



Universidad Michoacana de San Nicolás de Hidalgo

Facultad de Derecho y Ciencias Sociales

División de Estudios de Posgrado

Maestría en Derecho de la Información

**Tesis para obtener el grado de Maestra en Derecho de la
Información**

**“Entre el Espionaje y la Colaboración con la Justicia:
(Geolocalización y Retención de Datos Personales por Mandato de
Autoridad)”.**

Presenta

Licenciada Martha Leticia Torres Ortega

Director de Tesis

Doctor Juan Carlos González Vidal



Morelia, Michoacán Junio de 2017

Mi profundo agradecimiento a mi asesor de tesis por todas sus enseñanzas a lo largo de la presente investigación, a mi familia y al Consejo Nacional para la Ciencia y Tecnología, ya que sin su apoyo no hubiera sido posible la culminación de este trabajo.

CONTENIDO

Introducción.....	1
-------------------	---

CAPÍTULO I

1. LA SOCIEDAD DE LA INFORMACIÓN Y EL ESTADO

1.1 Concepto de la Sociedad de la Información.....	6
1.1.1 La ampliación del espectro representacional. Referencias históricas de las tecnologías de la información.....	9
1.2 El Individuo frente a la Sociedad de la Información.....	17
1.2.1 La Identidad.....	17
1.3 El papel del Estado y sus instituciones frente a los desarrollos tecnológicos y su implementación como mecanismo de control en el ejercicio del poder.	24
1.3.1 El Estado actual.....	24
1.3.2 Estado y Poder.....	28

CAPÍTULO II

2. LA SEGURIDAD NACIONAL Y LA PROCURACIÓN DE JUSTICIA EN MÉXICO EN EL CONTEXTO DE LA SOCIEDAD DE LA INFORMACIÓN

2.1 Las funciones administrativas del Estado.....	34
2.2 La intervención administrativa como forma de regulación del Ciberespacio.....	36
2.3 LA intervención administrativa a nivel supraestatal.....	37
2.4 El tema de la Seguridad Nacional, concepto y definición.....	38
2.4.1 Los servicios de inteligencia en México y la crisis de la seguridad Nacional.....	44

2.4.2 El combate a la criminalidad y las nuevas medidas del Estado	48
2.5 La Seguridad Publica en México	51
2.6 Salud pública	57
2.7 El orden público	59

CAPÍTULO III

LA GEOLOCALIZACIÓN Y RETENCIÓN DE DATOS PERSONALES COMO MEDIDAS DE PROCURACIÓN DE JUSTICIA EN MÉXICO

3.1 La Retención de datos y la geolocalización como herramienta del Estado en la procuración de justicia concepto y alcance jurídico	66
3.2 Los Concesionarios y prestadores de servicios de telefonía celular como sujetos obligados y el tratamiento de los datos personales en México	74
3.2.1 Los Datos objeto de tratamiento	78
3.3 Los principios de proporcionalidad y de finalidad en el tratamiento de datos	86
3.3.1 La autorización judicial y autoridad competente para la intervención en relación con el derecho a la inviolabilidad de las comunicaciones	90
3.4 La autodeterminación Informativa como bien jurídico del derecho a la protección de datos personales y su relación con la intimidad	92
3.5 Breve referencia al sistema de Retención de datos en el sistema jurídico español	98
3.6 Análisis de los artículos 189 y 190 fracciones I, II y III de la LFTR.	107
3.7 La postura de los Órganos Garantes ante la retención de datos personales en poder de las compañías de telefonía celular	113

CONCLUSIONES.

BIBLIOGRAFÍA.

RESUMEN

La armonización entre la seguridad de los habitantes de un país y las medidas de vigilancia establecidas por el Estado es factible mediante la implementación de una legislación clara y precisa que garantice al ciudadano el goce de sus derechos humanos como es la privacidad y protección de datos personales a fin de evitar abusos de poder. En México, la conservación de datos personales por parte de las compañías de telefonía celular y la geolocalización como medidas establecidas por la Ley Federal de Telecomunicaciones y Radiodifusión, surge en medio de un ambiente de vulnerabilidad para el gobernado frente a la falta definiciones concretas que justifiquen la vigilancia como es la de Seguridad Nacional y orden público.

ABSTRACT

Harmonization between security of the inhabitants of a country and the surveillance measures established by the government is feasible through the implementation of clear and precise legislation that guarantees the citizen the enjoyment of their human rights, as the privacy and protection of personal data in order to avoid abuses of power. In México, the preservation of personal data by the cellular companies and geolocation as measures established by the Federal Telecommunications and broadcasting act, arises amid an environment of vulnerability for the governed against the lack of concrete definitions that justify the surveillance such as national security and public order.

Palabras clave: Sociedad de la Información, Identidad, Seguridad Nacional, Autorización judicial, Conservación de Datos.

Introducción

Con fecha 9 de julio del 2014 fue aprobada por el Congreso de la Unión, la reforma a la Ley Federal de Telecomunicaciones y Radiodifusión de la cual se desprende como uno de los temas más polémicos, el referente a los artículos 189 y 190 en sus fracciones I, II y III, los cuales plantean la injerencia por parte del Estado Mexicano en la vida privada de los individuos a través de los lineamientos de Colaboración en materia de Seguridad y Justicia.

Esta nueva base legal establecida en nuestro sistema, ha puesto en tela de juicio precisamente el tema de la privacidad y datos personales en manos de la autoridad estatal con el apoyo de las compañías de telecomunicaciones, bajo la justificación de la colaboración con la Justicia y la seguridad Nacional, lo cual ha generado reacciones tanto de asociaciones civiles como de partidos políticos ante el peligro inminente de vulnerar derechos fundamentales, como son la privacidad y, el derecho a la protección de datos personales.

Se trata de un tema que fue debatido en el ambiente académico y político en la etapa inmediata posterior a la reforma de los artículos 189 y 190; sin embargo la discusión ha perdido fuerza frente a las decisiones contundentes de la corte, por lo que no ha sido suficientemente explorado y por tanto carece de evolución legislativa alguna, lo cual se agrava ante el desconocimiento por parte del legislador en la materia.

No obstante los intentos de las asociaciones civiles y decisiones de organismos como es el caso del Alto Tribunal de la Unión Europea, el cual ha considerado dichas medidas como excesivas, estamos frente a una temática que

en México no ha sido concluyente y que involucra serias violaciones a los derechos humanos.

La Comisión Nacional de Derechos Humanos ha interpuesto una queja para impugnar dicha reforma sin resultado alguno, la Suprema Corte ha declarado que dicha intervención será posible en casos de extrema urgencia, un grupo de 219 organizaciones civiles emitieron una carta dirigida al Instituto Nacional de Transparencia y Acceso a la Información Pública Gubernamental (INAI) y al Gobierno Federal, a fin de mostrarle su preocupación por la posible violación al derecho a la privacidad y al derecho a la protección de datos personales de los usuarios de los servicios de telecomunicaciones.

El tema adquiere mayor complejidad si consideramos la inesperada reacción de los órganos garantes, como es el caso del INAI que, en respuesta a dicha reforma, resolvió con una votación de cuatro contra tres comisionados, no ejercitar la acción de inconstitucionalidad ante la Suprema Corte de Justicia de la Nación en contra de la misma, lo cual ha generado aún más polémica por tratarse de la principal Institución garante del derecho de protección de datos personales en México, dando lugar a consecuencias de gran magnitud como es el impacto en la confianza social frente a las Instituciones. La percepción de los bienes jurídicos protegidos por el derecho a la protección de datos personales como son la intimidad y la autodeterminación informativa, inhibe el ejercicio del derecho al acceso a la información pública ante una institución carente de credibilidad.

La presente investigación resulta pertinente debido a que se trata de un tema muy poco explorado, que no ha sido agotado y requiere una consolidación teórica debido a la necesidad de recuperar la dignidad humana que sustenta a los derechos de privacidad y protección de datos personales y que, potencialmente, representa un grave peligro si no se toman las medidas legislativas necesarias.

Por lo anterior, dichas disposiciones deben ser subsanadas y detalladas por medio de ejercicios de ponderación y de derecho comparado que permitan conocer al legislador mexicano los fallos y las incongruencias con la finalidad de que el

secreto que rodea a la vigilancia no sea la justificación para permitir abusos de poder.

Se debe garantizar por un lado el derecho a la seguridad nacional y seguridad jurídica y, por el otro, el derecho a la vida privada y la protección de datos personales, derechos entre los cuales existe una línea muy delgada que puede ser fácilmente cruzada por una ley ambigua, imprecisa y deficiente.

El tema de la conservación de datos es algo que atañe a nuestra vida cotidiana de manera directa y que debe estar sustentado en la razón legal; la privacidad está en juego, por lo que se debe profundizar en el tema a fin de crear conciencia no solamente en el espíritu del legislador en el entendido de contar con leyes especializadas en materia de conservación de datos que cubran las exigencias de una sociedad que está en constante evolución tecnológica y social, sino en la sociedad misma en cuanto a la responsabilidad en el manejo de sus datos personales.

Con base en lo anterior es necesario que los artículos 189 y 190 de la Ley Federal de Telecomunicaciones establezcan de una manera explícita y coherente los sujetos, requisitos y procedimientos necesarios para determinar en qué casos procede tanto la retención de datos personales como la *geolocalización*, de tal manera que sean consideradas como herramientas que realmente permitan colaborar con la administración de justicia, sin que ello implique la violación de derechos fundamentales, como es la protección de datos personales.

Bajo los términos señalados, podemos considerar que los artículos 189 y 190 fracciones I, II, y III carecen de precisión y claridad en su redacción, por lo que vulneran el pleno ejercicio de los derechos a la vida privada y protección de datos personales establecidos en el artículo 16º Constitucional, toda vez que legitiman a la autoridad para implementar la localización geográfica de las personas en tiempo real y avalan la conservación de datos personales por parte de las empresas concesionarias a petición de dicha autoridad de gobierno.

La regulación en análisis carece de un sustento integral que garantice a todos los involucrados las condiciones de aplicabilidad que permitan el goce de los derechos humanos; el sujeto vigilado en su carácter de usuario de telecomunicaciones, no cuenta con los mecanismos legales apropiados para acceder, omitir, corregir y cancelar sus datos personales cuando se les requieren por parte de las compañías de telecomunicaciones.

El Estado actual busca implementar medidas de seguridad con el propósito de combatir la criminalidad, bajo un sistema de vigilancia digital sustentado en la recolección de la identidad de los gobernados sin tener acceso a los mismos, lo que nos conduce a considerar la importancia del teléfono celular como una herramienta capaz de proporcionar una cantidad de datos indiscriminada a las empresas proveedoras, los cuales, transmitidos al gobierno, le permiten acceder a todos y cada uno de los movimientos del usuario del servicio, creando un historial respecto de los lugares que ha visitado y con la capacidad de construir un perfil sobre su ideología, preferencias, estado de salud y todos aquellos aspectos más íntimos de su vida.

Si partimos de la percepción de que la corrupción prevalece entre las instituciones de seguridad pública, la exposición de dicha información puede resultar de gran utilidad a los grupos criminales, que vinculados con las autoridades pueden victimizar aún más al sujeto de la vigilancia, que ya sufre en sí una vulnerabilidad y falta de certeza jurídica en el manejo de sus datos, siendo expuesto a un riesgo constante de ser blanco de la delincuencia, como es el caso de la extorsión y el secuestro.

Mediante un comparativo del sistema jurídico mexicano en materia de conservación de datos y el sistema jurídico español, nos podemos percatar que no obstante que España no está obligado a compartir el criterio de la Directiva 24/2014 que declara a la geolocalización y conservación de datos como invasiva a la privacidad, si cuenta con su propia Ley de Conservación de Datos que regula la retención por parte de las compañías de telefonía celular, así como un organismo que vela por el cumplimiento del derecho a la protección de datos personales de los ciudadanos, como es la Agencia Española de Protección de Datos.

El propósito de la presente investigación es desentrañar el sentido de los artículos 189 y 190 fracciones I, II y III, a fin de determinar su deficiente redacción que coloca al usuario del servicio de telefonía móvil en un estado de fragilidad frente a las prácticas de vigilancia del Estado que, a través de las compañías de que brindan dicho servicio, tiene acceso indiscriminado a la información de aquél, afectando su privacidad y derecho fundamental a la protección de datos personales.

El presente análisis nos permitirá establecer un contacto directo en la búsqueda de información sobre el tema de la conservación de datos a fin de incrementar los conocimientos y establecer una postura definida con el propósito de estar en condiciones de influir y modificar las distintas concepciones y teorías que generen un impacto en la normatividad mexicana.

El acceso indiscriminado a bases de datos genera información sumamente valiosa que permite consolidar el poder de las Instituciones frente al gobernado bajo la excusa de combatir la delincuencia. La única forma de detener este descontrol y afectación de derechos es fomentando la creación de cuerpos normativos modernos, adaptados al avance de la tecnología y que de manera integral protejan a todos los involucrados en el proceso de conservación de información.

Es importante cuestionarnos como principio fundamental de legalidad, el alcance de las decisiones y perjuicios que puede generar un gobierno que no está sometido a control alguno por autoridades judiciales imparciales e independientes, ni órganos de supervisión pública autónomos.

CAPÍTULO I

1. LA SOCIEDAD DE LA INFORMACIÓN Y EL ESTADO

1.1 CONCEPTO DE LA SOCIEDAD DE LA INFORMACIÓN.

El desarrollo de las nuevas tecnologías de la información y las telecomunicaciones ha ido modificando nuestra forma de comunicarnos, dando paso a la creación del nuevo modelo llamado la Sociedad de la Información, la cual ha sido cuestionada por algunos teóricos, como en el caso de Castells, quien la considera como escenario del aislamiento del individuo en sus relaciones sociales, así como de situaciones de poder en los vínculos de tales individuos con los órganos estatales en su calidad de reguladores de dicha sociedad. (2000:22)

“Mientras que la innovación técnica se produce por oleadas y requiere el sostén de la movilización del capital, se tiende a etiquetar a la sociedad de acuerdo con lo que, por una variedad de razones, parece ser su tecnología de comunicaciones dominante. “La era de los ferrocarriles”, “La era de la radio”, “La era de la televisión” y “La era del cine”, se han ido superponiendo una a otra. La prensa, que, como “cuarto estado” no dio nombre a ninguna era, dio en cambio, publicidad a las otras etiquetas” (Burke, 2002: 295).

El paradigma de las tecnologías de la información, que surge en los años 70 en los Estados Unidos, concretamente en California, como consecuencia de la economía global y la geopolítica mundial, materializó un nuevo modo de producir, comunicar y vivir, como menciona Castells, la revolución de la tecnología de la información, de forma medio consciente, difundió en la cultura material de nuestras sociedades el espíritu libertario, que floreció en la década de los sesenta.

Tan pronto como se difundieron las nuevas tecnologías de la información y se las apropiaron diferentes países, culturas, organizaciones, surgieron metas

heterogéneas que explotaron en toda clase de aplicaciones y usos que retroalimentaron la innovación tecnológica, acelerando la velocidad y el alcance del cambio tecnológico y diversificando sus fuentes (2001:32).

Por lo que ve a la cuestión lingüística, nos menciona Burke que surgieron las palabras “flujo” y “fluir” al igual que la palabra “Información” como expresiones muy recurrentes relativas a la “tecnología de la Información”, misma que empezó a ser utilizada en círculos de gestión empresarial y “teoría de la información” en matemáticas.

La persona que más plenamente expresa la idea de una “economía de información” y una “sociedad de la información”, ya en el aire, fue un joven norteamericano, Marc Porat, asociado por entonces al Aspen Institute y quien publicó un trabajo titulado “Global Implications of the Information Society”; en 1977 en su primera forma: se lo encomendó la United States Information Agency (Burke, 2002:291).

La palabra información tiene su origen en el verbo medieval francés, *enforme*, *informe*, el cual significaba “dar forma a”, por lo que la nueva expresión “sociedad de la información” dio forma a un grupo de aspectos hasta entonces con débil relación entre sí, conocimiento, noticias, literatura, entretenimiento, que se intercambiaban a través de diferentes medios y de diferentes materiales: papel, tinta, tela, pintura, celuloide, cine, radio, televisión y ordenadores. Para los años 70 los mensajes públicos y privados, verbales y visuales, comenzaron a tratarse como “datos”, es decir como información que era susceptible de guardar y coleccionarse a través de la tecnología electrónica.

Posteriormente, ya para el siglo XX, los términos *informatique* e *informatización*, provenientes también del francés, relacionados no solo con la comunicación, sino también con cuestiones empresariales y políticas gubernamentales, generaron un vínculo entre estos términos y la computarización; naciendo así, en Francia el término *L'informatisation de la société*, traducido al inglés como *The computerization of the society*. (Burke, 2002:292-293).

Herminia Campuzano considera que la universalización de los recursos informáticos y el desarrollo de las nuevas tecnologías, si bien provocan una revolución técnica en el estado de la ciencia, no agotan ahí sus efectos. Su impacto también es cultural, económico, legal y social. Actos básicos del ser humano como la comunicación, exigencias de su bienestar, como el empleo, la educación, la sanidad o necesidades derivadas de su ser social, como el comercio, se ven influidos por ellas (2000: 19).

Bajo el contexto anterior, define a la sociedad de la información “como un nuevo modelo de organización industrial, cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas tecnologías de la comunicación. Supone una informatización de los diversos sectores, dirigida a abrir una vía de participación de los ciudadanos en todas las facetas de la vida económica y social, así como a obtener en último término, una mejora en su calidad de vida” (Campuzano, 2000: 20).

Entre las tecnologías de la información se incluyen: la microelectrónica, la informática, las telecomunicaciones, como son la televisión, radio, la optoelectrónica y la ingeniería genética, las cuales se han desarrollado y expandido de manera especial en las últimas décadas del presente siglo, los descubrimientos avanzan y se perfeccionan cada vez más.

El observatorio de la Sociedad de la Información y del Conocimiento de la Universidad Autónoma de México, respecto a las tecnologías digitales, ha establecido que “El concepto de “sociedad de la información” hace referencia a un paradigma que está produciendo profundos cambios en nuestro mundo, al comienzo del nuevo milenio. Esta transformación está impulsada principalmente por los nuevos medios disponibles para crear y divulgar información mediante los flujos de información, las comunicaciones y los mecanismos de coordinación, se están digitalizando en muchos sectores de la sociedad, proceso que se traduce en la aparición progresiva de nuevas formas de organización social y productiva.

Para Escobar de la Serna, la Sociedad de la Información es aquella caracterizada, entre otras cosas, por el surgimiento de una serie de medios técnicos de transmisión e información, originados por la expansión de las nuevas tecnologías y por los cambios operados en la sociedad misma, que provocan numerosos comportamientos tanto en lo individual como en lo colectivo, y sobre la formación de hábitos culturales que lógicamente darán lugar a una adecuada y progresiva regulación jurídica “Constituye un fabuloso mecanismo de distribución de poder y por eso mismo, de su capacidad para promover y garantizar la libertad...” (Escobar, 2004:33).

La característica primordial de la sociedad de la Información, a diferencia de las otras transiciones que ha habido a lo largo de la historia, es esa transformación masiva en todos los campos y formas de expresión del conocimiento humano, lo que ha provocado una reacción instintiva por parte del individuo, a fin de controlar las consecuencias inimaginables generadas especialmente debido a la velocidad con que se ha producido ese desarrollo científico y tecnológico, cuya intención ha sido crear un nuevo mundo globalizado e interconectado, que sin embargo de manera simultánea ha tenido efectos opuestos, como toda revolución.

Otro aspecto importante que destaca en las definiciones anteriores, es la calidad de vida y garantía de libertad que, de acuerdo a los autores mencionados, proporciona la tecnología dentro del contexto de la era de la información, que si bien, es determinante para guiar el destino de una sociedad, por supuesto, aplicada adecuadamente como representación de cambios sociales e históricos, también produce efectos colaterales en las relaciones sociales entre los individuos como tales y frente al sistema estatal.

1.1.1 LA AMPLIACIÓN DEL ESPECTRO REPRESENTACIONAL. REFERENCIAS HISTÓRICAS DE LAS TECNOLOGÍAS DE INFORMACIÓN.

Así como en las anteriores revoluciones durante la existencia de la humanidad, el espectro representacional ha presentado cambios culturales profundos; en la actualidad, bajo el contexto de la Sociedad de la Información, dicho espectro amplía las formas de comunicación, desapareciendo tiempo y espacio, lo cual coloca al ser humano frente a una multiplicidad de fenómenos que nos ofrecen una gran cantidad de posibilidades de comportamiento y en sus relaciones con los demás.

El desarrollo de la virtualidad constituye, en todo caso, una expansión del espectro representacional: sea la visita a un museo o a una tienda, estamos ante variantes novedosas de interpretación. Quizá el aspecto más importante a subrayar es este punto, en que esas variantes dan lugar a otra serie de interpretaciones que van a extender la competencia cognitiva de los “usuarios” de la cultura y por tanto sus modos de categorización de la experiencia. (Vidal, 2004: 95)

A partir de los orígenes que tuvo el internet como herramienta militar, desde 1957, mediante la puesta en órbita del Satélite SPUTNIK por parte de la Unión Soviética, ha venido a modificar la jerarquización de los medios de comunicación de una manera avasallante, colocando en segundo término a la televisión y al cine, ante su sorprendente desarrollo en las últimas décadas, al grado de que, en la actualidad es prácticamente imposible calcular los sitios web que existen y los servidores a los que tenemos acceso, ese primer fin militar, se ha transformado en comercial y de negocios, no obstante, hay estudiosos que consideran, que este desarrollo puede también tener fines, por ejemplo, en el ámbito académico, mediante la publicación de trabajos de otros, de manera legal o ilegal. Con mínimos conocimientos informáticos y con acceso a internet, “Así la idea de publicación restringida queda parcialmente superada dentro de la nueva dinámica”. (Vidal, 2004: 96).

Todo proviene de algún conocimiento previo, en algunas ocasiones, como complemento y en otras como una reacción contraria y radical, todo tipo de ideologías y manifestaciones culturales parten de un punto o un antecedente, ya

sea en la ideología, en la ciencia, en el arte, las etapas históricas se traslapan una con otra para crear distintas formas que mezclan lo antiguo con lo contemporáneo.

“Hay que insistir que de acuerdo con Zima... no debe llevar a una posición radical que suponga la simple sustitución de unos paradigmas por otros... ya que subsisten elementos ya dados en la etapa precedente. En términos distintos, podemos asumir que ciertas formas de semiosis se añaden a otras preexistentes, produciéndose eso sí una jerarquización entre ellas, aunque tampoco debemos excluir la posibilidad de que en ocasiones puedan producirse desplazamientos” (Vidal, 2004: 96).

Peter Burke considera que a partir del surgimiento de los ordenadores la palabra “era” es sustituida por la de “generación” aplicable tanto a los ordenadores como a las personas y en cada una de las “eras” se plantearon problemas similares en torno a la relación con la “propiedad” de los medios con su “contenido”, del contenido con la “estructura” y de la “estructura” con la tecnología y en particular con la innovación tecnológica. Todo estaba ligado al control. En todas las épocas se ha asociado la necesidad de control del presente y el futuro por razones personales, políticas y económicas. (Burke, 2002:p. 296)

El lanzamiento del Sputnik en 1957, constituyó un acontecimiento que despertó el interés mundial por el espacio y una reacción de competencia por parte de los Estados Unidos ante la tecnología de la Unión Soviética mediante el Telstar, el primero de una gran cantidad de satélites futuros, lo que hizo necesario un marco de control a través de La ley de Satélite de Comunicaciones de 1962, lo que llevó a montar una nueva compañía La Communications Satellite Corporation, cuyo accionista mayoritario era la compañía AT&T.

En 1963 fueron lanzados Syncom I y II, Telstar II, y al año siguiente Syncom III transmitió los juegos Olímpicos desde Tokio y para 1964, se estableció una International Telecommunications Satellite Organization Company, que para 1975 ya contaba con ochenta y nueve miembros.

Por su parte Europa también comenzó a desarrollar su tecnología satelital, en 1983 se creó la Agencia Espacial Europea, que lanzó su primer satélite, en 1974 se consolidó un acuerdo franco-germano para la construcción de un sistema de satélites cooperativo llamado Synfonía, que proporcionaba la transmisión de sonido y circuitos telefónicos entre Europa y África y posteriormente con América Latina.

