pleno ejercicio de la libertad y la dignidad de los individuos, grupos y clases sociales, cuya *seguridad* protege esta Constitución. (Las cursivas son nuestras)

Por lo que respecta a la regulación secundaria, es la Ley Federal de Seguridad Nacional la que principalmente establece las funciones que deberán llevar a cabo las agrupaciones encargadas de velar por el cumplimiento de este derecho, así como las excepciones por causa justificada. El artículo primero de dicha como objetivo; establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la seguridad nacional, en sus respectivos ámbitos de competencia.

Dentro de las atribuciones del Centro Nacional de Investigación y Seguridad Nacional se encuentra el adquirir, administrar, desarrollar y operar *tecnología especializada*[25] para la investigación y difusión confiable de las comunicaciones del gobierno federal en materia de

[25] Dentro de ésta se encuentra el equipo de videovigilancia, que permite llevar a cabo la función asignada a los órganos de seguridad de una manera más eficaz en el combate a la delincuencia y/o la prestación de auxilio a la sociedad e incluso para la prevención de siniestros, o ataques a la seguridad nacional.

seguridad nacional, así como para la protección de esas comunicaciones y de la información que posea.

Asimismo, el segundo párrafo del artículo 25 establece que:

> En materia de procuración de justicia, el Centro será auxiliar del Ministerio Público de la Federación y prestará cooperación, apoyo técnico y tecnológico, intercambio de información sobre delincuencia organizada y las demás acciones que se acuerden en el Consejo, observando en todo momento respeto a las formalidades legales, las garantías individuales y los derechos humanos.

Como se puede observar de la descripción del párrafo anterior, la seguridad debe beneficiarse de la tecnología que tiene a su alcance el centro nacional de investigación y seguridad nacional, pero siempre respetando el contenido de los derechos fundamentales de los habitantes.

De manera más concreta, ya en el marco jurídico local, existen ordenamientos que contienen disposiciones precisas sobre el uso de tecnologías de videovigilancia para la seguridad pública, como en el caso del Distrito Federal, y en los estados de Aguascalientes y Colima.

La Ley que Regula el uso de Tecnología para la Seguridad Pública del Distrito Federal,[26] podemos destacar lo siguiente, respecto de la videovigilancia:

El objeto de la Ley (artículo 1°):

- Regular la ubicación, instalación y operación de equipos y sistemas tecnológicos,
- Contribuir al mantenimiento del orden, la tranquilidad y estabilidad en la convivencia,
- Prevenir situaciones de emergencia o desastre e incrementar la seguridad ciudadana,
- Regular la utilización de la información obtenida por el uso de equipos y sistemas tecnológicos en las materias de seguridad pública y procuración de justicia,
- Con la información obtenida, generar inteligencia para la prevención de la delincuencia e infracciones administrativas.

Algunas definiciones importantes con relación a la videovigilancia (artículo 2°) son:

---

[26] Publicada en la *Gaceta Oficial del Distrito Federal* el 27 de octubre de 2008.

- *Cadena de Custodia*: documento oficial donde se asienta la obtención de información por el uso de equipos y sistemas tecnológicos por la Secretaría así como sus características específicas de identificación; con objeto de cada persona o servidor público a la que se le transmite la información suscriba en la misma su recepción, así como toda circunstancia relativa a su inviolabilidad e inalterabilidad, haciéndose responsable de su conservación y cuidado hasta su traslado a otra persona o servidor público;
- *Equipos tecnológicos*: conjunto de aparatos y dispositivos para el tratamiento de voz o imagen, que constituyen el material de un sistema o un medio.
- *Inteligencia para la prevención*: conocimiento obtenido a partir del acopio, procesamiento, diseminación y aprovechamiento de información, para la toma de decisiones.
- *Medio*: dispositivo electrónico que permite recibir y/o transmitir información para apoyar las tareas de seguridad pública.
- *Sistema tecnológico*: conjunto organizado de dispositivos electrónicos, programas de cómputo y en general todo aquello basado en tecnologías de la información para apoyar tareas de seguridad pública.
- *Tecnología*: conjunto de técnicas de la información, utilizadas para apoyar tareas de seguridad pública.