De esta manera, se generó un profundo cambio en la industria de la televisión, cuyas transmisiones ahora tenían como base la tecnología satelital, surgiendo la participación de todos los países del mundo por el lanzamiento de satélites al espacio, lo que dio lugar a la creación de un sinnúmero de compañías de transmisión de información vía satélite como el caso de Sky, en Inglaterra, propiedad de Murdoch, figura poderosa tanto en la televisión como en la prensa y que, demostró que la televisión vía satélite comercial podría ser una empresa rentable, principalmente en deporte y presentación de noticias (Burke, 2002:331)

En 1969 Peter Drucker, uno de los más importantes analistas de la transición a la era de la información, consideró que no obstante que ya había compañías internacionales que estaban embarcando hasta mil ordenadores por mes, no había en este campo todavía un equivalente a la bombilla eléctrica de Edison, estableció que ese equivalente sería un “artilugio electrónico” que se vendiera más barato que un aparato de televisión, susceptible de ser enchufado en cualquier sitio en que hubiera electricidad y diera acceso inmediato a toda información necesaria para el trabajo escolar, del nivel elemental a la universidad, además de un uso para muchas otras cosas más (Burke,2002:294).

A partir de que los equipos de cómputo dejaron de ser concebidos como meras máquinas de calcular (a partir de los años setenta), no solo se limitaron a sus funciones de comunicación sino que surgieron nuevas formas para todo tipo de servicios, adquiriendo en cuanto a la apariencia física de los equipos un minimalismo, incluyendo progresivamente, más funciones y aplicaciones.

De acuerdo a Burke, la aparición del internet como tal, surge entre septiembre de 1993 y marzo de 1994 cuando la red hasta entonces solo se había

dedicado a la investigación académica, por lo que se convirtió en red de redes abierta a todo el mundo, el acceso al público al software de búsqueda hizo posible atraer a los usuarios, a los que entonces se llamaba adaptadores y a proveedores pioneros del software.

Como se mencionó con anterioridad, los orígenes del internet se encuentran en la física y en la política de defensa que funcionó por primera vez en 1968, con el apoyo financiero de la Administración de Investigación de Proyectos Avanzados del Departamento de Defensa de los Estados Unidos, fundado en 1957 como parte de la respuesta gubernamental al Sputnik.

Así, Castells nos habla de la “cultura de Internet” dentro de la cual se destacan primordialmente los productores de internet, es decir, los productores usuarios y por otro lado los consumidores usuarios de internet, entendiendo como cultura una construcción colectiva que trasciende a las preferencias individuales e influye en las actividades de las personas pertenecientes a dicha cultura, en éste caso los usuarios y productores de internet.

Establece como característica de “La cultura de internet” una estructura en cuatro estratos superpuestos: la cultura tecnomeritocrática, la cultura Hacker, la cultura comunitaria virtual y la cultura emprendedora. La cultura tecnomeritocrática costumbres en las redes de cooperación en torno a proyectos tecnológicos; la cultura comunitaria virtual, añade una dimensión social a la cooperación tecnológica, al hacer de internet un medio de interacción social selectiva y pertenencia simbólica; por lo que ve a la cultura hacker ésta se caracteriza por tener una organización, pero de carácter informal, o sea, no impuesto por las instituciones de la sociedad.

El vínculo clave entre estas culturas, considera Castells: “Lo constituye el carácter abierto y modificable del software de internet, y especialmente del código de fuente del software. La distribución libre de los códigos fuente, permite a cualquier persona modificar el código y desarrollar nuevos programas y aplicaciones, en una espiral ascendente de innovación tecnológica basada en la

cooperación y la libre circulación de conocimientos técnicos” (Castells, 2001: 52-53).

Trejo García, nos expone que hoy en día los servicios más usados en internet son: Correo electrónico, el cual nos permite enviar cartas escritas con el ordenador a otras personas que tengan acceso a la red; podemos tener contacto con cualquier persona del mundo que disponga de conexión a internet. Este mecanismo es muy usado en el área laboral, pues su uso trae consigo un considerable ahorro de llamadas, tiene un gran potencial en el intercambio de información, ya que reduce de un modo importante el tiempo de transferencia. La World Wide Web, consiste en un sistema de distribución de información, almacenada en la red a través de páginas web, que no son más que páginas de texto con gráficos o fotos y por medio de las cuales muchas empresas han entrado al mercado de internet; el FTP (File Transfer Protocol) permite enviar datos por internet, sin guardar la información en disquetes para usarla en otro ordenador, es utilizado tanto por empresas, como por particulares que quieren dar a conocer sus creaciones informáticas a nivel mundial; el servicio IRC (Internet Relay Chat) nos permite entablar una conversación en tiempo real con una o varias personas por medio de texto, se trata de un medio de entretenimiento y de actividades laborales (Trejo,2006:4).

En cuanto al surgimiento de las tabletas electrónicas, Theodore Roszak nos dice: “...Fue el club Homebrew donde Steven Wozniak presentó su nuevo microordenador en 1977. El nombre que le dio a la máquina-Apple (manzana) aportó un matiz orgánico, levemente rústico con el que se pretendía suavizar las aristas de la tecnología hacer de la máquina un objeto sencillo y amigable. El nombre recordaba también la compañía de discos fundada por los Beatles (2005: 171).

Por lo que ve a los servicios de telefonía, son las últimas aplicaciones que han aparecido para internet. Nos permiten establecer una conexión con voz entre dos personas conectadas a internet desde cualquier parte del mundo sin tener que pagar el costo de la llamada internacional. Algunos de estos servicios incorporan

no solo voz sino también imagen, a esto se le llama videoconferencia (Trejo, 2006: 4-6).

Tanto el desarrollo de la computación como el de la telefonía celular, han sido determinantes en el desarrollo de las tecnologías desde hace más de 20 años, sin embargo, la telefonía celular hasta hace unas décadas había sido incipiente para soportar las aplicaciones básicas del uso de internet en la década de los noventas y el inicio del 2000, por lo que una vez que el internet y la web alcanzaron lo que parecería su auge y evolución, la telefonía inició un desarrollo imparable superando cualquier imaginación sobre su potencial por parte de los usuarios, trasladando a la palma de la mano aplicaciones superiores a las de las propias computadoras, en cuanto a velocidad, que ningún modem de servicio local o banda ancha pudiera ofrecer.

Las tecnologías móviles, han estado presentes en nuestra sociedad, representando una herramienta que facilita tanto la vida cotidiana, como las tareas más complejas relacionadas con el trabajo, los estudios la vida productiva y económica de la sociedad, así como toda una serie de aplicaciones que se han incrementado con el tiempo.

Hablar de la historia de los celulares es referirnos a un tiempo muy breve, se trata de un dispositivo que nos remonta a un control remoto, capaz de conectar a miles de usuarios en el planeta mediante una infraestructura de comunicaciones que jamás hubiéramos imaginado hace unas cuantas décadas, por lo que su estudio por parte de la ingeniería, la eleva a una ciencia exacta que, prefigura lo que el futuro nos depara en esta materia.

En la actualidad, las tecnologías móviles cubren la mayoría de las áreas de servicios de telecomunicaciones y entretenimiento, que abarcan envío de mensajes de texto y multimedia y en los últimos años, la actualización de la información de las redes sociales.

Dentro de este contexto, aparece el concepto de geolocalización como una de las tantas aplicaciones que ha generado el uso de internet, no reconocido aún

por la Real Academia de la Lengua, en virtud de no ser aceptado ni incorporado por la comunidad lingüística, consiste en una práctica relativamente nueva, relacionada con la tecnología satelital cuya historia es más larga y que, actualmente se adapta a los nuevos dispositivos móviles y computadoras con acceso a internet, se trata de la ubicación geográfica de un objeto, en un sistema de coordenadas determinado.

Este servicio implica un conjunto organizado de hardware y software, que se encuentra diseñado especialmente para capturar, almacenar, manipular y analizar en todas sus posibles formas la información geográfica referenciada.

La geolocalización tiene distintas utilidades, entre las que destacan: las aplicaciones web, las herramientas dentro de procedimientos judiciales, instrumentos comerciales y de mercadotecnia, entre otros.

Si bien la evolución tecnológica ha constituido un medio de gran importancia en la generación de movimientos sociales y las expectativas en sus inicios, surgió en el sentido de que favorecería la interacción del gobierno con los individuos; los estados autoritarios, aparentemente, han perdido fuerza, ante la capacidad de información respecto de fuentes no sometidas al mismo frente de la globalización, mermando su dominio sobre la comunicación.

Por otra parte, la realidad histórica nos muestra, no obstante las expresiones de la opinión pública, a través de foros virtuales como es el caso de Facebook y twitter, los gobiernos hacen caso omiso a tales opiniones, utilizando estos instrumentos para publicar su información de manera unilateral, sin generar una verdadera interacción con los gobernados y para tal efecto, es de gran relevancia el papel que llevan a cabo los medios de comunicación entre los que destacan por ser perfectos en ésta acción comunicativa dirigida de uno a muchos, que sigue siendo la norma política, la televisión, la radio y la prensa.

Aunado a las reestructuraciones tecnológicas, se presentan en la actualidad otros factores importantes, como son convulsiones políticas y cambios geopolíticos,

sin embargo, uno de los más grandes desafíos a los que se enfrentan los Estados es el de la criminalidad, tanto nacional como transnacional (crimen organizado, extorsión, tráfico de personas, de órganos etc.) que atenta contra la seguridad de los países tanto desarrollados como en vías de desarrollo, desestabilizando la seguridad y conservación del tejido social en detrimento de la economía.

La estrategia política actual como medio de generación de poder se produce desde dos perspectivas entonces, la primera consiste en la apertura del espacio de información y comunicación global, abierto a todos sus participantes como son organizaciones internacionales, empresas etc., y por otro lado como un gobierno a nivel nacional que tiene que adoptar, no obstante autodenominarse gobierno abierto (nueva tendencia política), una estrategia de información ajustada a proteger sus intereses nacionales y sociales, lo que constituye el objetivo principal de los gobiernos actuales.

Así mismo, el desarrollo desmesurado de la tecnología y su repercusión en los medios de información, hace imprescindible dos factores sustanciales: por un lado la responsabilidad cívica de los ciudadanos de hacer un uso racional tanto de la tecnología como de la información contenida en los medios, a través de una educación y formación tanto en el modo de uso, como en la construcción de una opinión pública objetiva y validada por el estudio y la capacidad de análisis (aprender a seleccionar con quien nos informamos y que aspecto de la información vale o no la pena considerar), y el segundo factor, que estriba en la regulación adecuada y simultánea a la aparición de estos avances tecnológicos que impactan en la sociedad de la información y me parece que la función que lleva a cabo el Derecho de la Información como ciencia jurídica en sus aspectos teórico y práctico, es fundamental para hacer frente a los nuevos retos que nos ofrece este nuevo modelo de sociedad.

1.2 EL INDIVIDUO FRENTE A LA SOCIEDAD DE LA INFORMACIÓN.

1.2.1 LA IDENTIDAD.

Las pantallas de los ordenadores generan la posibilidad de acceder a múltiples ventanas, que representan diferentes mundos virtuales, multiplicando las posibilidades de asumir distintas personalidades de los usuarios, lo que permite modificar su yo, por medio de la metáfora.

Desde su surgimiento, dichas funciones han permitido acceder a distintas funciones en un mismo momento de manera simultánea, lo que genera un notable ahorro de tiempo y esfuerzo, por lo que el individuo es capaz de realizar distintas tareas y recibir distintos tipos de información en un solo momento.

El desarrollo de ventanas en las interfaces del ordenador fue una innovación técnica motivada por el deseo de conseguir que la gente trabajara de forma más eficiente, al poder merodear de una aplicación a otra (Turkle, 1997:18).

Por lo que respecta al término MUD, este es utilizado para englobar todos aquellos juegos de ordenador basados en diferentes clases de software (MUSE, MOO o MUSH).

El mundo virtual representa el escenario experimental para transformar mediante la construcción de identidades nuevas, al grado de aparecer en el mundo virtual como lo opuesto a lo que realmente somos. “La identidad después de todo se refiere al equilibrio entre dos cualidades, en este caso entre la persona y su personaje, sin embargo en los MUDS, uno puede ser muchos personajes” (Turkle:1997:18).

En base a lo anterior podemos observar que el elemento de la identidad, al parecer, se ve fragmentada debido a la multiplicidad de opciones que nos ofrecen las tecnologías de la Información, lo que a su vez conlleva consecuencias a nivel socio-cultural en una sociedad que se supone debería caracterizarse por la homogeneidad.

Castells define la identidad como el proceso mediante el cual un actor social se reconoce a sí mismo y se construye el significado, en virtud sobre todo de un

atributo o conjunto de atributos culturales determinados, con la exclusión de una referencia más amplia a otras estructuras sociales.

Dentro del contexto de la sociedad de la información, resulta importante ahora más que nunca, la necesidad de rescatar al sujeto en sí mismo, en su personalidad y su cultura, que se ve fragmentada frente al fenómeno de la globalización, que parece integrarnos a todos bajo los mismos parámetros en pro de las transformaciones sociales y al cual se ha dado un nuevo contexto denominado el yo colectivo, construido bajo una mezcla de “espiritualidad, tecnología avanzada, conexiones empresariales y la cultura de la fatalidad milenarista” (2001:50) .

Turkle opina que hace una década se pensaba al ordenador como un segundo yo, una relación de identidad de uno a uno, la persona a solas con la máquina, sin embargo, ahora se trata de un sistema de redes, que es el internet y que se expande con rapidez y que enlaza a millones de personas en nuevos espacios que transforman la manera en que pensamos, la naturaleza de nuestra sexualidad, la forma de nuestras comunidades y nuestras verdaderas identidades. (1997: 17).

Así mismo, Carlos Scolari establece que debido a la visibilidad de los ordenadores o equipos de cómputo mediante su accesibilidad en todos los hogares y oficinas, cambiaron radicalmente la interacción Persona-Ordenador, en la cual el instrumento pasa a ser parte del propio cuerpo, lo que denomina “interfaz” y considera, una especie de prótesis o extensión de nuestro cuerpo (2004:44).

Dentro de las distintas concepciones de lo que se conoce como “interfaz” con relación a la evolución de las tecnologías de la información, Scolari precisa que dicha interfaz “ya no es considerada como un dispositivo hardware, sino un conjunto de procesos, reglas y convenciones que permiten la comunicación entre el hombre y las máquinas digitales” (2004: 44).

Turkle determina que el ordenador no es solamente una herramienta o un espejo, sino que ahora se puede atravesar el espejo y vivir en mundos virtuales

que es lo que se conoce como “cibespacio”, lo que se ha convertido en algo tan rutinario en la vida del ser humano como es el hecho de leer nuestro correo electrónico o la reserva de un boleto de avión en una red informática, creando así mismo comunidades virtuales en donde se interactúa con gente de todo el mundo a la cual incluso se llega a conocer íntimamente sin conocerla físicamente. Lo que conlleva a lo que denomina “La cultura de la simulación”, que afecta nuestras ideas sobre la mente, el cuerpo, el yo y la máquina y en donde el poder de la simulación informática desarrolla un potencial ante la complejidad del mundo real para comprenderlo desde abajo, por lo que dicha simulación permite realizar nuestros sueños de comprender fenómenos complejos sin construirlos desde sus principios primarios, sino a través de la simulación que nos permite jugar con ellos (1997:60).

El debate sobre la unitariedad o multiplicidad del yo, ha visto una avasalladora inclinación hacia la segunda teoría (la de la multiplicidad) que considera un descentramiento del ego, especialmente en el caso de internet como elemento de la cultura informática y en donde las personas son capaces de construir un yo, al merodear por muchos yos, como es el caso de las personas que conocen y se relacionan con alguien más por internet y suelen sentirse más conectados a su identidad, estando frente a la computadora que al tener un encuentro físico con esa persona, ante el temor de no llenar las expectativas de su personalidad (1997: 227).

Así mismo, dicha multiplicidad se agudiza entre los cibernautas al pretender asumir todas las identidades que siempre han deseado, bajo el anonimato que les concede la tecnología del mismo internet, por lo que pueden interactuar con personas alrededor del mundo aparentando una identidad que nada tiene que ver con su realidad e incluso suplantar la identidad de alguien más, especialmente en el caso de personajes públicos, interceptando sus comunicaciones con los demás y formulando declaraciones en su nombre.

Durante los ochenta, las nuevas tecnologías cambiaron, así como los medios de comunicación; los cambios se han hecho palpables en la forma de comunicar desde los periódicos impresos, hasta la radio, la televisión y los aparatos

de video, que se propagaron por todo el mundo revolucionando la industria musical, la capacidad de los aparatos de grabaciones para modificar el sentido único de las imágenes generó una fusión entre la vida real y la pantalla, desarrollando una aptitud ilimitada del individuo para filtrar las imágenes que quiere ver y escuchar.

Al respecto, Jean Francois Lyotard (1979), considera a las computadoras como un factor de control para legitimar los enunciados, a través de la “informatización de la sociedad” provocando la fragmentación de otras formas de validación del conocimiento (Vidal, 2004:88).

En realidad, la validez del conocimiento es secundaria ante la prioridad que la misma sociedad otorga a los medios a través de los cuáles se tiene acceso a dicho conocimiento, es decir, adquiere más trascendencia la velocidad con que se accede a determinado tema que su sustento epistemológico y en este sentido es importante destacar la manera en que la tecnología, de un momento a otro deja de ser innovadora, debido al surgimiento intempestivo de nuevas formas de comunicación, esto es: un día un aparato de telefonía celular resulta una gran novedad, sin embargo seis meses después surge la versión del mismo pero con mucho más funciones que el original, lo que convierte al anterior en algo obsoleto y aburrido, ocasionando un fervor social por adquirir lo más novedoso en avances tecnológicos, a fin de lograr una posición que los identifique con un estatus social elevado, al grado de que el medio de comunicación (sea equipo de cómputo, equipo de telefonía o cualquier medio con acceso a internet) lo defina dentro del contexto social y cultural.

Mark Poster considera que la comunicación efectuada por medios electrónicos genera consecuencias inevitables en las interrelaciones sociales, y que esta clase de comunicación, por las mismas circunstancias en que surgió y se difundió, está en estrecha relación con la mercantilización y el consumismo (Vidal, 2004).

Al respecto, resulta interesante la distinción que hace Cass Sunstein entre los conceptos de ciudadano y consumidor en la era de la información, precisando

que, no obstante que las tecnologías aumentan las posibilidades de elección, ello no implica necesariamente un beneficio para los consumidores, es decir, no por el hecho de adquirir más bienes, significa que mejore su vida, por lo que esas decisiones no agotan la idea de libertad, ya que un gobierno democrático está diseñado para servir a los ciudadanos y no a los consumidores, el ciudadano en cambio pretende una verdadera calidad de vida y ello implica buscar políticas y objetivos diferentes a los del consumidor que consiste en lograr sus “más altas aspiraciones a través de las Instituciones democráticas” (2003: 105-106).

En efecto, nos encontramos ante a una paradoja en la cual, las tecnologías parecen combatir el aislamiento del individuo frente a la sociedad, interconectándolo en tiempo y espacio, sin embargo en realidad se trata de una fragmentación social en donde el radicalismo, basado en un conocimiento deficiente lo puede llevar a perder su identidad.

En efecto, el surgimiento del internet a través de las computadoras, ha generado un profundo cambio en las interrelaciones sociales, sin embargo el contexto social se ha agudizado debido a la aparición en el mercado Internacional de las llamadas “tabletas” y “equipos de telefonía móviles”, que son aparatos minimalistas en cuanto a su tamaño, pero contienen una gran cantidad de funciones que hace dos décadas sería imposible imaginar en cualquier sociedad del mundo, ni siquiera en la más evolucionada tecnológicamente.

Estos equipos portables de manera individual, son una extensión de la persona que los lleva, como lo sostiene Scolari; de tal manera que representan una condición económico-social que define al individuo en su relación con los demás.

De acuerdo a los resultados que arrojaron los Estudios de hábitos y Percepciones de los mexicanos sobre internet y diversas tecnologías asociadas, como parte del *World Internet Project*, se determinó que el número de horas dedicadas a internet ha aumentado de manera notable en el trabajo y en el hogar, mientras que ha disminuido en las escuelas y cibercafés. De hecho el tiempo en cibercafés disminuyó de 2009 al 2011. Así mismo, el número de horas semanales

dedicadas a internet a través de teléfonos inteligentes ha rebasado el total de horas dedicadas a internet desde cibercafés y la escuela. Por lo que se considera que en los próximos años, seguramente se incrementará el tiempo dedicado a internet desde los teléfonos inteligentes (Islas, 2012: 494).

Dentro de las tecnologías de la Información mencionadas con anterioridad, surge el concepto de Geolocalización, el cual resulta relativamente nuevo y constituye una de las más recientes aplicaciones que forman parte de las funciones de la telefonía celular y satelital, este ha sido implementado desde hace aproximadamente dos años a la fecha, y se refiere a la localización geográfica de un dispositivo, ya sea un dispositivo móvil o una computadora conectada a internet que funciona mediante una triangulación que permite identificar la dirección IP, conformada de números, llamados octetos que se refieren al país y tipo de red: se trata de un identificador único en el mundo y es capaz de informar el país, la ciudad y el horario en que se ubica una persona (Ciberseguridad, Gits, Informática; 2003).

En la actualidad los teléfonos móviles son dispositivos anexos prácticamente a la persona; de acuerdo con información de la Comisión Federal de Telecomunicaciones (COFETEL), el 85% de los mexicanos traen consigo un teléfono celular y se mantienen en constante comunicación ya sea por el mismo o por medio de las redes sociales (Facebook y twitter).

Dentro de este sistema de globalización y colectivización informativa a través del intercambio de datos, nos encontramos en un contexto en el cual la identidad puede ser modificada por el avance de las tecnologías de la información.

Así, tenemos siguiendo a Sunstein, que el individuo se encuentra de frente ante esta sociedad red y sociedad de la información, básicamente (como hemos comentado con anterioridad) desde dos perspectivas, la primera como consumidor y parte contratante, frente otros individuos y al gobierno y como ciudadano que ostenta una vida privada, en la cual se coloca en una situación de vulneración al poner en riesgo sus datos personales frente a esa sociedad red en donde fluyen y circulan de una manera descontrolada (2003: 106).

Con base en lo anterior, se hace preciso determinar hasta qué punto se están vulnerando los derechos fundamentales a la vida privada y protección de datos personales, mediante la utilización de los mecanismos legales implementados por los sistemas normativos y qué falta por hacer al respecto.

La cuestión estriba en el hecho de qué tan cautelosos debemos ser para sumarnos a esta sociedad de la información y que tan responsables en el manejo de datos personales, a fin de evitar en la medida de lo posible ser víctimas de la misma o como se cuestiona Sunstein, “si las prácticas sociales que están surgiendo, entre las que se incluyen los modelos de consumo, fomentan o bien comprometen nuestras más altas aspiraciones” (2003:105).

1.3 EL PAPEL DEL ESTADO Y SUS INSTITUCIONES FRENTE A LOS DESARROLLOS TECNOLÓGICOS Y SU IMPLEMENTACIÓN COMO MECANISMO DE CONTROL EN EL EJERCICIO DEL PODER

1.3.1 EL ESTADO ACTUAL.

“El Estado como construcción histórica se encuentra en medio de la problemática de la transformación social. Finalmente es el Estado quien a través de las leyes, políticas, programas y actividades establece los marcos normativos y orientadores del quehacer de las sociedades” (Araya, 2005).

Como sostiene Eduardo Araya, durante la segunda mitad del siglo XX el proceso de transformación del Estado ha presentado dos etapas, aquella de la década de los setenta y ochenta, que se puede resumir en la idea de la retirada del Estado mediante la desregulación de importantes áreas de la economía y la devolución de importantes ámbitos de acción a los particulares, y por otro lado la etapa que surge a partir de la declaración del Banco Mundial, en el año de 1997, en donde se revitalizó la presencia del Estado como factor clave para el desarrollo de las naciones; en su desenvolvimiento durante el siglo XX aparece como

promotor de la ciencia y tecnología en los diferentes ámbitos, como son, la medicina, la cuestión empresarial y la carrera espacial. (Araya, 2005).

El ingreso de los distintos Estados en el mundo hacia la sociedad de la información, ha sido paulatino, a la cabeza se encuentran los países europeos, cuyos tratados Internacionales han marcado la pauta para que los países latinoamericanos se incorporen a las políticas implementadas, de acuerdo al grado de resistencia o apertura de los gobiernos, ante los cambios tecnológicos que pudieran representar una amenaza contra sus intereses.

Sin embargo, frente al contexto actual del desarrollo de las tecnologías de la información, el Estado adquiere una connotación distinta, ya que parte de una base de igualdad que le permite a los distintos sectores sociales el acceso a dichas tecnologías. Se requiere un nuevo Estado, ya no como monopolizador de la información, como lo ha sido en otras épocas, sino como ente regulador que busca el equilibrio y acceso igualitario de todos los sectores en el aprovechamiento de la información, de tal manera que en esa integración queden plenamente satisfechos todos los derechos inherentes a la persona como elemento constitutivo de una verdadera democracia frente a un poder público equilibrado en el manejo de dicha información.

El papel del Estado se ve transformado frente a la obligación de proporcionar el acceso a la sociedad civil de manera equitativa, lo cual conlleva hacia problemas más complejos.

Los cambios que conlleva la sociedad de la Información y para los cuales debemos estar preparados, no implican simplemente la modernización, mejora y facilidad de acceso a la Administración pública. Significa instauración de nuevos servicios, nuevas formas de actividad empresarial, de relaciones sociales.... Medidas legislativas que protejan la seguridad del cambio de datos... (Campuzano, 2000: 34).

La Cumbre Mundial de la Sociedad de la Información, llevada a cabo en dos fases, la primera en Ginebra, Suiza en 2003, la segunda en Túnez en 2005,

determinó dentro de la primera, su declaración de Principios “Construir la Sociedad de la Información: un desafío Global para el nuevo milenio” en los cuales reconoce el gran desafío que representa la desigualdad, entre quienes tienen acceso a las tecnologías de la Información y aquellos que no tienen esa posibilidad, estableciendo entre muchos otros, como uno de sus compromisos “La abstención de los Estados de adoptar medidas que vayan en contra del bienestar de los ciudadanos” (Ponce, 2005:50).

No obstante los intentos de los gobiernos por cubrir las necesidades que implican los cambios tecnológicos de la sociedad, el rezago se va profundizando a medida que surgen innovaciones en las formas de comunicación, que si, en un principio se basaban en un equipo de cómputo, ahora se extienden hacia las formas más depuradas como son las tabletas y los mini-equipos de telefonía celular, con lo cual el individuo tiene un acercamiento físico más directo con el resto de la sociedad, lo que fortalece la desproporción política y legislativa de los sistemas estatales que permanecen rezagados ante la innovadora tecnología que día a día se desarrolla.

“En poco más de una generación, la tecnología para la transferencia de información, se ha vuelto sencillamente demasiado grande y demasiado dinámica para reglamentarla con rigor” (Roszak, 2005: 211).

Por otro lado, la expectativa que existió con el surgimiento del internet y las nuevas tecnologías como instrumentos de fomento para la democracia, ha desaparecido poco a poco, debido a la falta de interactividad entre el gobierno y el gobernado mediante los derechos a solicitar información de éstos últimos, a emitir opiniones respecto de la misma y a pedir respuestas personalizadas a sus representantes; lo que se traduciría en una especie de examinación hacia el gobierno, derecho indispensable para la configuración de la democracia, en cambio el gobierno, ha adquirido una postura unilateral al informar al individuo, coartando la información y obstaculizando el derecho de réplica respecto de la misma. “Los gobiernos a todos los niveles, utilizan el internet, principalmente como tablón de

anuncios electrónicos para publicar su información, sin realizar un verdadero esfuerzo de interacción real” (Castells,2001:176).

La forma de comunicación con el Gobierno se basa en la política de medios de comunicación o, como les llamaría Sunstein, los intermediarios del interés general quienes funcionan en base a una política mediática personalizada, organizada en torno a la imagen de los candidatos a elecciones.

El estado en la sociedad de la información y el conocimiento debiera centrarse en su papel de cohesionador e integrador de la sociedad, entregando las bases para la reducción y control de los naturales conflictos de la sociedad, particularmente en un mundo turbulento y globalizado, lo que supone regular lo necesario e intervenir en la medida de lo social y políticamente pertinente, para asegurar gobernabilidad (Araya; 2005).

Esa gobernabilidad se logra mediante la eficiencia en su desempeño como respuesta a las demandas de la sociedad de la información por medio de una interacción con la sociedad, como lo propone el *e-gobierno* (gobierno abierto), a fin de lograr el tan anhelado en todas la épocas históricas: bienestar de la colectividad.

Con el desarrollo de las tecnologías de la información, en especial el internet, ha surgido una nueva forma de gobernabilidad distinta a los modelos clásicos.

La gobernanza de internet es uno de los temas más polémicos, que ha estado en el centro del debate entre los asociados estadounidenses y los organismos internacionales, en las Cumbres Mundiales de la Sociedad de la Información (CMSI) y en el Foro para la Gobernanza en internet (FGI), con el fin de acordar una regulación administrativa, financiera y Jurídica Internacional de la red (Amador, 2012:295).

No obstante lo anterior, Byung Chul Han, en su texto *Psicopolítica*, describe de qué manera funciona la nueva tendencia del régimen neoliberal basado en la teoría de la autoexplotación del hombre como “empresario de sí mismo”, abandonando la ideología marxista sustentada en la explotación de clases, ello en

virtud a la desaparición de clases que impera en el panorama neoliberal actual (Chul-Han,2014:25).

El autor rebasa la teoría de Foucault que sostiene el método disciplinario como instrumento de poder (Normativo y prohibitivo), al considerar la sociedad actual como una sociedad que voluntariamente se somete a la dominación, en respuesta a la condescendencia del Estado, lo que le permite una libertad aparente, se trata de un poder silencioso e invisible que tiene como objeto de producción a la información y a los programas; sin embargo el nuevo sistema neoliberal no se fundamenta en libertad individual sino en la libertad del capital:

La técnica del poder del régimen neoliberal adopta una forma sutil. No se apodera directamente del individuo. Por el contrario se ocupa de que el individuo actúe de tal modo que reproduzca por sí mismo el entramado de dominación que es interpretado por él como libertad (Chul-Han, 2014: p.25).

1.3.2 ESTADO Y PODER

Held se cuestiona sobre la transformación de elementos tales como la territorialidad, el control monopólico de la fuerza y la violencia, una estructura impersonal de poder y la propia legitimidad del Estado (Held, 2001:45).

La esencia económica del poder del Estado frente a la sociedad de la Información no se distingue en gran medida de los movimientos socioculturales y tecnológicos que se han gestado en otras épocas, como es el caso de la revolución Industrial; Por lo que siempre ha existido el motor económico como impulsor del desarrollo de nuevas tecnologías, Tal y como lo llegó a considerar Foucault;

Si la gubernamentalidad del Estado se interesa, y por primera vez en la materialidad fina de la existencia y la coexistencia humana, en la materialidad fina del intercambio y de la circulación y toma por primera vez en cuenta ese ser y ese mayor bienestar y lo hace a través de la ciudad y los problemas como la salud, las calles, los mercados, los granos, los caminos, es porque en ese momento el comercio se concibe como el instrumento principal del poder del Estado".(Foucault; 2006:16).

En efecto, el Estado se ha desvinculado de sus responsabilidades de bienestar hacia la población en el contexto del desarrollo de las tecnologías de la Información, en virtud de una preponderancia de carácter económico; olvidando así el fin primordial de la sociedad de la Información, que es el conocimiento aplicado al bien común.

El Desarrollo de las tecnologías se ha vinculado solo a la dimensión económica, y por lo tanto no tiene otra consideración que la utilidad y la ganancia. El desarrollo tecnológico no ha ido acompañado de los cambios sociales que permitan un mínimo de control del proceso. Este control fue ejercido durante mucho tiempo por la política en el ámbito del poder del Estado; sin embargo el avance científico y tecnológico, ha sobrepasado hoy los límites del control político y del estado mismo, siendo abandonado a su propia lógica de acción, bajo los parámetros de la ganancia económica (Gainza,2003:124).

Desde el surgimiento de las tecnologías de la información, el Estado se ha servido de las mismas como parte de sus estrategias políticas; en los Estados Unidos, el llamado Proyecto Cambridge creado por el Departamento de Defensa con la finalidad de llevar a cabo investigaciones en el campo de las Ciencias Sociales, a través de un informe en el año de 1971 determinó:

Con estas técnicas, se podría considerar en unos pocos días las estrategias posibles para una invasión a Cuba o Vietnam del Norte. Probablemente más tarde, pero todavía en el futuro previsible, tales técnicas podrían emplearse para decidir la conveniencia para intervenir o no en unas elecciones en el extranjero (Roszak, 2005: 229).

A lo anterior hay que agregar:

“El poder es la capacidad relacional que permite a un actor social influir de forma asimétrica en las decisiones de otros actores sociales de modo que favorezcan la voluntad, los intereses y los valores del actor que tiene el poder”. (Castells;2009:33).

Dentro del contexto de la Sociedad de la Información, la concepción clásica del poder, así como sus fuentes, se han modificado debido al fenómeno de la globalización debido a cambios de autoridades que trascienden de lo nacional hacia una pretendida armonización con intereses supranacionales.

A lo largo de la historia, el poder del Estado se manifiesta a través de su capacidad de control sobre la información como parte de la política, sin embargo como menciona Cruz Díaz de Terán, la *transfronterización* de la Información en la actualidad, impide el control absoluto por parte del Estado.

Hablar de sociedad red, es hablar de globalización, la sociedad se sitúa frente a un nuevo contexto que genera nuevas concepciones de los términos hogar, familia, clase, democracia, dominación, Estado, economía política entre otros. En el caso del Estado, el poder trasciende las fronteras nacionales para dar paso a una nueva concepción del mismo, ello no implica su desaparición, sino de una nueva forma de organización social, con una reestructuración y evolución diferente.

La circulación de información tiene pues naturaleza transfronteriza, por tanto, un gobierno jamás podrá hacerse con el control absoluto por sí mismo, solo tiene dos alternativas, o cierra completamente el acceso a la red, o cuenta con los demás Estados y negocia con ellos un control más o menos compartido. Esta podría denominarse la visión fiscalizadora de internet, y a ella se suman la mayoría de los gobiernos totalitarios y casi la totalidad de los democráticos (Díaz de Terán, 2007:95-120).

La participación del Estado en la Sociedad de la Información ha sido determinante mediante la apertura de las Tecnologías de la Información hacia la sociedad en general, considerando que dichas tecnologías, todavía hace unas décadas estaban reservadas para fines militares e institucionales. Sin embargo esa apertura no es absoluta, en principio, debido a lo que se conoce como brecha digital, entendida por el “trecho que existe entre aquellos individuos que tienen

acceso a las nuevas tecnologías y los que no”(Ponce; 2011: 48); y que parte de la desigualdad económica entre los Estados tomando como base los desarrollos tecnológicos que les permite tener más o menos acceso a dichas tecnologías y, por consiguiente, a sus ciudadanos, quienes son blanco dentro de los mismos países, de la misma inequidad, al no tener acceso a dichas tecnologías y por consiguiente vivir marginados en la sociedad de la información, como es el caso de los migrantes, los indígenas o las personas de escasos recursos económicos.

El poder que históricamente había pertenecido al Estado de una manera más absoluta e ilimitada, en la actualidad se frena en un principio en la sociedad red, a partir de la dominación que parte de la lógica “inclusión-exclusión” en las redes globales a la que se refiere Castells, en el sentido de imponer, la cual depende la capacidad de desarrollo de redes de una sociedad a otra, excluyendo a aquellos territorios, actividades o personas que poseen muy poco valor para llevar a cabo tareas relacionadas con la red (Castells, 2009: 52).

“Nos encontramos entonces frente a una nueva forma de poder distinta a la tradicional, nuevas formas de dominación propias de la sociedad red, si bien con nuevas formas y nuevos actores, las formas más cruciales de poder siguen la lógica del poder para crear redes” (Castells, 2009:76).

El Estado actual se enfrenta a una nueva sociedad intercomunicada y globalizada por lo que se ve en la necesidad de una transformación que tiene como sede asociaciones y redes de estados, en los cuales aparece una soberanía compartida, como es el caso de la Unión Europea, u otras con fines comerciales como el Mercosur, o bien con fines de seguridad como lo es la OTAN, en todos los casos se trata de organizaciones que pretenden definir estrategias para administrar el mundo de acuerdo a los intereses de los países que participan en los mismos.

Otra forma de transformación del Estado en la sociedad red o de la información, es a través de la creación de Instituciones internacionales para la resolución de problemáticas específicas, como es el caso del Banco Mundial, el

Tribunal Internacional de Justicia, la Organización de las Naciones Unidas, entre muchos otros.

Sin embargo, no obstante que el desarrollo que las tecnologías de la información ha permitido que el individuo aumente su capacidad de opinión pública y de participación ciudadana en la interacción con el gobierno debido al acceso a mayor información, como nos menciona Roszak, el gobierno es el cliente más rico y mejor dispuesto de la Industria de la Información, toda vez que sigue siendo el que retiene mayor número de datos (Sanidad, Educación y Asistencia Social, Comercio, Defensa, Administración Fiscal y Seguridad Social), tiene entre todos estos datos, de dos mil a cuatro mil millones de fichas coincidentes en parte sobre el público norteamericano. Por lo que establece que llevar fichas no es ninguna novedad para los gobiernos del mundo moderno; pero la escala en que el estado actual documenta las vidas de sus ciudadanos no tiene precedentes (2005: 171).

Siguiendo a Chul-Han, (2014: p.14), nos dirigimos como sociedad hacia una “psicopolítica digital”, que avanza desde una vigilancia pasiva hacia un control activo, la libertad está en crisis, ya que nosotros mismos somos quienes la determinamos, ofreciendo toda información a los demás de manera indiscriminada.

“La psicopolítica digital transforma la negatividad de la decisión libre en la positividad de un estado de cosas” (2014: p.14) y para esto se utiliza la herramienta del *Big Data* el cual según el autor, positiviza a la persona en cosa, la cosa es más transparente que la persona, lo que deviene en la desaparición de la persona y de la voluntad libre.

La psicopolítica se verifica a través de un ejercicio de poder que reviste características muy peculiares respecto de las forma tradicionales basadas en la violencia e imposición de preceptos legales y prohibiciones; se trata de un poder inteligente, silencioso e invisible que no busca la sumisión del hombre ante el mismo, sino la dependencia, y lo lleva a cabo de acuerdo al autor, por medio de la complacencia, es decir haciendo valer la voluntad de los sujetos sometidos.

Bajo el contexto de la sociedad de la información, el Estado actual se reinventa frente a un mundo globalizado en donde existe una mayor presión, a través de las políticas y acuerdos Internacionales por el respeto de los derechos humanos, lo que representa el contrapoder del mismo, se trata de una sociedad aparentemente proactiva, que juega a poner en tela de juicio las funciones Institucionales, pero que en realidad se enfrenta a un ente que parece no abandonar la antigua formulación de la política que dio origen a las tecnologías de la información durante la Segunda Guerra Mundial y que consiste en la autoprotección para su subsistencia, la de la dominación y el control.

Los conceptos de Individuo y Estado se han visto notablemente transformados a partir de la profunda transición de la Sociedad de la Información, debido al desarrollo de las tecnologías; el Big Data constituye la herramienta más importante para almacenar el perfil completo de un individuo, y lo más preocupante, es que voluntariamente alimentamos esas bases de datos.

La observancia y respeto de los derechos humanos, parece cumplida, cuando el Estado genera esa sensación de libertad y permisión que hace sentir al sujeto como parte de éste nuevo modelo de Sociedad, estos cambios se perciben de manera directa en las relaciones culturales, sociales, políticas y económicas entre ambas partes, lo que impide cualquier reacción en contra de los gobiernos, diluyendo poco a poco la capacidad de manifestación de una sociedad rebasada por las tecnologías.

Las concepciones clásicas, que el derecho positivo ha desarrollado respecto a la relación Individuo y Estado, bajo la idea de control del segundo sobre el primero, no han sido superadas en realidad, no obstante una participación más activa de la sociedad en los asuntos que anteriormente estaban reservados para el Estado.

Los nuevos sistemas liberales permiten al Estado transformarse ante las dudas sobre su legitimidad aprovechando los recursos tecnológicos, como es el *Big Data*, buscando nuevos mecanismos de recuperación del control en el ejercicio del

poder, mediante la implementación de legislaciones que estén en sintonía con las exigencias Internacionales de una política globalizante que le permita pretender que se encuentra a la altura de las principales potencias del mundo.

CAPITULO II

LA SEGURIDAD NACIONAL Y LA PROCURACIÓN DE JUSTICIA EN MÉXICO EN EL CONTEXTO DE LA SOCIEDAD DE LA INFORMACIÓN

2.1 LAS FUNCIONES ADMINISTRATIVAS DEL ESTADO

El desarrollo de la Sociedad de la Información ha seguido su ruta en la búsqueda de lograr una economía del conocimiento competitiva y dinámica, los países se han incorporado paulatinamente a lo largo de las últimas décadas al modelo, algunos con mayor velocidad que otros dependiendo el contexto político, social y económico que los define. Sin embargo, la cuestión de la regulación, ha observado notables transformaciones bajo el panorama del ciberespacio, en donde el papel del Estado, como lo hemos explicado en el capítulo anterior, se redefine en orden de satisfacer una mayor cantidad de potestades y obligaciones de una forma más activa las cuales son dirigidas a su finalidad natural, que es el bien común.

Así es como al aumentar los objetivos del Estado surge la necesidad de ampliar sus funciones, las cuales tendrán verificación a través de la administración pública. Es por medio del aparato administrativo como adquieren relevancia las políticas articuladas en la Constitución. La administración pública se proyecta en la realidad como una función del Estado, ya que este al ser una entidad abstracta y global, no puede materializar su voluntad por sí mismo, sino a través de sus órganos (Huerta, 2005:124).

Huerta se refiere a la principal función estatal, basada en la idea que sustentó al Estado absolutista, la de policía, entendida en el sentido de la vigilancia y garantía de seguridad y orden social, sin embargo a la vez pretende limitar el poder mediante principios generales y reglas, que conllevan al bienestar de los súbditos, Sin embargo este modelo se ve rebasado a partir de la Revolución Francesa por el Estado garante de los derechos humanos a través de un deber de abstención, de no intervención en las relaciones privadas (p.127-128).

Toda Constitución prevé un modelo a realizar, el cual consagra los principios y valores que constituyen las premisas de actuación del estado y la sociedad a quien regula... generalmente los modelos se construyen tomando en consideración los intereses preponderantes para una sociedad en un momento específico (Huerta,2005:126).

Así, tenemos que el Estado se va transformando a través de la historia, de vigilante a garante de derechos humanos, para dar paso a otros modelos como es el liberal caracterizado por una actitud “intervencionista”, En opinión de Huerta “no tiene una connotación exclusivamente negativa, la participación pública o su intromisión en sectores de actividad privada puede tener un fin social, me refiero en el caso en que el estado presta o asegura un servicio” (p:127).

La actividad administrativa, se contempla como una “triada”, policía, servicio público y fomento. Las medidas policiales se caracterizan por la posibilidad de la utilización de la coacción y se justifican en la necesidad de mantener el orden público (Huerta, 2005:139).

Debido al surgimiento de las nuevas tecnologías de la información, concretamente el internet, actualmente emergen nuevas formas de regulación distintas a las tradicionales, que se limitaban a la regulación estatal.

La regulación de internet, en general de las redes, implica la intervención ya sea administrativa o autorregulada, esto es, de la administración o de organismos privados, tanto sobre el territorio de internet (el ciberespacio) como sobre sus usuarios (cibernautas), ya estén estos sometidos a normas jurídico-públicas (administrados) o a normas técnicas (autorregulados), (Moles,2004:92).

La intervención administrativa, siguiendo a Huerta, debe tener tres principios básicos: El de igualdad, que debe entenderse ante todo como igualdad de trato, la ausencia de discriminación o de concesión de privilegios arbitrarios, la discrecionalidad y la libertad de apreciación que conserva la administración pública y le permite elaborar balances de la conveniencia de un ejercicio de un derecho o de una limitación, pero de ninguna manera como un poder arbitrario; El segundo principio a que se refiere la autora, es el de proporcionalidad y congruencia de la intervención, con los objetivos que la justifican, lo que se traduce en una ponderación entre la carga impuesta y el fin perseguido; y por último nos remite al principio de libertad individual, como un deber que emana del ordenamiento jurídico mismo y al que tendrá que ajustarse la actividad administrativa (Huerta, 2005:143).

2.2 LA INTERVENCIÓN ADMINISTRATIVA ESTATAL COMO FORMA DE REGULACIÓN EN EL CIBERESPACIO

Las funciones del Estado en el ciberespacio han generado un nuevo comportamiento en el desarrollo de las mismas, ante una red global que lo obliga a participar en una cooperación internacional con otros Estados respecto a temas como el de la seguridad.

Castells nos explica los intentos de los Estados por recuperar el control en la seguridad de la información que la globalización cibernética ha puesto en situación de vulnerabilidad y nos explica:

Como internet y las redes informáticas en general, han interconectado al país entero, al mundo entero en realidad, las vías de penetración a los sistemas de seguridad son prácticamente ilimitadas. Pero existe un antídoto muy poderoso que podría contribuir a reforzar la inseguridad en todo el sistema: la difusión de tecnología de encriptación avanzada entre las organizaciones y la gente en general. Sin embargo los gobiernos están obstaculizando la difusión de la tecnología de la encriptación, con la excusa de que ello contribuiría a reforzar las actividades criminales (Castells, 2001:182).

No obstante, el autor considera que este sabotaje por parte del Estado, a fin de evitar la difusión del fenómeno de la encriptación se revierte y finalmente deja al propio Estado y a la sociedad indefensos ante los ataques en la periferia de la red.

2.3 LA INTERVENCION ADMINISTRATIVA A NIVEL SUPRAESTATAL

Aunado a las formas de intervención estatal, consistentes en la autorregulación relacionada concretamente con el ciberespacio o la estatal propiamente dicha, existe la intervención supraestatal, a las que alude Moles, como aquellos niveles de intervención más allá del Estado, y que son dirigidos básicamente a sectores vinculados con tareas de información, interceptación de comunicaciones y operaciones de espionaje (Moles. 2004:147).

La intervención administrativa en el ciberespacio puede materializarse tanto, a través de medidas de autorregulación o bien de una estructura Estatal, sin embargo dicha intervención puede provenir de esferas más allá de lo estatal por medio de actividades de interceptación de comunicaciones y espionaje, en el caso de la Unión europea se cuenta con un exitoso instrumento de investigación policial denominado Sistema de Información de *Schengen*, estructurado con base a los denominados “Acuerdos de *Schengen*” (Luxemburgo) y a través de los cuales Alemania, Francia y los Estados del Benelux establecen una mayor colaboración en materia policial.

Este acuerdo originado en 1985, ratificado en 1990 e integrado a las directrices del Tratado de Amsterdam de 1997, fue firmado por los ministros de exteriores de la Unión Europea, siendo sustituido el comité ejecutivo de Schengen por el Consejo de Justicia Interior.

A partir de los años noventa, surgieron toda una serie de propuestas a fin de crear sistemas de registro y vigilancia en Europa, una de las organizaciones que

más influencia ha tenido a nivel mundial, es la llamada ILETS, creada en 1993 y cuyas siglas significan en español Seminario Internacional de Telecomunicaciones de los Cuerpos de Seguridad de Estado, la cual está respaldada por la Agencia de Seguridad Nacional (NSA), “el objetivo de estas dos agencias es, en esencia extender, las medidas aprobadas en los EEUU al resto de los países del mundo” (Mostazo, 2002:s/p).

En el año de 1994, el parlamento holandés propuso que Europa adoptara el documento llamado ENFOPOL que consiste en una clasificación estándar de la Unión Europea para documentos relacionados con asuntos de policía y mantenimiento de la ley y el cual “significaría que los fabricantes de nuevos sistemas de intercambio o de comunicaciones tendrían que incorporar interfaces de interceptación para poder cumplir con las normas internacionales” (Moles, 2004:151).

En el año de 1998 en Roma, ENFOPOL se adapta a las nuevas tecnologías y se establecen por parte de los expertos bosquejos que definen los requisitos para interceptar internet.

El debate llevado a cabo en el parlamento Europeo en septiembre de 1998, reveló planes conjuntos de la UE y el FBI para cooperar en la construcción de un sistema de vigilancia global para las telecomunicaciones, aunque se negó a los europarlamentarios el acceso a los documentos relacionados. Los planes de intervención se dirigen hacia cualquier tipo de telecomunicación datos cifrados o en forma de texto llano, telefonía móvil, el nuevo sistema *Iridum* y otros servicios de telefonía móvil por satélite que puedan aparecer), (Moles, 2004:153).

La Intervención estatal se manifiesta a través de la administración pública y ésta a su vez, se materializa por medio de las políticas públicas, en el caso que nos ocupa, la conforman las política de seguridad Nacional, Sin embargo, cabe cuestionarnos qué es la seguridad nacional y cuál es su sustento legal en México.