Sobre la instalación de equipos de videovigilancia (artículos 4° a 9°), se establecen los criterios y principios para ello:

- Se hará en lugares en los que se contribuya a prevenir, inhibir y combatir conductas ilícitas y a garantizar el orden y la tranquilidad de los habitantes.
- Queda prohibida la colocación de equipos y sistemas tecnológicos, al interior de los domicilios particulares, así como aquella instalada en cualquier lugar, con objeto de obtener información personal o familiar.
- Los criterios para definir el lugar de instalación de videovigilancia son:
    - Lugares y zonas peligrosas.
    - Zonas con alto índice delictivo.
    - Cruces y avenidas de tránsito abundante y peligrosos.
    - Lugares donde se registran los delitos de mayor impacto.
    - Lugares donde mayor actos contra el civismo.
    - Lugares que por su naturaleza puedan ocasionar riesgos o alertar sobre fenómenos de la naturaleza que provoque daño a la sociedad.

Sobre el uso y tratamiento de la información que se recabe o almacene mediante los sistemas tecnológicos (artículo15):

- Prevención, investigación y persecución del delito, de infracciones administrativas y para servir como evidencia en juicios de cualquier tipo donde se admitan.

Respecto al principio de licitud, la información que re obtenga con videovigilancia, no podrá ser usada como medio de prueba (artículo 16), cuando:

- Provenga de la intervención de comunicaciones privadas no autorizadas conforme a la ley.
- Cuando se clasifique, analice, custodie, difunda o distribuya sin apegarse a la a ley.
- Cuando se obtenga del interior de un domicilio o violente el derecho a la vida privada de las personas.

La obtención de información por videovigilancia será medio de prueba en los procedimientos ministeriales y judiciales de justicia para adolescentes, y administrativos, seguidos en forma de juicio (artículo 29).Y será prueba plena si se cumplió con la cadena de custodia (artículo 25) y salvo el caso en que, durante el transcurso del procedimiento correspondiente, se acredite que fue obtenida en contravención de alguna de las disposiciones de la presente Ley (artículo 35).

En el estado de Aguascalientes existe la Ley de Videovigilancia, en la que se define a la videovigilancia como: “la captación de imágenes con o sin sonido por los cuerpos de seguridad pública estatal o municipales o de seguridad privada”. Aunado al reglamento a dicha ley, en la cual detalla las atribuciones que tendrán los distintos integrantes de los órganos que la lay señala para el cumplimiento de la seguridad pública.

El estado de Colima cuenta con la ley que regula la videovigilancia en el estado, misma que establece algunos puntos importantes, como el señalamiento de cuáles son los espacios públicos abiertos, cerrados, además de los derechos de los ciudadanos respecto de la videovigilancia y el tratamiento de la información.

En su artículo 5° establece algunos términos a destacar, como:

- *Video vigilancia*: al sistema de video vigilancia es aquel medio electrónico compuesto por una o varias cámaras, ya sean digitales o análogas y un sistema de grabación y visualización.

- *Espacio público*: el lugar donde cualquier persona tiene el derecho de circular e implica un dominio público cuyo uso es social y colectivo.
- *Espacio privado*: el Conjunto del espacio doméstico y el espacio personal.
- *Espacio privado con uso público*: son aquellos lugares de carácter privado que cumplen funciones materiales y tangibles con el fin de satisfacer las necesidades colectivas con una dimensión social, cultural y política.

Y agrega algo relevante, el hecho de considerar derechos para los ciudadanos respecto del deber de informar de manera clara y permanente de la existencia de grabaciones obtenidas del sistema de videovigilancia (artículo 19). Además de establecer, en diversos artículos, la exigencia al cumplimiento de los principios de los datos personales.

VI. CONSIDERACIONES FINALES

A manera de consideraciones finales podemos decir que la videovigilancia es un fenómeno que cada día se da con mayor frecuencia tanto en el ámbito público como en el privado, sin embargo y como se señaló, es primordialmente empleada en el campo de la seguridad, pues el temor que ha generado la creciente inseguridad arroja al Estado y al particular a buscar protección con ayuda de la tecnología.