2.4 EL TEMA DE LA SEGURIDAD NACIONAL CONCEPTO Y DEFINICION

El tema de la seguridad nacional resulta muy ambiguo en atención a la interpretación jurídico-filosófica tan diversa que se le ha otorgado en los distintos lugares y épocas, por lo que ha sufrido grandes transformaciones en atención a los fenómenos sociales del último siglo; la definición tradicional limitada a una protección frente a todo elemento exterior de una nación, queda rebasada por fenómenos que han transformado la vida interna de un país:

Tras el fin de la guerra fría y como consecuencia de la globalización, las amenazas dejan de poseer un carácter puramente militar, ampliándose el concepto de seguridad. Problemas globales, transfronterizos en su mayoría, tales como el crimen organizado, el terrorismo, la degradación del medio ambiente, la disputa por los recursos naturales, los flujos incontrolados de refugiados, la inmigración no regulada, la pobreza y el hambre se han convertido en riesgos para la humanidad de una importancia similar a la de la tradicional defensa militar. Por ello es preciso ampliar el concepto de seguridad en materia multisectorial y a distintos niveles, y considerar que la territorialidad y la defensa militar no deben ostentar la predominancia. Además, en el último lustro y bajo la repercusión de la actual crisis económica global, el entorno internacional, cada vez más complejo, vendría a señalar que los retos a la seguridad de hoy, no pueden ser divididos entre aquellos de carácter “interno o externo” y entre “civiles y militares” (Iglesias,2011:2).

La seguridad nacional constituye el elemento indispensable para que el Estado obtenga una forma de asegurar el poder como medio de subsistencia; no obstante lo anterior hay un fuerte cuestionamiento en la actualidad sobre la justificación de la validez de los medios que utiliza el Estado mismo para hacerla valer.

Las bases teóricas de la seguridad nacional son a tal grado ambiguas, que su definición misma no merece consenso, ni siquiera entre quienes reconocen la validez del concepto, se cuentan por decenas las definiciones dadas a conocer. Un supuesto valor de organización del Estado, atributo asignado a la seguridad nacional entre sus voceros, que no alcanza consenso en cuanto a su objeto, fines e instrumentos, necesariamente arroja dudas sobre su justificación misma (López, 1998:1).

Existen dos factores importantes que debemos destacar al tratar de arribar al concepto de seguridad nacional, el primero es su asociación con el tema de la represión y el segundo, el relativo a la hegemonía (mencionada páginas atrás) ejercida por Estados Unidos, al tratar de imponer sus políticas frente a un mundo globalizado, sin embargo, en opinión de algunos autores como Carmen Martí, debería utilizarse una definición específica para cada país, en la que prevalezca la claridad y precisión (Martí, 2006:219-245).

Un nuevo concepto de seguridad nacional, supondría formular nuevos fundamentos para que sea socialmente aceptado, políticamente correcto y culturalmente unificador. Es decir, conseguir que la idea deje de asociarse de manera automática a una concepción represiva para que sea susceptible de convertirse en un parteaguas que defina los intereses nacionales con independencia de la ideología profesada (Curzio, 2007: 81).

No obstante lo anterior, el concepto de seguridad nacional ha tenido una fuerte carga ideológica a partir de los intereses de Estados Unidos, antes y después de la guerra fría mediante la imposición de políticas que atienden a un llamado de protección respecto a ataques ideológicos y políticos, previo a dicha etapa del comunismo y después del terrorismo, al respecto, siguiendo a Curzio:

El concepto de seguridad Nacional, todavía resulta polémico en México. Las connotaciones políticas e ideológicas, que se han ido sedimentando en él, no facilitan un debate constructivo en un momento en el que por lo menos cuatro factores concurren para hacer un planteamiento general: 1) El fin de la guerra fría, 2) La transición política hacia la democracia, 3) La relativización del concepto de soberanía en un mundo globalizado y 4) la Crisis generada por el terrorismo internacional (Curzio,2007:81).

Al finalizar la segunda Guerra Mundial, y bajo la “amenaza” de la Unión Soviética como principal enemigo del mundo, acorde a la propaganda anticomunista de los norteamericanos, el término de seguridad nacional adquirió una relevancia como elemento indispensable de las nuevas políticas liberales;

La nueva posición norteamericana como superpotencia, su hegemonía compartida con (y amenazada por) la Unión Soviética, hizo emerger un orden internacional que basculaba sobre dos gigantes “Estados de seguridad nacional”; la lógica de la bipolaridad se tradujo en las correspondientes alianzas militares y fuera del bloqueo soviético, se reconstruyó el orden económico internacional bajo la tutela de organizaciones auspiciadas por Estados Unidos (Gilmore, 1977: 105).

En efecto, el concepto de seguridad nacional ha sufrido distintas percepciones de acuerdo a los diversos contextos internacionales que han prevalecido en las diferentes épocas, alejados de todo realismo y raciocinio, obedeciendo a toda una serie de intereses políticos y económicos dictaminados por las políticas imperialistas de los Estados Unidos, que durante la invasión a Vietnam, en su momento la invocaron como justificación, sin embargo al término de la guerra, se transforma el término en obediencia a la crisis del acceso a los recursos energéticos como un componente indispensable para la seguridad nacional.

La concepción actual de Seguridad Nacional del imperialismo norteamericano no concibe a los presentes procesos sociales y políticos del área de Latinoamérica como amenazas o peligros de seguridad, o de seguridad continental, solo destaca algunos problemas como el narcotráfico y el terrorismo para ciertos países, así como la necesidad de una política de recuperación económica de corte neoliberal. La región es vista casi como un área pacífica (más bien pacificada) visión que encuentra mayor sustento ante la desaparición del bloque socialista, enemigo externo, y de fuerzas nacionalistas y democráticas latinoamericanas, el enemigo interno (Piñeyro, 1994:s/p).

Actualmente podemos hablar de dos concepciones del término seguridad nacional, la tradicional y la que podríamos considerar contemporánea:

Es posible distinguir entre las definiciones tradicionales de seguridad nacional que tienden a focalizarse entre las capacidades materiales y en el uso y control de la fuerza militar por los estados y las concepciones recientes que aluden a amenazas militares, políticas, económicas, sociales o ambientales que afectan no solo a los estados sino a los grupos de individuos. En estas últimas en la noción

de amenaza lo que constituye el aspecto central y conduce al Estado a dar forma a una agenda de seguridad nacional que rebasa por mucho las cuestiones meramente militares, para incorporar los peligros para la economía, el medio ambiente, los recursos naturales, políticos y culturales (Martí, 2006: 219-245).

Al elemento de “la amenaza”, como distintivo y permanente del término de seguridad nacional, se incorporan nuevos aspectos que alejan al concepto cada vez más de la verdadera naturaleza de seguridad, la cual debería tener un sustento democratizador y concordar con el proyecto de seguridad de cualquier nación.

Curzio considera que los elementos mencionados como son: la hegemonía de los Estados Unidos para dirigir los destinos de la seguridad nacional en Latinoamérica, así como el elemento represivo que ha caracterizado al concepto, han deteriorado la verdadera naturaleza y esencia del término en cuestión.

Al respecto, Laborie Iglesias nos menciona el debate que divide el tema de la seguridad nacional entre los partidarios del uso del “*soft power*” “poder blando” y los del “*hard power*”, concepto acuñado por Joseph Nye en su libro: *Bound the lead: The Changing Nature of American power*, (1990); y en el cual, estos últimos (hard power) consideran que únicamente las medidas coercitivas de diversa índole, junto a unas fuerzas armadas y capaces, constituyen la forma de garantizar la seguridad.

Por otra parte los defensores del llamado “poder blando” y con la Unión Europea a la cabeza, piensan que es preciso utilizar predominantemente elementos de naturaleza persuasiva, para alcanzar los objetivos políticos vinculantes; así mismo el autor refiere a otros puntos de vista que combinan están dos tendencias, “aparentemente antagónicas”, se trata del uso de elementos tanto económicos como diplomáticos, en donde el uso de la fuerza militar, lejos de ser descartado, constituye una herramienta en ocasiones imprescindible, “se hacen patentes las denominadas tres “D” de la seguridad: Defensa, Diplomacia y Desarrollo” (Iglesias, 2011:4).

En el caso concreto de México, el concepto se ha desprestigiado cada vez más con el paso del tiempo, al grado de que en la actualidad se le identifica con la protección al régimen político que prevalece en determinado tiempo y lugar.

El último elemento que deforma la esencia de una idea de seguridad nacional que refleje las aspiraciones de todos los mexicanos, es producto de las perversiones que el concepto ha sufrido en la historia reciente del país. La idea de seguridad nacional, como hemos visto, se asimiló con facilidad con una idea de seguridad del Estado y, por las características del sistema político mexicano, se convirtió en seguridad del régimen que a su vez, suponía la seguridad de un partido político y de los grupos y personas que dominaban en un momento determinado. La idea de seguridad nacional se equiparó en la opinión pública con la seguridad de un grupo político. Como han señalado algunos analistas (Curzio, 2007: 82).

López Ernesto López Portillo, realiza un análisis interesante respecto a la vaguedad del término seguridad nacional en la normatividad mexicana, partiendo del objeto de protección del derecho, es decir del llamado bien jurídico tutelado consagrado en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, que a letra dice: “nadie puede ser privado de la vida, de la libertad o de sus propiedades, posesiones o derechos, sino como la propia constitución prescribe”.

Cuando se busca, en cambio, el bien o interés jurídico tutelado por la seguridad nacional es una vasta serie de conceptos que conjugan y sobreponen principios políticos y jurídicos, lo cual arroja como resultado una fórmula que al incluirlo todo, evade la precisión de su significado y alcances (López, 1998:2).

López Portillo se refiere como ejemplo de lo anterior al Plan Nacional de Desarrollo 2001-2006 el cual invocaba las “verdaderas amenazas” a las instituciones, la desigualdad, la vulnerabilidad de la población frente a los desastres naturales, la destrucción ambiental, el crimen, la delincuencia organizada y el tráfico ilícito de drogas, de lo cual deduce que en interés tutelado se proyecta hacia cualquier política pública; lo anterior coincide con la agenda de inteligencia para la

seguridad nacional establecida por el Centro de Investigación y Seguridad Nacional (CISEN) de la Secretaría de Gobernación y que involucra los temas de narcotráfico; Grupos subversivos y organizaciones afines; Crimen Organizado; Inseguridad Pública; Corrupción; Terrorismo Internacional; Proliferación Armamentista; Ingovernabilidad; Estabilidad Económica; Desigualdad Social; Inestabilidad Regional; Demografía; Energía; Ecología; Salud; Desarrollo equilibrado; Alimentación; Educación y Recursos naturales.

Siguiendo a López Portillo, se aprecia, ante esta lista ilimitada de conceptos, una temática ilimitada de amenazas hacia las Instituciones de Gobierno que permea una ambigüedad respecto al riesgo que atenta contra la Seguridad Nacional y que en consecuencia, genera una ausencia de precisión para determinar el bien jurídico protegido por la misma (López, 1998:4).

2.4.1 LOS SERVICIOS DE INTELIGENCIA EN MEXICO Y LA CRISIS DE LA SEGURIDAD NACIONAL

Después de la desaparición de la Dirección Federal de Seguridad DFS y de Investigaciones Políticas y Sociales, se crea en el año de 1985 el DISEN, Dirección de Investigación y Seguridad Nacional, que en el año de 1989 bajo el contexto de la llegada de Carlos Salinas de Gortari a la Presidencia de la República como consecuencia de unas cuestionadas elecciones calificadas de fraudulentas, se modificó el nombre de DISEN por CISEN, Centro de Investigación y seguridad Nacional, como se le conoce actualmente, el cual no reflejó cambio profundo alguno en cuanto a su estructura, que continuó siendo la misma bajo los lineamientos y mecanismos de operación de la antigua Dirección Federal de Seguridad.

Hace 20 años el gobierno federal creó el Centro de Investigación y Seguridad Nacional (Cisen) y lo dotó de un sistema de operación clandestina que durante la primera década de su existencia representó para las dos últimas administraciones del régimen priísta - antes de la alternancia de 2000- una de las alternativas más confiables como fuentes de información clasificada en asuntos de política interior y de seguridad nacional (Torres, 2009:11).

Sin embargo, no obstante haber renovado sus instalaciones y capacitado a sus agentes y analistas en organismos de inteligencia como es la CIA en los Estados Unidos, el CISEN desde su creación, ha carecido de la credibilidad como una Institución garante que apunte hacia una protección eficaz de la seguridad nacional, lo anterior debido a la ambigüedad de su marco jurídico y a la corrupción, falta de coordinación que impera entre sus operadores y desprovisto de un sistema de inteligencia eficaz.

El Cisen nació subordinado a la Secretaría de Gobernación, en cuyo reglamento interno se establecieron sus principales atribuciones. Siete breves párrafos bastaron para legitimarlo en medio de la ambigüedad jurídica. Establecería y operaría “un sistema de investigación e información para la seguridad del país” y “se encargaría de convertir en inteligencia el dato, el informe o el testimonio recabado, decía el artículo 28 del reglamento que le dio vida (Torres, 2009: 42).

En México, el concepto en análisis, ha sido relacionado por mucho tiempo con cuestiones de política exterior y fuerzas armadas, lo que ha denotado un marcado desinterés por parte de la ciudadanía, ello aunado a la dispersión de las funciones de los servicios de Inteligencia, que al carecer de un sustento normativo en su formación, se han desacreditado, como fue el caso de la Dirección Federal de Seguridad durante el periodo del presidente Miguel de la Madrid, que, como nos menciona Luis Astorga, “nació corrupta”, el autor refiere a la época en que Miguel de la Madrid, delegó la responsabilidad de la misma a la Secretaría de Gobernación (segob) bajo la autoridad de Barttlet, quien a su vez recomendó a José Zorrilla para dirigirla y a quien el presidente de la Madrid solicitó despedir a algunos funcionarios por tener nexos con “traficantes”; desobedeciendo las indicaciones y nombrándolos paradójicamente asesores de dicha institución, personaje (Zorrilla) que posteriormente fue acusado del homicidio del periodista Manuel Buendía. (2007:17-18).

La falta de continuidad y coordinación provocada por el desconocimiento de las administraciones de gobierno, que sexenio tras sexenio buscan reinventar las actividades de lo que actualmente se conoce como CISEN, anteriormente

Dirección Federal de Seguridad y que en la actualidad funge como el principal órgano de espionaje civil, han generado una verdadera crisis carente de sustento normativo frente a una ley de seguridad que como ocurre a nivel internacional, no define objetiva y racionalmente el término de seguridad nacional.

De acuerdo a Benítez Manaut, durante el sexenio de Vicente Fox en México (2000-2006), el tema de la seguridad nacional careció de debate alguno, puesto que no hubo reformas estructurales de trascendencia ni recomposición alguna de los dos ministerios militares que son: la Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR), las políticas de seguridad continuaron bajo los mismos lineamientos que durante el largo régimen encabezado por el Partido Revolucionario Institucional (citado por Basombrio, 2013:31).

La hegemonía de los Estados Unidos, referida en páginas anteriores, que incorpora el término de seguridad nacional a sus políticas neoliberales, encuentra su influencia en México a partir de los atentados terroristas del 2000 a través del gobierno de Vicente Fox, que aunado a los conflictos internos del país, incluye esta nueva amenaza a la agenda de seguridad nacional.

En el gobierno de Fox, se agregaron temas sociales al concepto de seguridad nacional, como la migración y, sobre todo el efecto de los atentados terroristas del 11 de septiembre del 2001, que fue muy profundo, pues integró el terrorismo internacional a la agenda mexicana de seguridad, comenzando una era de intensa cooperación con estados Unidos (Bondi, 2004:s/p).

En el documento *The National Security Strategy of the United States of América* de septiembre de 2002, vincula el terrorismo, que en ese momento constituía una prioridad con el tráfico de drogas equiparable al mismo, por lo que establece:

La pobreza no convierte a la gente pobre en terroristas y asesinos. Sin embargo, la pobreza, las Instituciones débiles y la corrupción pueden hacer vulnerables a los Estados débiles ante las redes terroristas y los cárteles de droga dentro de sus fronteras (citado por Astorga, 2007:27).

No obstante, como lo apunta el analista Jorge Torres, mientras que el Ejército Popular Revolucionario se encontraba en su momento más activo de reclutamiento, el presidente Vicente Fox, el secretario de Gobernación, Santiago Creel y el Director del CISEN, Eduardo Medina Mora, cancelaron los programas secretos de infiltración, dejando en la oscuridad a los analistas de inteligencia del centro, lo que a su vez provocó un ambiente de expectativas de movimiento armado. No solo del EPR sino de 14 grupos de guerrilleros más que prevalecían en el país, desactivando sistemáticamente al centro desde inicios del sexenio.

Durante el periodo Foxista surgen, desde la ciudadanía, fuertes reclamos por incorporar en la agenda, la seguridad del ciudadano común y corriente debido a la ola de violencia que simultánea al crecimiento del narcotráfico prevalecía en las calles.

Para el año 2005, el CISEN, ya no tenía el prestigio ni la credibilidad que se le atribuyó en la segunda mitad de la primera década de su existencia, Los Pinos dejó de valorarlo como un verdadero órgano de inteligencia. Eduardo Medina Mora, quien continuaba a cargo como Director del Centro impulsó una Ley de Seguridad Nacional, a manera de reivindicar la crisis en que estaba inmerso, dicha ley entró en vigor en el mes de noviembre del 2005, nos explica Jorge Torres:

Se establecieron las reglas de coordinación para atender los asuntos de seguridad del país. Las decisiones se tomarían en el Consejo de Seguridad Nacional, “la instancia deliberativa cuya finalidad es establecer y articular la política en la materia. El Cisen quedó inmerso en dicho consejo junto a las secretarías de Gobernación, Defensa, Marina, Seguridad Pública y Procuraduría General de la República, entre otras atribuciones como “elaborar los lineamientos generales en el plan estratégico y la Agenda Nacional de Riesgos”. En materia de procuración de justicia, el Cisen se convirtió en auxiliar del Ministerio Público de la Federación en términos de apoyo técnico, tecnológico e intercambio de información. También se le facultó para intervenir comunicaciones previa solicitud al Poder Judicial para su autorización (Torres, 2009:158).

La promulgación de la nueva ley de Seguridad Nacional del 2005, generó un ambiente de mayor incertidumbre en las funciones operativas del Centro de Inteligencia, mediante el texto del artículo 31, que establece: “Al ejercer atribuciones propias de inteligencia, las instancias gozarán de autonomía técnica y podrán hacer uso de cualquier método de recolección de información, sin afectar en ningún caso las garantías individuales ni los derechos humanos...”

A veinticinco años de su fundación, no obstante que la estructura del CISEN conserva actualmente cuatro de las áreas claves para la obtención de la información política y la producción de análisis de inteligencia; como son las direcciones de Investigación, Análisis y Contrainteligencia, y mantiene como subdirección, el área de servicios técnicos, como una estructura burocrática con una infraestructura tecnológica, sus métodos y objetivos para acceder a la información continúan siendo cuestionables como un órgano de inteligencia profesional que garantice la observancia de los derechos humanos.

2.4.2 EL COMBATE A LA CRIMINALIDAD Y LAS NUEVAS MEDIDAS DEL ESTADO.

A partir del 11 de septiembre del 2001, el terrorismo desestabilizador, se convirtió en el tema prioritario relacionado estrechamente con el tráfico de drogas como una de las estrategias principales para su financiamiento

Siguiendo al analista Jorge Torres, testimonios de funcionarios de inteligencia, han señalado que Eduardo Medina Mora, como Director del Cisen dejó de lado la agenda de investigación de las bandas de narcotraficantes, cuya omisión- que comparte con todas las demás instancias de gobierno dedicadas al crimen organizado- provocó que los cárteles crecieran y se fortalecieran como nunca antes (Torres, 2009:160).

Posteriormente, el presidente Felipe Calderón incorpora a la agenda de seguridad prioritariamente, el tema del narcotráfico, como una verdadera amenaza, por lo que a través de la llamada “iniciativa Mérida” en el año 2006, se funda un

programa de cooperación entre México y los Estados Unidos. La herramienta principal que utiliza el gobierno de Calderón es el uso de las fuerzas armadas; el Ejército nacional fortalecido por el gobierno, se lanza a las calles a combatir el crimen organizado, generando un ambiente de tensión entre la ciudadanía y su confianza en las instituciones, agregando nuevas situaciones sobre violación de derechos humanos en el ejercicio de sus funciones.

Desde 2010, en México se ha decretado un gran debate sobre el poder acumulado por las organizaciones criminales. La discusión envuelve polémicas sobre si el Estado está ganando o perdiendo la “guerra” así declarada por el presidente Felipe Calderón y sobre si los cárteles han evolucionado de meras organizaciones criminales a algo superior que podría poner en peligro la gobernabilidad y la transición a la democracia. El elemento de vulnerabilidad de la estrategia criminal es el aumento de homicidios en el país en los últimos años, de 2007 a 2011 (Benítez, 2013:33).

La lucha intensa del gobierno de Calderón contra el narcotráfico, provocó el incremento de la violencia en el territorio nacional, al grado de ser considerado el Estado mexicano por los analistas, como un Estado fallido, en virtud de la falta de control de los sistemas de seguridad.

Benítez explica cómo “desde 2010, en México se ha abierto un gran debate sobre el poder acumulado por las organizaciones criminales. La discusión envuelve polémicas sobre si el Estado está ganando o perdiendo la “guerra” así declarada por el presidente Calderón y sobre si los cárteles han evolucionado de meras organizaciones criminales a algo superior que podría poner el peligro la gobernabilidad y la transición a la democracia” (citado por Basombrio, 2013: 26).

Aunado a la problemática descrita que cuestiona la capacidad del gobierno mexicano para combatir eficazmente los cárteles del narcotráfico, las teorías que vinculan a los propios funcionarios públicos de gobierno con el crimen organizado se han incrementado con los años en los tres niveles de gobierno, federal, estatal y municipal, pero de manera especial en la esfera de los municipios en donde se ha dado el fenómeno de la pérdida de territorialidad.

A nivel municipal, por la fragilidad financiera y política de los municipios ubicados en áreas rurales, las organizaciones criminales han logrado financiar campañas electorales, dando paso a una variable que antes solo había estado presente en los municipios de Sinaloa o Guerrero en el pasado, pero nunca a nivel expandido: *La narcopolítica*. Existe el caso emblemático a cerca del nivel de penetración de los cárteles del narcotráfico en las estructuras de gobierno: las relaciones del gobernador de Quintana Roo, Mario Villanueva, con los cárteles de tráfico de drogas de Colombia a México, vía el Caribe y Centroamérica (Benítez, 2013:37).

Otro fenómeno de suma importancia que contribuye a la crisis y la incapacidad del Gobierno para dar respuesta a la ola de violencia que se vive en México, es la postura del Estado frente a la utilización de las Tecnologías de la información por parte de la delincuencia; Toda vez que no existen los procedimientos en materia de criminalística, que de manera especializada den respuesta fehaciente a este problema, lo anterior en virtud de que no se obtiene la evidencia suficiente para la persecución y sanción de los sujetos que cometen las conductas antisociales y por tanto llegar al cabal cumplimiento de la Justicia; al respecto Oscar Lira nos comenta:

A partir del atentado del 11 de septiembre del 2001 contra las Torres Gemelas en la ciudad de Nueva York... el cual fue planeado y ejecutado a través del uso y aprovechamiento de las tecnologías de la información y comunicaciones, así como a la amenaza digital dirigido al ataque de sistemas financieros, sistemas de defensa, bases de datos, difusión de virus entre otros factores, hace que se trabaje de manera seria y globalizada en la generación y aplicación de leyes enfocadas a castigar conductas delictivas cometidas mediante el uso de equipos de cómputo y sistemas de comunicación, ya sea como fin o como medio (Lira, 2014, s/p).

No obstante lo anterior, el Estado mexicano ha recogido en su regulación algunos intentos a fin de reglamentar el uso de las tecnologías de la Información como herramienta para la persecución de los delitos; Sin embargo tales disposiciones comprometen otros derechos como es el caso de la privacidad y la protección de datos personales, que pueden ser vulnerados debido a una indebida interpretación y falta de precisión de dichas disposiciones.

La propia legislación mexicana establece supuestos de excepción en el tratamiento de Datos Personales como es el caso de la Seguridad nacional, Seguridad y orden público

y la Salud pública. Sin embargo, el legislador tiende a invocar estos conceptos de manera recurrente en el texto de la ley, sin que exista una precisión doctrinaria o legal sobre los elementos que los conforman.

2.5 LA SEGURIDAD PÚBLICA EN MEXICO

En base a los criterios del mismo CISEN, el concepto de seguridad nacional y Seguridad Pública si bien, no son sinónimos, son conceptos estrechamente relacionados:

De acuerdo con la Constitución, la Seguridad Pública es una función concurrente a cargo de los tres niveles de gobierno. Comprende la prevención, investigación y persecución para hacerla efectiva, así como la sanción de las infracciones administrativas. La Seguridad Pública puede convertirse en asunto de Seguridad Nacional en el grado en que la manifestación criminal represente un riesgo para la integridad, estabilidad y permanencia del estado, para el orden constitucional, las Instituciones democráticas fundadas en el desarrollo social, económico y político, y en el grado en que constituyan un obstáculo para que las autoridades actúen contra la delincuencia organizada (CISEN, 2010, s/p).

La seguridad pública forma parte esencial del bienestar de una sociedad. Un estado de derecho genera las condiciones que permiten al individuo realizar sus actividades cotidianas con la confianza de que su vida, su patrimonio y otros bienes jurídicos tutelados están exentos de todo peligro, daño o riesgo. “Ante la realidad de un Estado que no cumple con una de sus principales funciones, la de suministrar seguridad, los ciudadanos tendrán que centrar todos o gran parte de sus esfuerzos, en la defensa de sus bienes y derechos” (González, 1995:125).

En diciembre de 1995 fue reformada la Constitución Política de Los Estados Unidos Mexicanos en su artículo 21 antepenúltimo y último párrafo en donde aparece el concepto de seguridad pública como “ la función a cargo del Estado que tiene como fines salvaguardar la integridad y derechos de las personas

así como reservar las libertades, el orden y la paz públicos; Así mismo, se modificó el artículo 73 fracción XXIII sobre las facultades del Congreso de la Unión para legislar y expedir leyes, establecer bases de coordinación entre la Federación, el Distrito Federal y los Estados y municipios en materia de seguridad pública:

La reforma de 1994 fue el detonante para que el Estado pusiera atención en el combate del fenómeno de la inseguridad en territorio nacional. Por tal motivo, creó nuevas instituciones y ordenanzas, transformó las leyes sustantivas existentes, adjetivas, ejecutivas y orgánicas del sistema de la seguridad pública, así como los subsistemas de la procuración de justicia y de la justicia penitenciaria (Martínez, 2007:12).

Así mismo, la Ley General que sienta las Bases de Coordinación del Sistema Nacional, en su artículo 3º, establece que la función de seguridad pública se realizará en los diversos ámbitos de competencia, por conducto de las autoridades de policía preventiva, del Ministerio Público, de los Tribunales, de los responsables de la prisión preventiva, ejecución de penas tratamiento de menores infractores; así como las demás autoridades que en razón de sus atribuciones deban contribuir directa o indirectamente al objeto de ésta ley.

El mismo artículo 3º se refiere a los fines específicos del estado en sus funciones en materia de seguridad pública: “La seguridad pública es la función a cargo del Estado que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar, el orden y la paz públicos”.

Del texto anterior, podemos inferir, siguiendo al autor González Fernández, (129-130) que los valores tutelados por la seguridad pública en el derecho positivo mexicano, son: La vida y la integridad de las personas, tutela que se lleva a cabo por medio de actividades de prevención, con lo cual, el legislador busca evitar la realización de ciertas conductas tipificadas en el ámbito penal como delitos; Aunado a ésta función preventiva, se establecen normas complementarias que protegen estos valores fundamentales contra posibles actos de autoridad, como es el caso de las detenciones arbitrarias y la tortura.

Las garantías individuales son otros de los valores tutelados en un régimen de seguridad pública, como es el caso de lo previsto en los artículos 14 y 16 constitucionales que protegen al individuo contra actos de molestia o de privación por parte de los cuerpos policiales en labores de investigación y prevención, así como por parte de los agentes del Ministerio Público o personal de las procuradurías; magistrados, jueces y demás miembros del Poder Judicial, y en el ámbito administrativo de los custodios o personal perteneciente a los centros de readaptación social.

Otro de los valores tutelados por la seguridad pública es el orden y la paz públicos, condiciones necesarias para la subsistencia del Estado y la procuración del orden, a fin de evitar el caos y la anarquía.

No obstante lo anterior, se deduce, de los preceptos invocados, una dicotomía que estriba por un lado en la sociedad y el Estado a respetar los valores de dichas disposiciones, pero por otro la facultad del Estado mismo, en caso necesario, para vulnerarlas, mientras cumpla con todas y cada una de las formalidades legales del procedimiento.

Continuando con González Fernández, los preceptos legales enunciados del sistema de seguridad de la función estatal, se pueden abordar, a partir de cuatro ámbitos principales:

1.- PREVENCIÓN Y VIGILANCIA

Esta parte implica atacar las causas que generan la comisión de los delitos y las conductas antisociales, así como generar políticas y realizar programas y acciones para fomentar en la sociedad valores culturales y cívicos. Entre estas causas destacan: educación, cultura, valores, vivienda, distribución de la riqueza, empleo y entorno social y familiar. “El planteamiento de que a la delincuencia solo se le puede combatir si se le reprime, y sancionar a los delincuentes es atacar el problema por sus consecuencias más obvias, no es la solución” (Fernández, 2010 :p.131).

En este sentido, el autor enfatiza la participación ciudadana como determinante para que esta función tenga éxito, la cual básicamente consistiría en la denuncia del delito que constituye la proporción de información como el elemento más valioso de una investigación; otra de las formas de participación a que se refiere es a través de propuestas hechas a las autoridades, como es el caso de los lugares y horarios más frecuentes donde se cometen los delitos, y por último se refiere a su colaboración, a través de medidas de prevención mediante capacitaciones de prevención del delitos en escuelas, organizaciones sociales y comunidades, así como, tomando medidas básicas de seguridad fomentando la autoprotección ciudadana.

2.- PROCURACIÓN DE JUSTICIA.

El artículo 21 de la Constitución Política de los Estados Unidos Mexicanos establece: “La persecución de los delitos incumbe al Ministerio Público y a la Policía Judicial, la cual estará bajo el mando inmediato de aquel”.

Son numerosas las funciones que jurídicamente corresponden a la Procuraduría: representar los intereses sociales, perseguir e investigar delitos, integrar averiguaciones previas, ejercer ante el Poder Judicial la acción penal, actuar y dar seguimiento a los procesos penales, participar en la representación de los menores y discapacitados, colaborar en establecer una política criminal, cuidar los derechos humanos, proteger los derechos de las víctimas y velar por la observancia de todo orden jurídico de nuestra sociedad (Fernández, 1995:132).

3.- ADMINISTRACIÓN DE JUSTICIA.

Héctor Fix Zamudio, define a la Administración de justicia como: “un concepto con dos acepciones: en primer término, se refiere a la actividad jurisdiccional del Estado y, en segundo lugar, implica el gobierno y administración de los tribunales” (Fix-Zamudio, 1992:s/p).

El artículo 21 constitucional establece: “la imposición de las penas es propia y exclusiva de la autoridad judicial”.

Esta etapa inicia con el ejercicio de la acción penal por parte del Ministerio Público, es lo que se conoce como consignación de la averiguación previa y se erige como acusador ante la autoridad judicial.

Los jueces y tribunales no se limitan únicamente a evaluar que se sostenga la acusación del MP y sancionar al delincuente, también tienen la función de supervisar el proceso de procuración de Justicia, son un mecanismo de control de este proceso. Cualquier irregularidad que se haya presentado en la etapa anterior debe ser atendida dentro de esta fase: Por tanto son los responsables de evaluar la actividad del MP (Pérez, 2004:26).

4.- REINSERCIÓN SOCIAL

Este aspecto de la Seguridad Pública está sustentado en el texto del artículo 18 constitucional que establece: “Los gobiernos de la Federación y de los Estados organizarán el sistema penal en sus respectivas jurisdicciones, sobre la base del trabajo, la capacitación para el mismo y la educación como medios de readaptación social del delincuente”.

En esta esfera, el Poder Ejecutivo vuelve a asumir el mando. El sistema de readaptación social es parte del Sistema Nacional de Seguridad Pública y es administrado por la Secretaría de Seguridad Pública. Sin un sospechoso es hallado culpable por un juez, entonces se le remite para que cumpla su condena. Existen una serie de instituciones que tienen como misión ejecutar y administrar las condenas y buscar la readaptación del reo una obligación del estado Mexicano establecida en el artículo 18 de la Constitución (Pérez, 2004:28).

Nos explica Benítez Manaut, que a partir de enero del 2013 el Gobierno de Peña Nieto ha transformado las estructuras del área de seguridad del Gobierno Federal. Suprimió la Secretaría de Seguridad Pública, responsable entre otras funciones de la Policía federal, y trasladó ésta con sus 37 mil integrantes, a la Secretaría de Gobernación. En el seno de esta secretaría se conformó la Subsecretaría de Prevención del delito, para implementar la estrategia integral de prevención, buscando recuperar el control de las 57 ciudades donde hay más

concentración de actividad criminal. Igualmente se creó la comisión Nacional de seguridad y se está configurando la Gendarmería Nacional, que llegará a tener 40 mil miembros hacia el año de 2017. Este cuerpo nuevo se integraría por miembros de las fuerzas armadas (SEDENA y SEMAR Secretaría de la defensa Felipe Calderón entre 2007 y 2012) (Benítez, 2013:45).

Sin embargo, no obstante la intención del legislador por crear un marco jurídico que regule la seguridad en México, así como las transformaciones en la estructuras de los órganos responsables de garantizarla, autores como Benítez Manaut consideran:

Hay evidencias que demuestra que la reforma del Estado en materia de defensa está detenida por el hecho de haber empoderado a las fuerzas armadas para su combate. De igual manera el aumento de casos de violaciones de derechos humanos y la correspondiente impunidad de los cuerpos de seguridad del Estado afecta la transición hacia la democracia, en cuanto no se puede otorgar a la población muchas garantías civiles como el derecho libre de tránsito por todo el territorio, o el derecho al debido proceso cuando sus garantías son violentadas por parte de funcionarios del Estado (Benítez, 2013: p.46).

El presidente Peña Nieto, desde su toma de posesión, el primero de diciembre de 2012, afirmó que implementara un plan de seguridad de emergencia para reducir rápidamente la violencia, recuperar la gobernabilidad afectada por el crimen organizado y reconstruir las instituciones de seguridad. Basándose en diez puntos:

- 1.- reducir la violencia y recuperar la territorialidad en las ciudades más afectadas;
- 2.- Devolver la seguridad en todas las entidades federativas;
- 3.- Recuperar la confianza ciudadana;
- 4.- Reorganizar los cuerpos policiacos en los tres niveles de gobierno;
- 5.- homologar la profesionalización, equipamiento y capacitación de la policía;
- 6.- aumentar el número de agentes capacitados de la Policía Federal;
- 7.- Aplicar en todo el país el sistema de justicia penal acusatorio oral;
- 8.- Impulsar planes integrales de prevención, que incluyan estrategias de

salud y educación; 9.- Disminuir al menos en 50 por ciento la tasa de homicidios y secuestros; y 10.- abatir la extorsión y trata de personas.

2.6 SALUD PÚBLICA

La salud se define como “un estado de bienestar físico, mental y social, con capacidad de funcionamiento y no únicamente la ausencia de afecciones o enfermedades” (Milton Terris, 1987), existen sin embargo otras definiciones como “La forma gozosa de vivir autónoma, solidaria y alegre” (Gol,1976), o bien como “la capacidad social para gozar de la vida, para tener placer de vivir” (Nájera, Enrique, 1991).

“la salud pública es la ciencia y el arte de prevenir las enfermedades, prolongar la vida y fomentar la salud y la eficiencia física, mediante esfuerzos organizados de la comunidad para sanear el medio ambiente, controlar las infecciones de la comunidad y educar al individuo en cuanto a los principios de la higiene personal, organizar servicios médicos y de enfermería para el diagnóstico precoz y el tratamiento preventivo de las enfermedades, así como desarrollar la maquinaria social que le asegure a cada individuo de la comunidad, un nivel de vida adecuado para el mantenimiento de la salud” (Winslow, Hibbert;1920:s/p).

La salud pública es aquella rama de la medicina, cuyo interés radica en la incidencia de los fenómenos de salud en una perspectiva colectiva. Se trata “de la ciencia y el arte de organizar y dirigir los esfuerzos colectivos destinados a proteger, promover y restaurar la salud de los habitantes de una comunidad” (Piedrola Gil, 1991).

Así, los organismos gubernamentales llevan a cabo la acción comunitaria para la protección y mejora de la salud de los habitantes de una comunidad, lo cual requiere la implementación de determinadas políticas en materia de salud,

considerando que las funciones de la salud pública son todas aquellas actuaciones que deben ser realizadas con fines concretos para la obtención de un objetivo central que es la salud de las poblaciones.

La vigilancia en salud pública puede entenderse como el proceso de recopilación sistemática, la consolidación ordenada y la evaluación de datos pertenecientes a la salud (tanto en individuos como en grupos), con una comunicación rápida de los resultados o aquellos que precisen conocerla y en particular aquellos que estén en condiciones de emprender acciones (OMS 1968).

En México, el organismo encargado de la administración de la salud pública es la Secretaría de Salud, algunas de sus funciones son la creación de políticas públicas en la materia, la creación de programas, la coordinación de programas de salud, administración del Sistema Nacional de salud, prevención, control y erradicación de enfermedades, creación de establecimientos de asistencia pública, elaboración de campañas educativas y, en general, velar por la calidad del sistema sanitario, el derecho y el acceso a los servicios de salud, el bienestar colectivo y la calidad de vida.

El estado mexicano surgido de la revolución de 1910, ha plasmado en diversos documentos (Constitución, leyes), señalamientos jurídicos que sirven de marco para formular las políticas gubernamentales orientadas a lograr el bienestar de la población mexicana. Tales planteamientos legislativos buscan rescatar las justas demandas y aspiraciones de los grupos sociales a fin de contribuir a la legitimación del estado, es decir a que se le considere como representante legal de los diferentes sectores e intereses sociales (Rojas Soriano, 1999:147).

La finalidad de la vigilancia en materia de salud pública está relacionada con aspectos como la morbilidad, la discapacidad y la mortalidad, así como la discapacidad y la mortalidad originadas por enfermedades prioritarias y para mejorar la salud de la población.

De acuerdo al Aula Virtual de países de la Salud Pública, Investigación y Control de Riesgos y Daños en Salud Pública la evaluación del desempeño de la función de vigilancia en salud pública por parte de las autoridades sanitarias nacionales que debe tomar en cuenta los siguientes indicadores, por áreas de intervención estratégica: Logro de resultados e implementación de procesos claves; Sistema de vigilancia para identificar amenazas a la salud pública; Capacidad para dar una respuesta oportuna y efectiva al control de los problemas de salud pública, Desarrollo de capacidades y de infraestructura; Capacidad y conocimiento de epidemiología; Capacidad de laboratorios de salud pública; Desarrollo de competencias descentralizadas; y servicios de asesoría y apoyo técnico en salud pública a escala regional y local, en asuntos de la vigilancia, la investigación y el control de riesgos y amenazas (2014:18).

2.7 EL ORDEN PÚBLICO

Al igual que el concepto de seguridad nacional y el de interés general, el de Orden Público carece de precisión e indeterminación; Sin embargo el orden público ha sido utilizado a lo largo de la historia del derecho como sistema de solución a un conflicto de leyes, relacionado históricamente como noción al reconocimiento de leyes extranjeras en el campo del derecho Internacional Privado, en el sentido de sustituir una ley extranjera por una ley nacional, es decir, aquellos casos en los cuales dos individuos involucrados en un conflicto pertenecen a Estados distintos y por tanto a sistemas jurídicos diferentes.

Atendiendo al concepto en sí, puramente hablando del orden público como excepción a la regla general, podemos decir que se trata de un concepto dotado de relativismo dependiendo el momento histórico de que se trate, “la mayoría de los tratadistas en lugar de darnos un concepto preciso de lo que es el orden público, han buscado explicarlo con ejemplos; generalmente citan la investigación de la paternidad, la polígama y la esclavitud, como instituciones

contrarias al orden público internacional, por pertenecer a principios o instituciones de tipo moral universal e inmutable” (Magallón;1965:22).

En este sentido, Montalvo Abiol, refiriéndose al ordenamiento jurídico Español establece, que no aporta definición alguna respecto al concepto de Orden Público, lo cual se observa igualmente en el ordenamiento jurídico mexicano, dicho autor considera que la búsqueda de una definición de Orden Público no resulta fructuosa, concluyendo que será la casuística y el sentido común los que determinen qué constituye el Orden público en cada momento; Sin embargo, reconoce la irracionalidad de esta conclusión, en el sentido de que si el orden público puede ser concebido como limitador de derechos y garantías, lo saludable democráticamente es que exista una mención expresa en el ordenamiento, que legitime este tipo de situaciones.

En el caso de México, la Suprema Corte de Justicia de la Nación, nos proporciona una interpretación histórico-doctrinal y se pronuncia en el sentido de que existe un nexo indisoluble entre el orden público y los fines del Estado, incluso como motivo de su justificación y existencia, ya que procura que sea la acción política la que defina, realice y garantice cierto orden entre los hombres para que realicen los propósitos que se impongan según su naturaleza, condición que, en el entendido de que solo donde existe paz y orden, pueden desplegar sus potencialidades y permitir que se cumplan los cometidos del Estado. Se trata entonces de una obligación general de los ciudadanos a respetar ese bien común que, además de que les permite vivir en ejercicio de sus libertades o derechos, fundamenta también la actuación del Estado, de modo que a la vez que es obligación del ciudadano para que permanezca o se desarrolle, es garantía y justificación del propio Estado, porque puede limitar las acciones individuales que contraríen o vulneren ese estado de equilibrio o de paz social en que los diversos intereses confluyen.

Así, de acuerdo a la interpretación de la Corte, se pueden inferir dos concepciones distintas del orden público, como un conjunto de reglas escritas y no escritas de carácter jurídico público y privado, bajo una concepción de corte

ético y moral como la condición básica para la vida social constituida por una heterogeneidad de intereses individuales que evitan destruir armonía y equilibrio social a través de un sentido de respeto y por otro lado se entiende como un conjunto de principios éticos, ideas y concepciones sociales que formarán la cultura jurídica en un determinado momento histórico; Así entonces la Suprema Corte considera que por su carácter esencial, la noción de orden público, comprende el conjunto de reglas que según una determinada visión histórica de la vida social de las relaciones entre los individuos, resulta necesaria para la existencia del Estado y el desarrollo del individuo en equilibrio, armonía y paz, lo que atañe a la defensa de las libertades, derechos o bienes fundamentales del hombre y de los principios en su organización jurídica, para realizarse como miembro de una sociedad (2011, Tesis:1241)

Una de las aportaciones más importantes sobre el tema es la que nos proporciona Cuesta y Martin (2010) refiriéndose a que, el orden social constituye un elemento estructural en el organigrama estatal. Este orden se fraccionaría en dos: orden moral y orden jurídico, y este a su vez, se dividiría en orden privado y público. El primero englobaría las relaciones privadas tan solo y, el segundo, el Orden Público, constituiría el elemento clave para la evolución y existencia de la sociedad. Lo anterior se relaciona con la teoría del bien común como fin del Estado, el cual requiere de dos elementos el del orden y el de la justicia para funcionar. Sin embargo, si bien la justicia requiere del orden para funcionar, el orden no requiere necesariamente de la justicia para su preexistencia.

Así entonces, el hecho de que el Orden público se concibe como uno de los fines del Estado de una manera genérica, no implica que esté delimitada su concepción debido a la incertidumbre en cuanto a su definición, como nos menciona Montalvo, "... de una cuestión, especialmente interesante, que dicha figura se ha venido utilizando a lo largo del desarrollo y perfeccionamiento del ordenamiento jurídico como una cláusula que podría establecer limitaciones a derechos y libertades" (Montalvo, 2010:198).

Bajo estos términos, en la realidad social el concepto de orden público se configura como elemento de limitador de derechos relacionado estrechamente con sistemas de gobiernos conservadores o represivos al ser relacionado directamente en el ámbito de los derechos por razón de orden público. Sin embargo como menciona el mismo Montalvo (2010): “si el Orden Público puede ser concebido como limitador de derechos y garantías, lo razonable es que exista una correspondencia concreta en el ordenamiento que legitime este tipo de situaciones. Desviarse de este sencillo esquema implicaría un detrimento en la eficacia de los derechos y libertades fundamentales y dejaría sin operatividad la función garantizadora de la propia constitución” (p.212).

En relación a los conceptos tanto de orden público como de seguridad nacional y seguridad pública, se determina que, si bien el orden público puede ser concebido como limitador de derechos y garantías, lo saludable democráticamente es que exista una mención expresa en el ordenamiento que legitime ese tipo de situaciones (p.198).

Ahora bien, entendiendo a la seguridad como la ausencia de riesgo en el ejercicio de los derechos, (Montalvo, 2010:213), y la seguridad pública como garantizar la tranquilidad pública y la seguridad del orden público y de su organigrama institucional cuyo mantenimiento se encuentra a cargo de organismos del Estado, especializados, y con ello, la seguridad interior del mismo. En sentido propio, la seguridad pública, al igual que la paz o el Orden Público, como concepto este último que puede subsumir a la figura de la seguridad pública, son bienes generados por el conjunto de condiciones subjetivas, impulsadas por el Estado y creadas por el grupo social en el poder, cuya imprecisión deja libre su ejercicio para provocar la limitación de otros derechos y libertades.

La Justificación coactiva del Estado se fundamenta en los conceptos de “Seguridad Nacional”, “Seguridad Jurídica”, Salud Pública y Orden Público, los cuales se encuentran interrelacionados de tal manera que los dos primeros conllevan al tercero que es el Orden Público, como fin primordial del Estado; Sin

embargo ante la falta de imprecisión legal y doctrinaria en sus respectivas acepciones, son instrumentos factibles de limitar los derechos y libertades de los individuos de una sociedad, puesto que aquello que no está definido resulta difícil de ser regulado por la normatividad.

En el caso concreto, la ambigüedad del término de “Seguridad Nacional” en virtud de la falta de un consenso que lo defina, impide a los gobiernos ser regulada normativamente, en virtud de lo cual, se diluye la concretización de los bienes jurídicos protegidos, que, de acuerdo a los distintos Planes nacionales de desarrollo como parte de las políticas públicas en la materia en México, incluso resultan ilimitados en su descripción por parte del legislador, es decir, no existe una precisión exhaustiva que determine de manera concreta, cual es el bien jurídico protegido por la seguridad nacional, lo que nos lleva a un estado de relativismo y ambigüedad en la actividad legislativa que constituye una franca deficiencia en un sistema democrático.

En este sentido, ante la disolución de un marco teórico y legal que defina correctamente la seguridad nacional, así como el Orden Público, resulta imposible referirnos a políticas de seguridad nacional basada en conceptos, principios constitucionales de seguridad interior, defensa exterior de la nación, seguridad pública, o bien procuración de justicia.

Aunado a lo anterior, en el sistema jurídico mexicano hace falta un afianzamiento de los órganos responsables de la seguridad nacional (CISEN) y seguridad pública (Fuerzas de Seguridad), bajo un enfoque de servicio de carácter civil cuyos intereses a proteger y maneras de operar, se vean contenidos frente a otras funciones del Estado, con el acompañamiento de una función legislativa acorde, que permita lograr los objetivos de proteger las verdaderas garantías de los gobernados.

“Los operadores de la seguridad nacional a lo largo del mundo lo reconocen: un aparato de seguridad nacional fuera de control, es precisamente el mayor riesgo para la seguridad nacional. Yo lo traduzco a otro giro: un aparato de seguridad fuera de control, es la mayor amenaza contra el Estado Democrático de derecho y

la más evidente traición al soporte ético que le dio vida y forma al ejercicio de poder en el estado moderno” (portillo, 1989: 17).

La inestabilidad Institucional del CISEN como máximo organismo de Inteligencia en México y las deficiencias normativas, han generado una afectación en los derechos y libertades de los gobernados que ven vulnerada su esfera jurídica ante la ausencia de certeza jurídica en el actuar de los organismos estatales.

Como nos explica Jorge Torres (2009), en el CISEN, se han intervenido teléfonos e investigado sin distinción a narcotraficantes, secuestradores guerrilleros, políticos, empresarios, líderes sindicales, estudiantes, sacerdotes, periodistas.... No hay tregua para la información que existe en sus archivos. (p.161)

Las políticas de seguridad pública en México, no han demostrado una verdadera coordinación que se vea reflejada en un beneficio real en la sociedad, no obstante la creación de nuevas Instituciones y sistemas para combatirla. Contrariamente a los objetivos del Estado, la criminalidad va en aumento ya sea por cuestiones relacionadas con la corrupción o debido al nexo entre los cuerpos policiales y la delincuencia.