La vdieovigilancia constituye, en sí misma, un fenómeno donde se enfrentan o colisionan varios derechos, debido al tratamiento de información que puede identificar o vuelve identificable a una persona, por un lado la “seguridad” y por el otro, la “privacidad”, la “libertad”, la “libre asociación” y “manifestación de las ideas” y el ahora derecho fundamental de “protección de datos personales”.

Este punto de impacto produce un conflicto que en cada caso concreto habrá de resolverse atendiendo a una ponderación de derechos que no siempre es sencilla, y más aún será necesario atender a resoluciones y experiencias internacionales bajo el respeto al Estado de derecho.

La ola de inseguridad guarda estrecha relación con lo efectivas que están siendo las políticas del Estado mexicano, pues son directamente proporcionales con la satisfacción de

necesidades, tranquilidad y libertades. Así que el uso de tecnologías no debe ser una preocupación para la sociedad ante el mal uso de la videovigilancia.

VII. FUENTES DE CONSULTA

ABA CATOIRA, Ana, "La videovigilancia y la garantía de los derechos individuales: su marco jurídico", A*nuario de Facultade de Dereito da Universidade da Coruña*. Coruña, España, núm. 7, 2003.

ACED FÉLEZ, Emilio, *et al*, *Seguridad, Privacidad, Confidencialidad. El desafío de la protección de datos personales*. TRILCE, Uruguay, Montevideo 2004.

AGENCIA de Protección de Datos Personales de la Comunida de Madrid, Guía de Protección de Datos Personales para Servicios Sanitarios Públicos*,* Madrid, España, Thomson Civitas, 2004.

MARCELLA JR., Albert J., *Privacy Handbook. Guidelines, exposures, policy implementation, and international issues*. Wiley and Sons, New Jersey, United States of America, 2003.

ORTEGA GIMÉNEZ, Alfonso, *et al, Guía Práctica sobre Protección de Datos de Carácter Personal para Abogados*; Difusión Jurídica, España 2008."

ALMUZARA ALMAIDA, C. *et al*. *Estudio práctico sobre la protección de datos de carácter personal*. Valladolid, España, Editorial Lex nova, 2007.

NAVALÓN FRANCISCO, Almodóvar, "El Dato Personal Terapéutico, European Pharmaceutical Law Group", Madrid, España, 2005.

RUIZ CARRILLO, Antonio, *Manual Práctico de Protección de Datos*, *Barcelona, España, Bosch 2005.*

TRONCOSO REIGADA, Antonio, *Estudios sobre Administraciones Públicas y Protección de Datos Personales. EI encuentro entre agencias autonómicas de protección de datos personales*. Agencia de Protección de Datos de la Comunidad de Madrid*,* Madrid, España 2006.

MIRALLES, A, Aparisi. *El proyecto genoma humano: algunas reflexiones sobre sus relaciones con el derecho*. Tirant lo Blanch, Valencia, España, 1997.

JORQUERA GONZÁLEZ, H., *Bases de datos genéticos de identificación criminal*. Santiago, Chile, 2002.

ARENAS RAMIRO, Mónica *El Derecho Fundamental a la Protección de Datos Personales en Europa*, Valencia, España, Tirant lo Blanch, 2006.

ARZOZ Santisteban, Xabier, "Videovigilancia y Derechos Fundamentales: Análisis de la Constitucionalidad de la ley Orgánica 4/1997". *Revista Española de Derecho Constitucional, a*ño 22, núm. 64, Madrid, España, enero-abril, 2002.

LAZCANO, Iñigo, *Coaut. "*La Distribución de Fotografías e Imágenes por la Policía y las Autoridades de Videovigilancia a los Medios de Comunicación." *Revista Vasca de Administración Pública.* núm. 67, Septiembre-Diciembre, España, 2003.

GONZÁLEZ-DUARTE, R.. *Los retos de la genética en el siglo XXI: genética y bioética*. *Estudi general*, 5. Barcelona, España, Edicions Universitat de Barcelona, 2002.

AXIS Communications. *Guía Técnica de vídeo IP.* 2006-2009.

----------. La evolución de los sistemas de vigilancia por vídeo. Disponible en línea, el 22 de Abril de 2010 en: *http://www.axis.com/es/products/video/about_networkvideo/evolution.htm#vidoeservers.*

----------. Sistemas de gestión de vídeo. Disponible en línea en: *http://www.axis.com/es/products/video/about_networkvideo/platforms.htm.* Consultada en agosto 2010.