Como podemos apreciar, los distintos conceptos analizados: “Seguridad nacional”, “Seguridad Pública” y “Orden público” como justificantes de las actividades del Estado, han sufrido transformaciones en su concepción atendiendo al momento histórico de que se trate, aunado al hecho de que carecen de precisión tanto doctrinal como legalmente, puesto que no obstante ser invocados constantemente en la redacción de las leyes por parte del legislador, están dotados de una profunda subjetividad que impide el goce de derechos y libertades a lo cual debe someterse una sociedad.

El efecto globalizador que permea actualmente en la sociedad de la Información exige una estandarización de las legislaciones de todos los Estados

que genera una producción legislativa improvisada y deficiente, la cual obedece a las exigencias de la firma de los Tratados y Convenios Internacionales, generando verdaderos conflictos de derechos en perjuicio de sociedades que se encuentran bajo contextos sociales, jurídicos y políticos complejos, como es el caso de México, en donde las Instituciones encargadas de la aplicación normativa no se encuentran debidamente cimentadas, capacitadas y fortalecidas, de manera que garanticen una certeza jurídica en el gobernado en el cumplimiento de sus derechos humanos.

CAPÍTULO III

LA GEOLOCALIZACIÓN Y RETENCIÓN DE DATOS PERSONALES COMO MEDIDAS DE PROCURACIÓN DE JUSTICIA EN MÉXICO.

3.1 LA RETENCIÓN DE DATOS Y LA GEOLOCALIZACION COMO HERRAMIENTA DEL ESTADO EN LA PROCURACIÓN DE JUSTICIA. CONCEPTO Y ALCANCE JURÍDICO

Los delitos como es la pornografía infantil, fraude, extorsión, falsificación, robo de información, alteración de información, espionaje, secuestro, entre otros, han existido desde antes de que se inventaran las tecnologías, y se encuentran debidamente tipificados en los ordenamientos legales. Sin embargo, los dispositivos móviles de comunicación, la telefonía celular, las tabletas y las computadoras conectados a internet se han sumado como una herramienta más al servicio de la delincuencia, por tanto el gran reto para las técnicas criminalísticas en la investigación de delitos en los últimos años consiste en la especialización del personal responsable de administrar la justicia de manera simultánea al desarrollo de las tecnologías de la información, sobre todo en materias como son la Ingeniería en sistemas de cómputo, electrónica y comunicaciones. Al respecto nos explica Lira Arteaga:

En nuestro país, existen importantes vacíos legales relacionados con el control de los proveedores de servicios de internet, telefonía celular y los fabricantes de programas de cómputo, los cuales en algunos casos impiden a los investigadores

de este tipo de conductas delictivas, obtener la evidencia suficiente para perseguir y procesar penalmente a los responsables directos e indirectos, de lo que se empieza a considerar mundialmente como ciberdelitos (Lira, 2014:15).

Si bien en una primera etapa los delincuentes llevaban a cabo sus prácticas a través de equipos de cómputo conectados a internet, en la actualidad debido al constante desarrollo de la telefonía celular y a la accesibilidad inmediata que implica portar un equipo para un usuario, la delincuencia adquiere una dimensión a otro nivel, lo que expone a las víctimas no solo frente a la delincuencia, sino a cualquier clase de injerencia por parte tanto de autoridades o bien de terceros, como son las empresas con fines mercadotécnicos.

Actualmente el avance de la tecnología ha hecho que los teléfonos celulares incorporen funciones que no hace mucho parecían futuristas, como juegos, reproducción de música en archivos MP3 y otros formatos, correo electrónico y SMS, agenda electrónica PDA, fotografía y videos digitales, video-llamada, navegación por internet, televisión digital, medio de pago, localizador e identificador de personas entre otros. Lo anterior convierte al teléfono celular en una herramienta indispensable en la vida laboral de las personas y, en consecuencia, para las mentes criminales como medio para delinquir (Lira, 2010:455).

Como parte de las políticas de seguridad pública en nuestro país destaca la referente a la procuración de justicia en términos del artículo 21 Constitucional, que señala: “la persecución de los delitos incumbe al Ministerio Público y a la Policía Judicial, la cual estará bajo el mando inmediato de aquél”.

Tal y como explica Santana Oronoz, se puede concebir la etapa de investigación como aquella en la cual el Ministerio Público practica diversas diligencias con el propósito de concentrar los elementos necesarios de convicción

que permitan la comprobación del hecho delictivo e identificar plenamente a las personas a quienes se les imputa los mismos (Santana, 2010:159).

El concepto de geolocalización es relativamente nuevo y ha sido implementado desde hace aproximadamente dos años a la fecha, y se refiere a la ubicación geográfica de modo automático, es decir, la localización geográfica de un dispositivo, ya sea un dispositivo móvil o una computadora conectada a internet, y la cual funciona mediante una triangulación que permite identificar la dirección IP, que se conforma de números llamados octetos que se refieren al país y tipo de red, se trata de un identificador único en el mundo y es capaz de informar el país, la ciudad y el horario en que se ubica una persona.

Este proceso es generalmente empleado por los sistemas de información geográfica, un conjunto organizado de hardware y software, datos geográficos que se encuentran diseñados especialmente para capturar, almacenar, manipular y analizar en todas sus posibles formas la información geográfica referenciada. Esta tecnología se puede decir que ha pasado por varias fases y se ha desarrollado con el tiempo; al principio solo era disponible para aquellos que tuvieran acceso a los altos costos que conllevaba la localización por satélite, posteriormente se integró a los navegadores de los vehículos, hasta la actualidad en que podemos ubicar nuestra posición con el teléfono móvil (Gimeno, 2010:111).

El desarrollo de las tecnologías ha permeado en todos los ámbitos de la sociedad, en el caso de la administración de Justicia, los procedimientos jurídicos para la investigación de delitos han tenido que incorporar toda una serie de técnicas y herramientas metodológicas, a fin de extraer y analizar la evidencia digital con el objeto de esclarecer con mayor certeza sus indagatorias utilizando técnicas y procedimientos nuevos, aplicados por los peritos en las tecnologías de la información.

De esta manera surge un nuevo tipo de investigación, la Informática Forense que de acuerdo al FBI (Federal Bureau of Investigation), se trata de “la ciencia de adquirir, obtener y presentar datos que han sido procesados electrónicamente y almacenados en un dispositivo, ya sea electromagnético, óptico o electrónico.

Lira Arteaga (2010) nos define la Investigación Forense aplicada en tecnologías de la Información como “ la rama de la Criminalística, que se aplica en la búsqueda, tratamiento y preservación de indicios, relacionados con una investigación, donde el equipo de cómputo y/o de telecomunicaciones ha sido utilizado como fin o medio para realizar una acción presuntamente delictiva” (p. 256).

El mismo autor establece como objetivo de dicha materia “el auxiliar a la autoridad solicitante en el descubrimiento de la verdad histórica de los hechos de un presunto acto delictuoso, donde utilizan como medio o fin, equipo y programas de cómputo, dispositivos digitales de almacenamiento de datos equipo electrónico y/o equipo o dispositivos de telecomunicaciones para identificar a los autores del hecho” (Lira, 2010: 258).

No obstante lo anterior, ya desde hace años, los sistemas de intervención de comunicaciones tradicionales han gozado de un gran descrédito debido a su falta de operatividad, por lo que ha resultado complicada a transición hacia las intervenciones digitales.

Un factor determinante en la actualidad para el funcionamiento de la intervención de comunicaciones es la conexión a internet, que es precisamente la utilizada para la comisión de los llamados delitos cibernéticos. Lira Arteaga nos explica:

Para que la computadora de un usuario navegue en internet, es necesario primero que se le asigne una dirección IP, la cual será su identificador mientras esté conectado a la red; por tanto no podrá haber otra máquina en el mundo que se identifique con la misma dirección IP al mismo tiempo (Lira, 2010:456).

Lira (2010) nos refiere que la telefonía móvil, también llamada telefonía celular, está formada básicamente de dos grandes partes: una red de comunicaciones (también llamada red de telefonía móvil), y los terminales, que son los teléfonos móviles, los cuales permiten el acceso a dicha red. La red de telefonía móvil consiste en un sistema telefónico en el que mediante la combinación de una red de estaciones transmisoras-receptoras y una serie de centrales telefónicas de conmutación, hace posible la comunicación entre terminales telefónicas portátiles (teléfonos móviles) o entre terminales portátiles y teléfonos de la red fija tradicional.

La Oficina conocida por sus siglas en Inglés MTSO (*Mobile Telephone Switching Office*), conocida en México como la oficina de conmutación de telefonía móvil, es aquella que controla el procesamiento, es decir supervisión, conmutación y distribución del gran número de estaciones que integran las torres emisoras distribuidas en las ciudades, así, una ciudad puede contar con cientos de torres emisoras:

Cada portador en cada ciudad tiene una oficina central llamada MTSO, la cual controla todas las estaciones telefónicas y estaciones base de la región... cuando el usuario desea realizar una llamada, el teléfono celular envía un mensaje a la torre, solicitando una conexión a un número de teléfono específico. Si la torre dispone de los suficientes recursos para permitir la comunicación, un dispositivo llamado *switch* conecta la señal del teléfono celular a un canal en la red de telefonía pública; la llamada toma en ese momento un canal inalámbrico, así como un canal en la red de telefonía pública, y ambos se mantendrán abiertos hasta que la llamada se concluya (Lira, 2010: 452).

En las últimas décadas, la telefonía celular y la complejidad de las capacidades tecnológicas que han desarrollado hasta nuestros días, ¹ han adquirido una enorme relevancia como repositorios de una limitada cantidad de información, que obliga a que sean tratados minuciosamente bajo la óptica de las legislaciones y en concreto, las relacionadas con actividades criminales.

1 Como son el procesamiento de voz y audio, documentos y correos electrónicos, así como las características adicionales que pueden revestir como es el llamado GPS que en sus siglas en inglés significa Global Position System, es decir, sistema de posicionamiento Global.

En una definición básica podríamos decir que la palabra geolocalización es la palabra que en español significa *geolocation*, que se refiere a la localización geográfica de un dispositivo, como puede ser un dispositivo móvil o una computadora con conexión a internet. Es comúnmente usado por páginas de internet que ofrecen opciones basándose en el país o ciudad donde te encuentras (2003, www.gitsinformática.com).

El teléfono transmite una propuesta de registro y la red mantiene los datos acerca de su ubicación en una base de datos (de esta forma la MTSO, sabe en qué célula se encuentra si quiere timbrar su teléfono). A medida que se mueve entre células, el teléfono detecta los cambios en la señal, los registra y los compara con los de la nueva célula cuando cambia de canal (Lira, 2010:454).

La geolocalización constituye sin duda una herramienta tecnológica de gran trascendencia, que puede rastrear la movilidad de una persona sobre toda una infinidad de ubicaciones geográficas como son centros de culto, educativos, etc. y que en general permite conocer el desenvolvimiento de un individuo a través de los sitios en los cuales se desplaza constantemente, recopilando una serie de datos que permiten crear un perfil exhaustivo de los más íntimos detalles de su vida, lo que nos lleva a cuestionar la exposición constante de que es objeto frente a inferencias en su intimidad tanto por parte de las autoridades “facultadas” para ello como frente a terceros que pudieran tener acceso a dichos datos.

En México el tema ha sido el centro de múltiples controversias a partir de las reformas al Código Nacional de Procedimientos Penales del 2008 relacionadas con las actuaciones de la Procuradurías y Ministerios Públicos en la utilización de esta

medida, así como de las obligaciones establecidas en los artículos 189 y 190 fracciones I, II y III, de la Ley Federal de Telecomunicaciones y Radiodifusión, a cargo de las compañías que prestan servicios de telefonía móvil a la conservación y entrega a las “autoridades” de los datos de sus usuarios.

Derivado de lo anterior, es imprescindible que, como cualquier otra tecnología, la geolocalización sea regulada en su implementación y utilización como herramienta de la procuración de justicia, dentro un marco jurídico que precise bajo qué condiciones debe operar tanto por parte de las compañías que ofrecen el servicio de telefonía celular, como del tratamiento por parte de las autoridades que tengan acceso a los datos y de igual manera que se proporcione, bajo el principio de previsibilidad al usuario de telefonía celular, la información concerniente a dicho tratamiento.

Es precisamente el tema de la geolocalización el cual ha venido a cuestionar la falta de justificación, que analizaremos con más detenimiento en el apartado correspondiente al tratamiento de los datos personales ya que, como nos refiere Rodríguez Laínz en cuanto a “los datos relativos a las comunicaciones, algunos de ellos, de especial relevancia como los referidos a la geolocalización, suponen una grave restricción de los derechos concernidos (refiriéndose a la protección de datos personales y a la privacidad como objeto del mismo); capaces incluso de dar lugar a la realización de un exhaustivo perfil de cualquier persona, y que pueden llevar a los ciudadanos concernidos a la sensación de que sus vidas privadas podrían ser objeto de una constante vigilancia”. (Laínz, 2014:148).

La cuestión no es determinar si el monitoreo en tiempo real de la geolocalización de un equipo móvil encuadra o no en un supuesto de inconstitucionalidad, sino analizar si las disposiciones legales que permiten a las autoridades (en este caso las procuradurías) el uso de éstas herramientas, están apegadas a los estándares jurisprudenciales, doctrinarios, constitucionales, así como internacionales, que establecen lineamientos respecto al derecho a la privacidad y protección de datos personales en cuanto a la vigilancia encubierta.

A raíz de la reformas del 2008 al Código Nacional de Procedimientos Penales, si bien la investigación de los delitos continúa a cargo del Ministerio Público con el auxilio de las policías, las cuales actuarán bajo la conducción y mando de aquél en ejercicio de tal función, se busca que la investigación no se limite a la recolección de datos y medios de prueba que puedan servir para el esclarecimiento de los hechos, sino que tengan una función dentro del proceso jurisdiccional, como lo establece el artículo 102 del citado código “incumbe al MP la persecución de todos los delitos ante los tribunales” (art.102 CNPP).

Dentro del texto del CNPP (que busca complementar lo establecido por los artículos 189 y 190 de la Ley Federal de Telecomunicaciones), denota una interpretación ambigua al pretender distinguir entre las “técnicas de investigación y los actos de investigación”, toda vez que en el capítulo referente a las técnicas de investigación señala los actos que requieren autorización judicial y los que no pero no establece metodológicamente cuales son unos y otros; solamente se limita a relacionar como técnicas de investigación a la cadena de custodia, el aseguramiento de bienes, instrumentos, objetos del delito, y el decomiso (art. 227 a 250 CNPP).

Ahora bien, como actos de investigación enumera: La inspección del lugar distinto a los hechos o del hallazgo, Inspección de personas, revisión corporal; inspección de vehículos; levantamiento e identificación de cadáver, entrega vigilada y operaciones encubiertas; entrevista a testigos y los demás que sirvan para fines de la investigación (art.251), peritajes (art.272), aportación de comunicaciones entre particulares (art.276), reconocimiento de voces, sonidos y cuanto pueda ser objeto de percepción sensorial (arts. 280 y 281), cateo (art.282) y localización geográfica en tiempo real (art.303). Ninguno de los señalados requiere autorización judicial.

El artículo 303 del citado Código Nacional de Procedimientos Penales establece que, cuando exista denuncia o querella, bajo su más estricta responsabilidad, el Procurador, o el servidor público en quien delegue la facultad, solicitará a los concesionarios o permisionarios o comercializadoras del servicio de

telecomunicaciones o comunicación vía satélite, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con los hechos que se investigan en términos de las disposiciones aplicables.

Sobre el proceder que el artículo 303 faculta al Ministerio Público para solicitar sin control alguno la geolocalización satelital de cualquier teléfono que, de acuerdo a su consideración se relacione con la investigación criminal de que se trata, Aldo Macedo considera:

Un proceder a partir de este dispositivo legal-tal como este planteado- llevaría a que: a) se sobredimensione el rol del Ministerio Público en el proceso penal, al asumir que su ejercicio sería per se impecable y, por tanto, no requiere someterse a escrutinio judicial que cuide su idoneidad o prevenga un desempeño, arbitrario, infundado o sesgado; b) prevalezca un discurso para el cual ciertas prácticas tecnológicas avanzadas-como la geolocalización satelital- estén disponibles en lo inmediato. Y, en consecuencia no implica el riesgo de una acción tendenciosa, o distorsionadora, es decir, tales prácticas son concebidas en sí como “neutrales”; c) que no se valoren como límites constitucionales la protección de datos personales, y, en general el principio de privacidad, por lo que si estos son vulnerados-queda claro que ocurrirá en la práctica- es algo que resulta inevitable “sacrificar” en aras de la investigación del delito, dado que lo importante es una respuesta eficaz de cara a la sociedad (Macedo,2015:162).

3.2 LOS CONCESIONARIOS Y PRESTADORES DE SERVICIOS DE TELEFONIA CELULAR COMO SUJETOS OBLIGADOS Y EL TRATAMIENTO DE LOS DATOS PERSONALES EN MEXICO.

Conforme a la Constitución Política de los Estados Unidos Mexicanos, así como a la Ley Federal de Telecomunicaciones y Radiodifusión, los títulos habilitantes para telecomunicaciones se dividen en **concesiones**, (servicios públicos de telecomunicaciones, redes públicas de telecomunicaciones, bandas de frecuencias

y en materia satelital), **permisos**, (comercialización de servicios de telecomunicaciones, estaciones transreceptoras) y **registros** (servicios de valor agregado).

Una dirección IP (Internet protocol) es un número que identifica de manera lógica la interfaz de un dispositivo (equipo de cómputo) dentro de una red, para que un usuario o compañía pueda tener acceso a Internet será necesario contratar los servicios de un proveedor de servicios de internet (ISP) que pondrá a disposición de los usuarios el servicio de manera fija o dinámica (Lira, 2010: 420).

La Ley Federal de Telecomunicaciones en México, en su artículo 3º fracción XIV, define a los concesionarios como aquellas “personas físicas o morales, titulares de una concesión de las previstas en esta ley”, así mismo, define a la comercializadora, en su fracción XI como: “toda persona que proporciona servicios de telecomunicaciones a usuarios finales mediante el uso de capacidad de una o varias redes públicas de telecomunicaciones sin tener el carácter de concesionario en los términos de esta ley”.

En la misma disposición, fracción LXIII, define los servicios de interconexión como: “Los que se prestan entre concesionarios de servicios de telecomunicaciones, para realizar la interconexión entre sus redes e incluyen, entre otros, la conexión de tráfico, su originación y terminación, enlaces de transmisión, señalización, tránsito, puertos de acceso, ubicación, la compartición de infraestructura para interconexión, facturación y cobranza, así como los servicios auxiliares de la misma y acceso a servicios”.

La Comisión Federal de Telecomunicaciones (Cofetel), establece que los concesionarios de nuestro país se dividen en dos grupos: los de telefonía celular y los concesionarios de telefonía celular inalámbrica, entre los primeros encontramos como concesionarios Grupo Telefónica Movistar, Iusacell y Telcel.

En México, el servicio de telefonía se ofrece por asignación de dos tipos de bandas, la banda A y la banda B; La concesionaria TELCEL presta el servicio en la banda B, misma que cuenta con cobertura nacional.

En 1991 se formó la Asociación Mexicana de Concesionarios de Radiotelefonía Celular, A.C. integrada por las compañías restantes que operan en México y que prestan el servicio de radiotelefonía celular por la Banda A; estas empresas cuentan con convenios entre sí y pueden prestar el servicio con cobertura nacional (roaming). Así mismo existe una división regional para la prestación del servicio en México, la cual cuenta con nueve regiones con coberturas y empresas que ofrecen servicios (Lira, 2010:455).

Los artículos 189 y 190, fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radio Difusión, establecen la colaboración de los concesionarios y prestadores de servicios de telefonía celular con la autoridad, así como los datos que dichos operadores deben conservar de los usuarios, atendiendo al mandamiento “de la autoridad competente en los términos que establezcan las leyes”, concretamente el 190, fracciones I, II y III como parte de dichas obligaciones, la de colaborar con la “geolocalización” de los equipos de comunicación móvil, de conservar un registro y control de comunicaciones que incluyan los datos del usuario y entregar el registro de dicha información en el caso de que la autoridad lo requiera.

Hablando específicamente de telefonía celular, en nuestro país, no contamos con acuerdos de colaboración entre autoridades y compañías de telefonía móvil que permitan optimizar el proceso de investigación de conductas delictivas, como el secuestro y la extorsión, ejecutados a través de un dispositivo móvil de comunicación (Lira, 2010:531).

Si bien el análisis de las líneas telefónicas para efectos de combate a la delincuencia se debe llevar a cabo con base en una relación de coordinación entre

el personal responsable de las telecomunicaciones (la compañía donde se detecta la intervención y/o el personal responsable del proveedor del servicio), resulta imprescindible cuestionarnos qué datos son los realmente necesarios para efectos de que la autoridad complemente la investigación criminal en atención al principio de proporcionalidad, cuál es la finalidad de la conservación de los mismos, la temporalidad y qué destino se dará a éstos una vez concluido el fin para el que fueron recabados y transmitidos por parte de la compañía de telefonía a la “autoridad judicial”.

Con base en los resultados del estudio denominado “¿Quién defiende tus datos?” realizado por las organizaciones: Red en Defensa de los Derechos Digitales (RD3) y la *Electronic Frontier Foundation* (eff.org; ¿Quién defiende tus datos?; 2015), las compañías de telecomunicaciones deben observar políticas adecuadas para proteger los derechos a la privacidad y la protección de datos personales de sus usuarios; sin embargo, en el caso de México, de las tres principales compañías que operan, se ha determinado que: “la compañía Telcel es la que tiene más bajos estándares de protección de privacidad y defensa de los datos de los usuarios ante los abusos de las autoridades en virtud a la falta de claridad en sus políticas de privacidad, de requerimientos de autorizaciones judiciales a las autoridades para la entrega de datos y metadatos de las comunicaciones y de reportes de transparencia públicos, también se demuestra la inexistencia de una defensa de sus clientes ante los tribunales en caso de una situación abusiva”, así como la ausencia de notificaciones a los usuarios cuando sus datos son solicitados por el gobierno.

El panorama descrito resulta preocupante ante el posicionamiento avasallante en el mercado con que cuentan las empresas Telcel y Telmex (propiedad de América Móvil), las cuales abarcan el 70% del mercado de líneas móvil, en México.

De acuerdo a dicho estudio, llevado a cabo por la RD3, se determina que la compañía Telcel ha recibido la mayor cantidad de solicitudes de metadatos y geolocalización por parte de las autoridades, acumulando la cantidad de 25,747 al primer semestre del 2016. “Telcel no opuso resistencia en ningún requerimiento a

pesar de que entre los solicitantes se encuentran autoridades no facultadas para pedir esa información”.

Por lo que respecta a las otras compañías de telefonía móvil que operan en el mercado mexicano, AT&T y Movistar, igualmente carecen de los procedimientos adecuados para notificar a sus usuarios qué información ha sido entregada cuando las autoridades solicitan información una vez transcurrido el término legal, lo cual, conforme al artículo 190 de la Ley Federal de Telecomunicaciones es de 2 años, sin reconocer explícitamente el derecho de los usuarios de acceder a sus propios datos, por lo que este se ve impedido para impugnar los abusos de autoridad ante la falta de un servicio de litigio estratégico que le permita a la empresa hacer frente a la defensa de los derechos de sus usuarios ante los tribunales.

El usuario afectado por una medida de vigilancia debe ser notificado, aunque esto no ocurra de manera inmediata dicha notificación debería llevarse a cabo una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, por ello las empresas que prestan servicios de telecomunicaciones deben intentar establecer una política de notificación a los usuarios” (eff.org; ¿Quién defiende tus datos?; 2015; consultado el 17 de enero del 2017).

El tratamiento de los datos personales por parte de las compañías de telefonía móvil adolece de una sistematización en sus procedimientos que garantice a los usuarios del servicio una seguridad y protección de su información, así como la restricción de derechos esenciales como son la cancelación, oposición y el conocer el destino de sus datos una vez transcurrido el término de tratamiento.

3.2.1 LOS DATOS OBJETO DEL TRATAMIENTO

El concepto de comunicación ha cambiado a lo largo de las distintas sociedades que se han desarrollado a través de la historia, sin embargo en las últimas décadas ha sufrido notables transformaciones, incluyendo todos los medios de

comunicación que existen y que a futuro pueden continuar surgiendo, en atención al desarrollo tecnológico.

Tomando en consideración que los datos parten de una documentación, como lo expresa Davara Rodríguez (2008:705), que son sometidos a un tratamiento o adecuación a un fin para obtener un resultado elaborado, los datos personales deben estar protegidos frente a terceros que no estén autorizados al acceso a los mismos.

Dentro de las corrientes que protegen a la intimidad individual frente a las amenazas que implican las tecnologías de la información, es importante el planteamiento de la conocida “Teoría del Mosaico” que, de acuerdo a Lucrecio Rebollo (2005), se trata de una construcción doctrinal, que se contrapone a la teoría sostenida por Fulgencio Madrid, “la teoría de las esferas” la cual refiere a la existencia de círculos concéntricos, que definen los distintos grados de privacidad de los datos de un individuo y en donde los más alejados del centro contienen información pública, el siguiente información de la vida privada y el más céntrico pertenece a la intimidad, es decir aquellos datos más sensibles e íntimos; en este sentido, la teoría del Mosaico la invalida: “dado que los conceptos de lo público y lo privado son relativos, pues existen datos que a priori son irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos unos con otros pueden servir para configurar una idea prácticamente completa de cualquier individuo, al igual ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado” (288-291).

Ahora bien, La inviolabilidad de las comunicaciones privadas forma parte del derecho a la intimidad o a la vida privada como derechos fundamentales y su objeto consiste en el secreto de las comunicaciones. “Se trata de un derecho reconocido por los textos constitucionales en el artículo 12 de la Declaración Universal de los Derechos Humanos, en el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos y se encuentra sustentado en el artículo 8 del Convenio de derechos Humanos y en el Artículo 7 de la Carta de Niza. 3

3 En el Diario Oficial de la Federación, el 3 de julio de 1996 se publicó el decreto por el que se adicionaron al artículo 16 Constitucional los párrafos noveno y décimo que regulan la intervención de las comunicaciones privadas: El decreto publicado el 18 de junio de 2008 modificó el párrafo noveno y dividió su contenido en dos párrafos, que quedaron como el decimoprimer y decimosegundo. Por otra parte el 1o de junio del 2009, se agregó al artículo 16 un párrafo segundo

En este mismo sentido nos explica Ovalle Favela que el párrafo segundo del artículo 16 establece, como regla general, el carácter inviolable de cualquier tipo de comunicación privada, dentro de las que quedan incluidas, entre otras, las telefónicas y las radiotelefónicas (mencionadas en la exposición de motivos de la iniciativa de 1996) así como los correos electrónicos. Que este derecho a la inviolabilidad se refiere a todo tipo de comunicaciones privadas, siendo confirmado en la sentencia dictada el 15 de junio de 2011 por la Primera sala de la Suprema Corte de Justicia dentro del Amparo en revisión 1621/2010, interpuesto por Rebeca Alegre Rodríguez. En la cual se afirma: “En definitiva todas las formas existentes de comunicación y aquellas que sean fruto de evolución tecnológica, deben quedar protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas” (fojas 43 y 44); (Ovalle, 2013:1803).

No obstante la protección al contenido de las comunicaciones privadas, existen otros datos que forman parte de dichas comunicaciones, por lo que debemos considerar que los dispositivos móviles permiten almacenar todo tipo de información, desde la dirección IP, incluyendo no solamente mensajes de texto, de voz, imágenes y videos, que constituyen propiamente el contenido en sí mismo, sino también los llamados datos de tráfico que implican los relacionados con el origen, destino de un mensaje o llamada así como la ubicación de una persona:

A fin de garantizar la reserva que se predica de que todo proceso comunicativo privado, resulta indispensable que los datos externos de la comunicación también sean protegidos. Si bien es cierto que los datos no se refieren al “contenido” de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre

que reconoce la protección de datos personales y por lo que respecta a las comunicaciones privadas estas quedaron contempladas en los párrafos, decimosegundo, décimo tercero y decimoquinto.

las circunstancias en que se ha producido la comunicación, ofreciendo así de modo directo o indirecto, la privacidad de los comunicantes. [...] Así, a modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, comunicantes o la duración de la llamada telefónica, llevado a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración (SCJN, Amparo 1621/2010, 2011).

En este sentido, La Suprema Corte de Justicia de la Nación, mediante la resolución 1621/2010, ha determinado que el derecho a la inviolabilidad de las comunicaciones protege tanto el contenido de las comunicaciones como los datos relacionados con dichas comunicaciones por lo que considera que, si bien, los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, señalando que el registro de los números marcados o la duración de la llamada telefónica llevado a cabo sin observar las debidas garantías para restringir el derecho fundamental al secreto a las comunicaciones, puede provocar su vulneración (México, Suprema Corte de Justicia, Amparo Directo en Revisión 1621/2010).

La cuestión estriba en determinar si los datos que proporcionamos al contratar con una compañía de telefonía móvil, se recaban en observancia a los principios de finalidad y proporcionalidad, es decir, si son realmente los necesarios para el fin solicitado y de qué manera se están resguardando por parte de estas compañías, si cuentan con los procedimientos adecuados para dicho tratamiento y, un tema aún más delicado, la transmisión de dichos datos a las autoridades por requerimiento judicial y otro aspecto no menos importante es si existen los

mecanismos de protección de los derechos de los usuarios ante el riesgo potencial de abusos de autoridad.

Debemos considerar en primer lugar la presencia indiscutible del fenómeno del Big Data, es decir, los “Metadatos de la Comunicación”, esto es, los datos personales (no solamente datos de tráfico) que se derivan de la interacción del individuo con las tecnologías a través de las comunicaciones: los datos personales generados en las comunicaciones electrónicas a través de teléfonos móviles y otras tecnologías, los cuales abren la posibilidad de recopilar información de manera indiscriminada y masiva y permiten crear perfiles de los individuos que genera un ambiente de vulnerabilidad de la privacidad y protección de datos ante el descontrol de información.

Tales datos, pueden proporcionar una inestimable fuente de información para averiguar y descubrir la comisión de hechos delictivos, facilitada o posibilitada mediante el uso de dichas redes de comunicación. Y así mismo, aunque en otro orden de importancia, los datos generados en las telecomunicaciones pueden resultar imprescindibles o de vital importancia (Ormazábal, 2008:1397).

La Ley Federal de Telecomunicaciones y Radiodifusión establece en su artículo 191 fracción II, el derecho con que cuentan los usuarios de los servicios de telecomunicaciones para la protección de datos personales en términos de las leyes disponibles.

Así mismo, La propia ley Federal de Telecomunicaciones y Radiodifusión define en su artículo 3º fracción LXIX como “Tráfico”, a los “Datos, escritos, imágenes, voz, sonidos e información de cualquier naturaleza que circulan por una red de telecomunicaciones”.

Así entonces, tenemos que en el proceso de análisis para la extracción de información de un teléfono celular se consideran datos, como es la identificación del número telefónico, el dispositivo, el número de llamadas entrantes, el número de llamadas salientes, los mensajes de texto recibidos y enviados, los archivos de audio y video, así como la recuperación de archivos o datos eliminados.

Las redes de contacto a través de los números telefónicos de contactos entrantes y salientes. La correcta explotación de bases de datos permite identificar y ligar todos los contactos de un cierto número de celular, y con el paso del tiempo brindar información de inteligencia para identificar y anular células completas de bandas de delincuencia organizada (Lira; 2010: 531).

Sin embargo, los datos que no constituyen propiamente el contenido de la comunicación, como son el destinatario, la fecha o bien la localización de los equipos móviles de comunicación, pueden incluso por sí mismos, constituir objeto de una injerencia excesiva por parte del sujeto obligado a la conservación y de la autoridad solicitante, de tal manera que se vean afectados derechos fundamentales como es la intimidad y la autodeterminación informativa.

Al respecto, Ormazábal Sánchez nos expone:

El derecho a la intimidad en su versión de derecho a la autodeterminación informativa, se vería seriamente afectado si los operadores de telecomunicaciones pudiesen comunicar sin trabas o limitaciones los datos generados en las comunicaciones de sus clientes... dejo fuera del objeto de las líneas que siguen la revelación del contenido mismo de dichas comunicaciones, lo que afectaría el derecho al secreto de las mismas y pretendo referirme a la posibilidad o licitud de dar a conocer ciertos datos relacionados con la comunicación, tales como su destinatario o la fecha en que tuvo lugar, de modo que el derecho que puede quedar afectado es el ya referido de la autodeterminación informativa, como manifestación del derecho a la intimidad (Ormazábal, 2008: 1397).

Como parte de las mencionadas reformas a la ley Federal de Telecomunicaciones y Radiodifusión, los artículos 189 y 190, en sus fracciones I, II y III, establecen la obligación de las Compañías de Telefonía celular a conservar los datos de sus usuarios por el término de dos años y la obligación de proporcionarlos a las autoridades cuando les sean requeridos previa autorización judicial.

Dichas disposiciones han sido validadas por la Suprema Corte de Justicia de la Nación, es decir, las disposiciones que permiten a las compañías de telefonía móvil la conservación de hasta por dos años un registro masivo e indiscriminado de datos relacionados con el destino, fecha, hora y duración de todas las comunicaciones, así como la ubicación geográfica de los dispositivos de los usuarios, estamos hablando de los metadatos de las comunicaciones, es decir información obtenida de información previa, "... nosotros entendemos qué son los datos: son la información que comunicamos, procesamos o consumimos en nuestra sociedad digitalizada en constante crecimiento.. los metadatos **describen** qué son esos datos..." (icann.org; consultado 23 de enero 2017). Dicha información es capaz de revelar cuestiones políticas, religiosas, sexuales, de salud, relaciones personales, lo que permite crear un perfil sobre la vida privada de los individuos de manera general asumiendo que todos somos sospechosos de una conducta delictiva, en tanto no se pruebe lo contrario.

Sin embargo quedan muchos vacíos legales que deben cubrir requisitos indispensables para la aplicabilidad de estos artículos, cuestiones técnicas y procedimentales que dejan en estado de vulnerabilidad al usuario de los servicios de telecomunicaciones y en este particular, de telefonía móvil.

En primer término es importante analizar cuáles son los datos realmente necesarios que se deben proporcionar al contratar un servicio de telefonía móvil, si las empresas realmente aplican los principios de proporcionalidad y finalidad y como nos menciona incluso, Rodríguez Laínz, el principio de previsibilidad "... de suerte que pudiera preverse por los ciudadanos, cuando y en qué circunstancias se puede acceder a dichas bases de datos de origen legal..." (Laínz, 2014:1523).

En segundo lugar, se debe considerar si existen los mecanismos necesarios por parte de las compañías de telefonía para asegurarse que la autoridad que está solicitando los datos es la legalmente autorizada.

En tercer lugar, si los datos requeridos por la autoridad son los estrictamente necesarios para la investigación criminal y si no se están proporcionando datos indebidamente que pongan en riesgo la privacidad del usuario.

En cuarto lugar, si existen mecanismos de notificación (una vez transcurrido el término de dos años) y que tratamiento se le ha dado a sus datos una vez transcurrido el término legal y los mecanismos de defensa a los usuarios para evitar abusos de autoridad.

Con relación a los datos de tráfico es importante dejar sentado que los artículos 189 y 190 de la ley federal de telecomunicaciones, no obstante que señala cuáles son los datos del usuario a conservar para efectos del servicio, no especifican cuales son los datos que las compañías telefónicas deben retener para efectos de transferir para causas criminales, por lo que de acuerdo a la teoría del mosaico cualquier dato, por irrelevante que resulte, puede ser determinante para definir el perfil de un individuo.

Como requisito indispensable para que las empresas de telefonía móvil de acuerdo con lo establecido en la ley (art. 189 y 190), proporcionen datos relativos a sus usuarios, a petición de las autoridades, debe mediar la autorización judicial.

No obstante lo anterior, el texto del artículo 189 carece de precisión al establecer: “Los titulares de las instancias de seguridad y procuración de justicia, designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación” LFTR). Con lo anterior se deja al individuo, cuyos datos sean susceptibles de transmisión fuera de todo conocimiento sobre qué autoridades realmente están facultadas para emitir dichas autorizaciones.

En el caso concreto de la geolocalización, la Suprema Corte de Justicia ha determinado que el requerimiento legal de autorización judicial, no es requisito para

el monitoreo continuo por parte de las autoridades, ya que no atenta contra la inviolabilidad de las comunicaciones (Amparo en Revisión 964/2015; SCJN).

Lo anterior representa un grave riesgo para la ciudadanía debido a la complicidad de las autoridades con los grupos criminales. Además es una contradicción porque para la solicitud de datos a las compañías concesionarias, sí requiere la autorización, pero para la geolocalización no.

Los procedimientos con que cuentan las compañías de telefonía móvil para salvaguardar los derechos de sus usuarios en obediencia a las distintas legislaciones que los protegen, como es la Ley para la protección al consumidor y la propia ley Federal de Telecomunicaciones y Radiodifusión resultan cuestionables al no estar definidos en la legislación de la materia, lo que atenta contra el principio de legalidad que debe regir todo procedimiento, así como a los accesos ilegítimos por parte de “cualquier” autoridad que se diga competente.

3.3 LOS PRINCIPIOS DE PROPORCIONALIDAD Y DE FINALIDAD EN EL TRATAMIENTO DE DATOS.

Tal y como refiere González Ballesteros, en la utilización de datos personales podemos distinguir entre los datos referidos a una persona que son susceptibles de recogida y elaboración de forma individualizada, no anónima, y aquellos otros con fines meramente estadísticos y anónimos. En el primer supuesto habrá que entender que hay un interés social preponderante respecto a los datos con referencia social, cuando se excluyan datos íntimos no exigibles razonablemente y toda autoacusación. El suministro legalmente obligatorio de datos de referencia personal exige la existencia de una ley que determine la finalidad de utilización de los mismos con toda precisión en cuanto al ámbito, y que los datos sean adecuados y necesarios para esa finalidad, siendo ilegal la recogida de datos y su acopio para fines indeterminados (González, 1987:s/p).

El principio de finalidad, también reconocido como principio de objetivo legítimo, justifica las infracciones a Derechos humanos previa la existencia de un propósito determinado que proteja un interés jurídico que lo legitime en una sociedad democrática, como nos explica Karitza Rodríguez:

En lo que respecta a las infracciones del derecho de la privacidad de las comunicaciones, la investigación de delitos graves, amenazas, amenazas concretas a la seguridad nacional son reconocidas como objetivos legítimos. La vigilancia de las comunicaciones no puede ser justificada por referencia a un interés general, como la “seguridad” o a una preocupación por la “seguridad nacional” abstracta e indefinida (Rodríguez, 2015: 10).

En dichos términos, el derecho a la Protección de datos personales, debidamente reconocido en nuestro Sistema Constitucional Mexicano en sus artículos 6 y 16, tiene como fundamento dos principios muy importantes, como son el de proporcionalidad y finalidad, los cuales se encuentran plasmados en el artículo 6º de la Ley Federal de Protección de Datos Personales en Posesión de Particulares; por lo que se debe prever como datos objeto de tratamiento solamente aquellos necesarios, pertinentes y que tengan relevancia en la investigación para el esclarecimiento del delito perseguido y, en cuanto a la temporalidad, recabar solamente los datos referentes a periodos acordes con la gravedad del caso concreto a la que se encuentra sometido el sujeto investigado.

Ahora bien, aplicando el principio de finalidad al contexto del derecho a la protección de datos, se requiere determinar el objetivo o fin por el cual se están recabando y conservando los datos personales de los usuarios de telecomunicaciones y de qué manera se van a tratar, y si en todo caso dicho fin es la persecución de delitos, se debería especificar a qué delitos se refiere concretamente.

En atención al principio de proporcionalidad como sustento de la intervención de datos, Karitza Rodríguez nos indica:

El principio de proporcionalidad requiere que las decisiones que interfieran con los derechos humanos consideren la gravedad de la interferencia y otros intereses en competencia caso por caso, y sólo permitan la infracción si el interés público logra un equilibrio adecuado frente a las pérdidas de derechos humanos. Más aún, cualquier medida que interfiera con los derechos humanos deben ser el medio menos invasivo para realmente lograr un objetivo legítimo (*necessaryandproportionate.org*; Rodríguez, 2013:12).

En los mismos términos, la autora considera que un Estado debe establecer como condiciones para proceder a la interferencia de las comunicaciones, “como mínimo”, las siguientes:

- 1.- Que exista un alto grado de probabilidad de que un delito serio o una amenaza específica a un objetivo legítimo ha sido o será llevada a cabo;
- 2.- Que existe un alto grado de probabilidad de que las pruebas pertinentes o materiales de tal amenaza específica al objetivo legítimo pueda ser obtenida mediante el acceso a la información protegida solicitada;
- 3.- Otras técnicas menos invasivas han sido agotadas, o sería inútil de tal manera que la técnica utilizada es la opción menos invasiva;
- 4.- La información accesada debe limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo;
- 5.- Cualquier exceso de información que se recaba no será retenida, pero en vez será destruida o devuelta con prontitud;
- 6.- La información será accedida únicamente por autoridades especificadas y utilizada solo para el propósito y duración para la que se dio la autorización;

7.- Que la vigilancia de las actividades solicitadas y las técnicas propuestas no menoscaben la esencia del derecho a la privacidad o libertades fundamentales.

El alto Tribunal Europeo, en la declaración de invalidez de la Directiva 2006/24/CE consideró como uno de los puntos focales base de la argumentación que las restricciones a la privacidad y protección de datos de carácter personal solamente podrían superar el juicio de valor, cuando pudieran considerarse estrictamente necesarias.

Para la superación de tales juicios de valor se hace indispensable que las personas cuyos datos hayan sido retenidos, tengan las garantías suficientes de que sus datos personales se encuentran efectivamente protegidos frente al riesgo de abuso y de ilegal acceso y uso de tales datos; máxime cuando los procesos de captación, retención y ulterior conservación responden a procesos automáticos; que como tales podrían mostrarse más vulnerables a accesos ilícitos o abusivos (apt. 55, STJUE; 2014).

La proporcionalidad que atañe igualmente a los plazos de conservación de datos, muestra un excesivo margen de discrecionalidad que es permitido en la normatividad mexicana, en cuanto a que obliga a las compañías de telecomunicaciones a conservar los datos por un periodo de dos años exactos, sin atender al caso concreto, tasando la injerencia en los datos, sin ponderar la intensidad de la injerencia dependiendo del caso concreto.

Los plazos que no son sometidos a criterio objetivo alguno que permitiera ponderar la mayor intensidad de la injerencia de unos respecto de otros, en función de la categoría de los datos relacionados; proponiendo para ello, basarse en su posible utilidad según criterios de valoración del objetivo perseguido o de las personas concernidas (Laínz, 2014: 1526).

La importancia de la aplicabilidad de los principios y su observancia en los textos constitucionales, es determinante para definir los niveles de democratización de una sociedad que se traduzca en un beneficio para los ciudadanos, a efecto de

protegerlos frente a abusos de autoridad que vean mermados sus derechos fundamentales, pues como menciona Maritza Rodríguez, "Los Principios Necesario y Proporcional proveen la base principal para evaluar si las prácticas de vigilancia e interceptación de comunicaciones de un estado se ajustan a los estándares internacionales de derechos humanos" (*necessaryandproportionate.org*; Rodríguez, 2013:7).

3.3.1 LA AUTORIZACION JUDICIAL Y AUTORIDAD COMPETENTE PARA LA INTERVENCIÓN EN RELACIÓN CON EL DERECHO A LA INVOLABILIDAD DE LAS COMUNICACIONES.

El requisito de la autorización judicial, a decir de algunos autores como es el caso de Karitza Rodríguez (2013:16), es incluso considerada como un principio en sí mismo y que está relacionado estrechamente con el principio del debido proceso judicial:

Como resultado, la vigilancia de las comunicaciones debe ser autorizada formalmente caso por caso por una autoridad judicial independiente e imparcial, con acceso a los conocimientos tecnológicos apropiados. Esto asegura que un estado no está actuando más allá de su facultad legal y que se dé la debida consideración a los derechos humanos de los afectados por la vigilancia. Se asegura que los derechos humanos del sujeto sean protegidos en cada etapa del proceso de autorización. Al exigir que el estado justifique cada acto de vigilancia ante un juez, este principio garantiza que la vigilancia de las comunicaciones se lleve a cabo únicamente cuando la necesidad y cuando el efecto en los derechos humanos es eliminado o se reduce al mínimo (Rodríguez, 2013:17).

Otro aspecto importante durante el desarrollo del proceso de vigilancia al que alude la autora, es el derecho con que debería contar el sujeto de la vigilancia de “impugnar la acción deseada por el estado”, el cual está estrechamente vinculado al principio de debido proceso.

En México, dichos principios se cumplen parcialmente, ya que en el caso de la intervención de comunicaciones privadas, así como en el acceso y análisis de la información que se encuentre almacenada en los teléfonos celulares, sí se requiere de autorización judicial sin embargo, en el caso de la obtención de datos de localización resulta diferente, pues la Suprema Corte de Justicia de la Nación ha concluido que no se requiere autorización judicial para la vigilancia de datos de localización en tiempo real, paradójicamente a lo que sostiene la propia Constitución en el sentido de proteger los metadatos de las comunicaciones.

En este sentido la Suprema Corte, mediante la Contradicción de Tesis 194/2012, establece que la falta de autorización judicial para la intervención de datos almacenados en un teléfono, implica una violación al derecho a la inviolabilidad de las comunicaciones:

En términos del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial Federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son producto de la evolución tecnológica, incluso del teléfono celular [...], deben protegerse por el derecho fundamental de la inviolabilidad [Además el acceso y análisis de los datos contenidos en un teléfono móvil sin contar con una autorización judicial constituye una violación al derecho a la inviolabilidad de las comunicaciones (SCJN, Contradicción de tesis 194/2012).

Así mismo, se plantea un déficit de la normatividad mexicana en el sentido de no precisar criterios objetivos al definir las autoridades competentes para tener acceso a los datos objeto de conservación y cuales autoridades son las facultadas para el uso en apego a la finalidad perseguida y hasta qué punto serían limitadas

dichas autoridades por las que autorizan a fin de evitar violaciones a los derechos humanos.

...al tratarse de datos personales, la solicitud de estos por parte de una autoridad, es un acto de molestia para el individuo. La LFTR se refiere a “autoridades competentes” como aquellas que tienen a su cargo la seguridad, la procuración y la administración de justicia. Ello significa que cualquiera de éstas, sin que medie mandato judicial, podrá solicitar los datos personales de cualquier usuario (Calero, 2014: s/p).

El artículo 190, fracción I de la ley Federal de Telecomunicaciones y Radiodifusión, obliga a las compañías de telecomunicaciones a “colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real de los equipos de comunicación móvil”, concediendo poder a las “agencias de seguridad” o “instancias de administración de justicia, las cuales no se encuentran definidas ni en la LFTR, ni en ninguna otra ley.

No obstante lo anterior, en el año 2016, la Suprema Corte de Justicia determinó como aquellas autoridades facultadas para acceder a los datos de ubicación son los Fiscales Federales y estatales, la Policía Federal y el Centro de Investigación y Seguridad Nacional (CISEN), por lo que aumenta en número las mencionadas por el artículo 303 del Código Nacional de Procedimientos Penales, Sin embargo la imprecisión y la contrariedad continúa en todos los textos en los cuales se encuentran dispersas estas disposiciones sobredimensionando el desempeño cuestionable de todas estas autoridades.

3.4 LA AUTODETERMINACION INFORMATIVA COMO BIEN JURÍDICO PROTEGIDO POR EL DERECHO A LA PROTECCION DE DATOS PERSONALES Y SU RELACIÓN CON LA INTIMIDAD.

Como nos explica Cerda Silva (2003), la intimidad surge como una reacción frente a las ilegítimas intromisiones de la prensa en la vida de las personas, el boyante desarrollo de los medios de comunicación de masas evidenció la insuficiencia del derecho a la intimidad como simple expresión de ámbitos de exclusión a la injerencia de terceros e hizo patente la necesidad de ampliar la protección que brindaba a su titular, para permitir que este pudiese disponer de control sobre la información personal que le compete.

En el mismo sentido, Pérez Luño sostiene que el catálogo de los derechos fundamentales no reviste un carácter estático y, así como a los derechos de primera generación con un marcado sello liberal que imputaba un rol pasivo al estado, se adicionó una segunda generación que demandaba un quehacer de impronta del Welfare State, a estos se ha sumado una tercera generación de derechos para la protección de los consumidores, del medio ambiente y de los propios datos personales (2002: 345-349).

La autodeterminación informativa como conceptualización subjetiva de los derechos de la privacidad e intimidad y como bien jurídico de la protección de datos, faculta al individuo a decidir por sí mismo en qué momento y dentro de qué límites desea revelar datos pertenecientes a su vida.