CONGRESO Iberoamericano de derecho e informática. Ponencias, VI Congreso iberoamericano de derecho e informática. Montevideo, Uruguay, 1998.

ETXEBERRIA GURIDI, José Francisco, *Videovigilancia y el Derecho a la Protección de los Datos de Carácter Personal*. Revista Vasca de Administración Pública. España, núm. 76, septiembre-diciembre,2006.

GARRIGA DOMÍNGUEZ, A. *Tratamiento de datos personales y derechos fundamentales*. Madrid, Dykinson, 2004.

IGLESIA CHAMARRO, Asunción, *Las comisiones de garantías de la videovigilancia*. núm. 68, Madrid, España, Revista de Derecho Político, 2007.

MORENO, Juan Damián, "Reflexiones sobre la reproducción de imágenes como medio de prueba en el proceso penal (a propósito de la llamada videovigilancia)". *Revista Vasca de Derecho Procesal y Arbitraje*. Tomo IX, núm. 2, Mayo-Agosto, San Sebastián, España, 1997.

MOYA GARCÍA, Rodrigo, *El uso de cámaras de video vigilancia como sistema de control empresarial*. Comentario a dictamen 2328-130 de la Dirección de Trabajo Revista Chilena de Derecho Informático. No. 2, Mayo, Santiago de Chile. 2003

NAVA AMORES, José, "La videovigilancia desde la perspectiva del grupo parlamentario de izquierda unida". *Revista Vasca de derecho Procesal y Arbitraje*. t. IX, núm. 2. mayo-agosto, San Sebastián, España, 1997.

NÚÑEZ VIDE, José Luis, "La prueba pertinente: Un Problema Constitucional y Otras Cuestiones. La videovigilancia". *Revista Vasca de Derecho Procesal y Arbitraje*. t. IX, núm. 2, mayo-agosto, San Sebastián, España.1997.

PÉREZ-CRUZ MARTIN, Agustín Jesús, "Videovigilancia y derecho a la Intimidad: ¿Un nuevo ejemplo de conflicto entre el derecho a la seguridad pública y el derecho fundamental a la intimidad?", *Anuario da Facultade de Dereito da Universidade da Coruña*. núm. 1, Coruña, España. 1997.

REAL ACADEMIA ESPAÑOLA. Diccionario de la Lengua Española. 22ª. ed., consultada en: abril de 2010, en: *http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=videovigilancia.*

RESQUERO IBÁÑEZ, José Luis, *"*Aspectos Administrativos de la Videovigilancia (Comentarios al Proyecto de Ley Orgánica de Utilización de Videocámaras por la FCSE en Lugares Públicos)". *Revista Vasca de Derecho Procesal y Arbitraje.* t. IX, núm. 1, mayo, San Sebastián, España, 1997.

REVISTA Seguridad Empresarial. *La evolución del mercado de la Videovigilancia,* disponible en línea en marzo de 2010, en: *http://www.seguridadempresarial.cl/index.php?option=com_content&view=article&id=917:la-evolucion-del-mercado-de-la-videovigilancia&catid=51:estrategialogistica&Itemid=139.*

TÉLLEZ VALDÉS, Julio Alejandro. "Regulación Jurídica de la Videovigilancia." Documento de Trabajo Derecho Constitucional, México UNAM, 2007.

----------. *Derecho informático*, 4ta. ed., México, Mc Graw Hill, 2009.

UII SALCEDO, María V. El Derecho a la Intimidad como Límite a la Videovigilancia. Revista de Derecho Político. núm. 63, 2005. Madrid, España.

VILLAVERDE MENÉNDEZ, Ignacio. "Nuevas Tecnologías, Videovigilancia, Derecho a la Protección de Datos y Ficheros Policiales". *Revista Catalana de Seguretat Pública*. núm. 17, Barcelona, España. 2006.

GALÁN JUÁREZ, M. *Intimidad: nuevas dimensiones de un viejo derecho*. Madrid, Editorial Universitaria Ramón Areces. 2005.