La autodeterminación informativa es la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos (Viggiola,1999:s/p).

Dicha autodeterminación presupone -como lo ha expuesto el Tribunal Constitucional Federal Alemán en su sentencia de 15 de diciembre de 1983 (ref. BvR 209/83)- que se le conceda la libertad de decisión sobre las acciones que vaya a realizar, o en su caso a omitir, qué, cuando, y con qué motivo se sabe algo sobre él, lo que no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de los ciudadanos, con la salvedad de que el ejercicio de esa

autodeterminación informática no es una facultad absoluta, pues el individuo tiene que aceptar, en principio, determinadas limitaciones en aras del interés general o preponderante de la comunidad. “Este concepto es identificable con una esfera de disponibilidad plena del individuo, siendo que será el mismo quien determine lo que debe o no estar reservado al conocimiento externo” (Nahabetián, 1984).

El fundamento quinto de la Sentencia del Tribunal Constitucional Español No. 292/2000 determina que, más allá del derecho a la intimidad reconocido como fundamental por la legislación española, adquiere una nueva dimensión mediante el derecho al control sobre los datos propios de la persona mediante la llamada “libertad Informática”, considerada como el derecho a controlar el uso de los mismos y que comprende entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos a aquél legítimo que justificó su obtención. (SSTC 11/1998, FJ5, 94/1998, FJ4).

De acuerdo al propio Tribunal Constitucional, el derecho a la protección de datos alcanza no solamente los datos de carácter personal, es decir, no solo los relativos a la intimidad o privacidad de una persona, sino todos aquellos datos, incluso públicos, que permitan la identificación de una persona y que resulten útiles para la confección de un perfil ideológico, racial, sexual, económico etc. o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

La privacidad es considerada un requisito previo a la inclusión en los procesos de participación democrática de un país. La ausencia de límites en el tratamiento de los datos personales de los ciudadanos les coloca en riesgo de su libertad personal, y más aún, en peligro de su libertad y su seguridad” (Nahabetián Brunet; 2011).

La autodeterminación informativa surge de la necesidad de protección del individuo frente al tratamiento de sus datos personales por parte de terceros, bajo el riesgo no solamente de ver vulnerada su intimidad sino debido a la vulnerabilidad de ser afectado por la comisión de delitos producto de la retención de datos por

parte de terceros a los que le han sido entregados para la prestación de un servicio.

Siguiendo a Marecos, se pueden distinguir dos sectores enfrentados con relación a la discusión de la autodeterminación informativa como derecho fundamental, uno de dichos sectores rechaza la consideración de la autodeterminación informativa como derecho fundamental argumentando que la reformulación del derecho a la intimidad es suficiente para ofrecer garantías individuales adecuadas; el otro sector sostiene, por el contrario, la idea de la necesidad de admitir la existencia de un nuevo derecho fundamental, cuya construcción se asienta sobre el reconocimiento al individuo de unas facultades de disposición y decisión respecto a sus propios datos personales. Desde esta perspectiva, podríamos considerar que la intimidad se atañe a un comportamiento pasivo por parte del titular de tal derecho frente a los poderes públicos y particulares y en el caso de la autodeterminación informativa, hablamos de un comportamiento activo frente al Estado y particulares en el tratamiento de los datos personales concretamente (Marecos, 2013:2).

Garriga Domínguez, por su parte, defiende la autonomía del derecho a la autodeterminación informativa, argumentando la existencia de cruciales diferencias entre este derecho y el derecho a la intimidad, así, afirma que este último se trata de un derecho ligado a la dignidad humana, caracterizado por un eminente contenido negativo para salvaguardar del conocimiento ajeno la parte de nuestra vida – la más cercana- personal y familiar. El derecho a la autodeterminación informativa tiene un objeto y un contenido diferente, su ámbito es más amplio y los elementos que lo componen más complejos (Garriga, 2004:18; citado por Marecos).

Nos referimos a dos distintos objetos jurídicos protegidos dentro del sistema de protección de datos personales, si bien ambos devienen de la intimidad, uno abarca una faceta más individual y el segundo más social, o colectiva, es decir, el individuo en sus relaciones sociales.

Navarro Jiménez nos describe la relación que se ha desarrollado en los últimos tiempos entre el derecho y la informática, derivado de lo cual surge el derecho informático y la informática jurídica, considerando que la protección de datos es un tema que aborda el derecho informático, cuyos estudios van encaminados a la salvaguarda de la información que no es propia y que obra en archivos públicos, bajo el riesgo de que su divulgación sea nociva para nuestra imagen, honor o intimidad, dicha protección considera el autor es entendida mediante el concepto doctrinal de derecho a la autodeterminación informativa que no es otra cosa que el ejercicio de la libertad informática (ordenjuridico.gob.mx, consultado el 24 de enero del 2017, p.20).

Lucas Murillo de la Cueva considera que el bien que tutelan los sistemas de protección de datos, no es la intimidad “física”, sino la intimidad informativa o autodeterminación informativa, según este autor no caben dudas razonables que impidan hablar de la existencia de este nuevo derecho, el cual se diferencia del derecho a la intimidad (Murillo de la Cueva, 1990:19; citado por Marecos).

La Ley Federal de Protección de Datos Personales en posesión de los particulares en México, en su artículo 8 establece: “Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la ley”.

En México, al derecho a la intimidad, no obstante, no ser considerado como derecho fundamental constitucionalmente, se le vincula estrechamente con el derecho a la autodeterminación de la información, como lo determina la Suprema Corte de Justicia de la Nación en la tesis I.3º.C.695 C, la cual establece al respecto:

DERECHO A LA INTIMIDAD, SU OBJETO Y RELACION CON EL DERECHO A LA AUTODETERMINACION DE LA INFORMACIÓN. Los textos constitucionales y los tratados Internacionales de derechos humanos recogen el **derecho a la intimidad** como una manifestación concreta de la separación entre el ámbito

privado y el público. Así el derecho a la intimidad se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sean simples particulares o bien los poderes del Estado; tal derecho atribuye a su titular el poder de resguardar ese ámbito reservado para el individuo para sí y su familia; así mismo garantiza el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la **autodeterminación de la información** que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quien y bajo qué condiciones puede realizar esa información. En este contexto el derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir obligación de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; así mismo el Estado a través de sus órganos debe adoptar todas las medidas tendientes a hacer efectiva la protección de éste derecho (Amparo en revisión 73/2008:1253).

En México podemos considerar que la vida privada o intimidad está protegida de forma múltiple a través de derechos como la inviolabilidad de las comunicaciones; el derecho a la protección de datos o el derecho del habeas data, el cual protege el derecho de todo individuo a conocer la información que guarda sobre su persona.

La normativa sobre protección de datos personales, cuenta con una tutela más dinámica que estática y, más allá de garantizar la intimidad de las personas, cuenta con su propio bien jurídico consistente en la autodeterminación informativa, mediante la cual faculta al individuo bajo su protección, a controlar la información que le concierne en el tratamiento frente al tratamiento automatizado de sus datos personales.

3.5 BREVE REFERENCIA AL EL SISTEMA DE RETENCION DE DATOS EN EL SISTEMA JURÍDICO ESPAÑOL.

En la actualidad, en la comunidad europea, el derecho a la protección de datos de carácter personal está reconocido como derecho fundamental por el artículo 8º de la Carta de Derechos Fundamentales de la Unión Europea celebrada en Niza el 7 de diciembre del 2000. La carta reconoce el derecho a la protección de datos como independiente del derecho a la intimidad y explica como contenido de dicho derecho: "Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan... Esos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación" (www.europarl.europa.edu, 2000).

En Europa, la Directiva 24/2006/EC, ha sido puesta en la mesa de debate debido a la contraposición que pretende, por un lado generar una seguridad anhelada socialmente producto de los atentados terroristas de Madrid y Londres; sin embargo ha sido objeto de múltiples cuestionamientos que nos llevan al ejercicio de ponderación entre dicha seguridad, frente a la protección del derecho de datos personales.

Como nos explica el analista Ponce Rodríguez: "acostumbrados como estamos a que nuevas tecnologías alteren nuestra vida cotidiana y contribuyan a la invasión de nuestra intimidad, no nos debe extrañar que el legislador nacional y el comunitario se ocupen con determinación de regular el uso de los datos personales en una sociedad cada vez más tecnológica. Precisamente esta preocupación social y política por un uso potencialmente nocivo de los avances tecnológicos en comunicaciones electrónicas es lo que ha impulsado la aprobación de la Directiva 24/2006/CE sobre la conservación de datos relacionados con la prestación del servicio público de telecomunicaciones" (Ponce, 2016, p.71-77).

El primer antecedente se registra en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento y libre circulación de datos personales; posteriormente en el año 2002 la Unión Europea, aprobó la Directiva 2002/58/CE relativa a la conservación de datos como parte de la lucha contra el terrorismo y el crimen organizado, considerando este último como un elemento crucial para tal efecto, obligando a todas las compañías de servicios de Telecomunicaciones de todos los Estados miembros de conservar los datos relativos a las comunicaciones de los usuarios a quienes prestan servicios, así como a costear el almacenamiento de millones de datos de usuarios, con el fin de colaborar en las investigaciones criminales de las autoridades nacionales de cada país.

En el año 2004, cuatro Estados miembros de la Unión Europea (Francia, Irlanda, Reino Unido y Suecia), presentaron un proyecto de decisión sobre la investigación y enjuiciamiento de determinados delitos graves sobre el almacenamiento y procesamiento de datos por parte de los proveedores de servicios de comunicaciones electrónicas públicas (CNS/2004/0813), Sin embargo fue rechazado por el Parlamento Europeo.

El 21 de septiembre de 2005, la Comisión Europea presentó una propuesta de Directiva sobre conservación de datos de tráfico que fue finalmente aprobada el día 15 de marzo de 2006. Se trata de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones.

La Directiva exige a los Estados miembros que garanticen que los operadores de telecomunicaciones conserven los datos de tráfico y de localización, generados o tratados por los proveedores de red y de servicios, a efectos de la investigación, detección y persecución de los delitos graves, tal como se definan en el derecho nacional. Los datos deben conservarse durante un mínimo de seis meses y un máximo de dos años (a decidir por los Estados miembros al incorporar la Directiva a sus ordenamientos jurídicos nacionales).

En la Directiva 2006/24/CE se propone armonizar las disposiciones de los estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal y como se definen en la legislación nacional de cada Estado miembro. (Art. 1.1).

El artículo 1.2 establece que la presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas o jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

El artículo 1.1. Del proyecto de la Directiva, hace referencia a “delitos graves” especificando “como el terrorismo y la delincuencia organizada” , pero el texto aprobado lo suprime.

De acuerdo al artículo 1.2 de la Directiva, los sujetos obligados son los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de telecomunicaciones. Los datos que se retienen son respecto de personas físicas y jurídicas.

El 2.2.b se refiere al “usuario” como aquella persona física o jurídica que utilice un servicio de telecomunicaciones electrónicas de acceso público.

De acuerdo a los artículos 4 y 8 se establece que pueden ser destinatarios de los datos solamente “las autoridades nacionales competentes”.

En cuanto al objeto de conservación, el art. 5 estipula que serán objeto de conservación los datos necesarios para: i) rastrear e identificar el origen de una comunicación; ii) identificar el destino de una comunicación; iii) identificar la fecha, y duración de una comunicación; iv) Identificar el equipo de comunicación de los

usuarios o lo que se considera ser el equipo de comunicación; vi) identificar la localización del equipo de comunicación móvil.

En el año 2011, la Comisión de la UE publicó un informe de evaluación, tal y como se requiere en el artículo 14 de la Directiva. El informe concluía que la conservación de datos ha demostrado su utilidad en las investigaciones penales contra el daño causado por la delincuencia organizada y el terrorismo, pero también incluía conclusiones en el sentido de generar críticas sobre el diseño de la Directiva, en particular por lo que se refiere al equilibrio entre seguridad y respeto a la intimidad de los ciudadanos de la UE.

No obstante lo anterior, en el año 2014, El Tribunal de Justicia de la Unión Europea determinó en su sentencia en los asuntos acumulados C-293/12 y C-594/12, la anulación de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, al considerar que constituye “una injerencia de gran magnitud y especial gravedad” en: “La injerencia amplia y especialmente grave de la directiva en los derechos fundamentales de que se trata, no está suficientemente regulada para garantizar que dicha injerencia se limite efectivamente a lo estrictamente necesario”, considera “la directiva abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objeto de lucha contra los delitos graves”.

Así mismo, se argumenta que la directiva “no fija ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes únicamente tendrán acceso a los datos y podrán utilizarlos para prevenir, detectar o reprimir penalmente, delitos que por la magnitud y la gravedad de la injerencia en los derechos fundamentales en cuestión, puedan considerarse suficientemente graves para justificar tal injerencia”, estima que el acceso a los datos no se supedita al control previo de un órgano jurisdiccional o de un organismo administrativo autónomo.

El Tribunal ha considerado que la directiva no contiene garantías suficientes que permitan asegurar una protección eficaz de los datos contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos de los datos. “En particular autoriza a los proveedores de servicios de internet a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican y no garantiza la destrucción definitiva de los datos al término de su periodo de conservación”.

La sentencia censura en su contenido la posibilidad de que los datos puedan salir del territorio de la Unión Europea (Sentencia de la Gran Sala, Pleno del Tribunal de Justicia de la Unión Europea de 8 de Abril de 2014, recaída en los asuntos C-293/12 y C-594/12).

El 18 de mayo del 2011, Las Autoridades Europeas de protección de Datos a través del grupo de Trabajo del Artículo 29, aprobaron un Dictamen sobre la incidencia y los riesgos para la privacidad de los “Servicios de geolocalización en dispositivos móviles inteligentes”.

El Dictamen analiza los riesgos de los servicios de geolocalización para la privacidad de sus usuarios, el marco jurídico aplicable y las garantías que los proveedores de servicios de geolocalización en dispositivos móviles deben cumplir; Destacan que los datos de localización de *smartphones* pueden revelar detalles íntimos sobre la vida privada de su propietario y permitir obtener patrones de conducta del titular del dispositivo para crear perfiles; de forma predeterminada, los servicios de localización deben estar apagados y su activación requerirá el consentimiento informado y específico del usuario; Los interesados deben poder retirar su consentimiento de manera fácil, sin ningún tipo de consecuencias negativas para el uso del dispositivo (Opinión 13/2011 on Geolocalization services on Smart mobile devices).

En España el artículo 18 de la Constitución establece:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Con base en lo anterior, los derechos a la protección de datos personales y a la privacidad en la legislación española, tienen un rango de derechos fundamentales reconocidos por la propia ley fundamental, en virtud de lo cual son garantizados por medio de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, que tiene por objeto como lo señala es su artículo 18.4, garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar.

Cabe señalar que esta ley derogó a la Ley Orgánica 5/1992, de 29 de octubre, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

La ley Orgánica de Protección de Datos establece en su artículo 4.1 el principio de proporcionalidad en el tratamiento de los datos, referente a que dichos datos sean adecuados, pertinentes y no excesivos en relación con el ámbito, así como las finalidades para las que se hayan obtenido.

Así mismo, en su Título IV, artículo 35, contempla al organismo de Derecho Público denominado Agencia de Protección de Datos, al cual define como un “Ente de Derecho Público con personalidad jurídica propia y con capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones”.

Dentro de sus funciones se establece: el velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y

cancelación de datos que almacenen datos personales (Art. 37.) en función de su tipología.

Su Reglamento de desarrollo es el Real Decreto 1720/2007, del 21 de diciembre, que determina las medidas técnicas de seguridad a implementar en los sistemas de información.

El Real Decreto 424/2005 del 15 de abril, en su artículo 2, recoge la definición de Geolocalización, establecida por la Directiva 2002/58/CE, la cual ha sido mencionada con antelación como “cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponible para el público”. Aprobándose de igual manera el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Con fecha 18 de octubre del 2007, se publicó la ley 25/2007 emitida por la Jefatura de Estado, relativa a la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la cual consta de 10 artículos agrupados en tres capítulos, estableciendo en el Art. 4 del Capítulo II: “los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta ley, se conserven de conformidad con lo dispuesto en ella..” (Agencia Estatal Boletín del Estado).

La mencionada ley establece que tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación hasta por el periodo de doce meses, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales (Art. 1.).

La ley de Conservación de datos generados o tratados en relación con la prestación del servicio de telecomunicaciones electrónicas de acceso público o de redes públicas de telecomunicación, constituye la transposición de la Directiva 24/2006/CE de la Unión Europea al ordenamiento español que busca imponer a los prestadores de servicios de comunicaciones electrónicas y de redes públicas de comunicación, como es el caso de telefonía fija o móvil o por internet, la obligación de conservar una serie de datos de sus usuarios, generados con motivo de la prestación y uso del servicio .

Esta ley se complementa con la Ley General de Telecomunicaciones que se adapta mediante la modificación 32/2003 del 3 de noviembre, en lo relativo al secreto de las comunicaciones, obligando a la identificación de los usuarios de las tarjetas de prepago quienes con anterioridad permanecían anónimos.

De acuerdo con la legislación, la finalidad de dicha conservación se traduce en que las autoridades policiales puedan solicitar a los operadores los datos de los usuarios, previa autorización judicial y utilizarlos durante las investigaciones, prevención y persecución de delitos.

Es importante destacar que la Directiva 24/2006/CE regula la conservación de datos con un carácter preventivo y no reactivo (mediante previo mandato judicial), al referirse a la conservación de datos respecto de todos los usuarios de los servicios, es decir, sin necesidad de que existan sospechas de antijuridicidad.

En este caso es importante hacer alusión a la Ley de Enjuiciamiento Criminal del Estado Español que en su artículo 579 determina, que el levantamiento del secreto de las comunicaciones se produce siempre con posterioridad a los hechos, por lo que, es necesario aportar ante el juez “indicios para obtener por estos medios, el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa”; por lo que solamente bajo dichas circunstancias, el juez podrá interceptar las comunicaciones por el término de hasta tres meses, prorrogables por iguales periodos.

No obstante la arbitrariedad que pueden generar tales determinaciones, como es la vulneración de los derechos fundamentales y afectación a la protección de datos personales y el derecho a la intimidad, el legislador comunitario considera que la cesión de los datos a las autoridades policiales para la persecución de los delitos solamente podrá realizarse caso por caso, cuando exista una resolución judicial específica que ampare tal cesión, lo cual no implica que se garanticen los derechos fundamentales en cuestión.

Otro aspecto importante (de carácter económico), que deviene de la Directiva, es el relativo al hecho de que, para cumplir con esa obligación de conservación, los operadores deberán almacenar millones de datos relativos a las comunicaciones realizadas por los usuarios, lo cual ha generado una enorme inconformidad por parte de las compañías de telecomunicaciones.

Ahora bien, atendiendo a cuestiones de la ordenación del sector, resultan de competencia nacional los tratamientos efectuados en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario, como son las previstas en los artículos que integran los títulos V y VI del tratado de la Unión Europea y en cualquier caso, el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del estado en materia penal, lo anterior implica que el desarrollo nacional puede producirse no solo contrariamente sino dentro de un marco totalmente estatal.

Bajo la óptica anteriormente descrita, la anulación de la Directiva 24/2006/CE no afecta automáticamente la validez de la ley 25/2007, de 18 de octubre de Conservación de datos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, por lo que el contenido de la primera y aplicabilidad continúan subsistentes dentro de la jurisdicción del Estado Español.

Así entonces, encontramos que si bien el ordenamiento jurídico español en materia de conservación de datos transpone el contenido de la Directiva 24/2006/CE mediante la Ley de Conservación de datos 25/2007, de 18 de octubre, su aplicabilidad al territorio español, atendiendo a la ley de enjuiciamiento criminal,

regula un tratamiento y conservación de datos personales de manera reactiva, esto es, previa una resolución de un juez que considere dicha intervención o conservación como factor indispensable para la comprobación de una conducta antijurídica y no como lo establece la Directiva en cuestión de manera preventiva. Por lo que obliga a los operadores de Telecomunicaciones a conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación hasta por el periodo de doce meses, así como a la cesión de dichos datos a los agentes facultados, siempre que les sean requeridos, previa autorización judicial.

En cuanto a la resolución del Tribunal Europeo en el sentido de anular la Directiva 24/2006/CE; el Estado Español no está obligado a acatarla de manera automática en virtud de que conforme al Tratado de la Unión Europea, no es aplicable en estos casos el derecho comunitario, quedando bajo la competencia del propio Estado español contradecir o bien establecer su propia legislación al respecto.

En cuanto a las medidas de seguridad y control por autoridad competente respecto de los datos conservados por mandato de la ley 25/2007, Rodríguez Laínz, considera que la legislación española definitivamente sí garantiza dichos estándares de protección, por lo que, aludiendo al artículo 8.1 de la normativa sobre Protección de Datos de carácter personal, determina la obligación de las operadoras de "...identificar al personal especialmente autorizado para acceder a los datos objeto de esta ley, adoptar las medidas técnicas y organizativas que impiden su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados (Rodríguez, 2014:1526).

3.6 ANÁLISIS DE LOS ARTICULOS 189 Y 190 FRACCIONES I, II Y III DE LA LFTR.

Los artículos 189 y 190 fracción I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión están incluidos en el título octavo denominado: De la Colaboración con la Justicia referente a las obligaciones en Materia de Seguridad y establece:

Art. 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

Los titulares de las instancias de seguridad y procuración de justicia, designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

Art. 190. Los concesionarios de telecomunicaciones y en su caso, los autorizados deberán:

- I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación aplicable.

El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta ley con dichas autoridades sea efectiva y oportuna.

- II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad que permitan identificar con precisión los siguientes datos:

- a) Nombre, denominación o razón social y domicilio del suscriptor;

- b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos) servicios suplementarios (incluidos el reenvío o transferencia de la llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados).
- c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario como en la modalidad de líneas de prepago;
- d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como del servicio de mensajería o multimedia;
- e) Además de los datos anteriores se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
- f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;
- g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y;
- h) La obligación de conservación de datos, comenzará a contar a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en el sistema que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar esos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso la entrega de la información a las autoridades competentes se hará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

La solicitud y entrega en tiempo real de los datos referidos en este inciso, se realizará mediante los mecanismos que determinen las autoridades a que se

refiere el artículo 189 de esta ley, las cuales deberán informarse al instituto para los efectos de lo dispuesto en el párrafo tercero, fracción I del presente artículo.

Los concesionarios de telecomunicaciones y en su caso los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.

Sin perjuicio de lo establecido en esta ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios, o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares;

III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta ley, que así lo requieran conforme a sus atribuciones, de conformidad con las leyes aplicables.

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

Estos artículos omiten especificar cuál es el propósito u objetivo de la retención de los datos personales, por lo que no establecen dichas causas, no obstante que se puede deducir que es la persecución de los delitos omiten describir los tipos penales considerados como “graves”, en cuyo caso procede dicha retención, lo anterior constituye un atentado a los principios de finalidad y proporcionalidad.

...en el caso que nos ocupa, los artículos 189 y 190 fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión, representan un problema, al menos, en términos de la finalidad y de la proporcionalidad. La LFTR es omisa en cuanto al objetivo que busca al tener acceso a los datos personales de los usuarios. Si desprendemos que es la persecución de los

delitos, la ley debería señalar a cuáles de estos se refiere específicamente (Calero, 2014: s/p).

En observancia al texto del artículo 189, en el párrafo que apunta a “la autoridad competente” como aquella que tiene a su cargo la seguridad y la procuración de justicia, se deduce que, toda autoridad que quede incluida dentro de esta materia puede, sin que medie autorización judicial, incluso, interceptar los datos personales de los individuos.

Como parte de todo procedimiento legal y con base en el principio de autoridad Judicial competente, se hace imprescindible que las autorizaciones de vigilancia sean tomadas por una autoridad capacitada en la materia, independiente e imparcial, lo cual garantiza al sujeto de la intervención, que un estado esté actuando dentro de los límites que la ley le impone y dentro de sus facultades para la observancia de los derechos humanos.

En torno a las “autoridades competentes” a que se refiere artículo 189, Murray y Zuckerman consideran que:

El lenguaje utilizado en el artículo 189 de la LFTR les da poder suficiente como para usar herramientas de vigilancia encubierta y que este poder no necesita quedar detallado en ninguna norma. Por ejemplo “la unidad de inteligencia financiera” de la Secretaría de hacienda y Crédito Público entra en la categoría de “instancias de seguridad” según el artículo 189 y un documento que no es la ley formal y materia conocido como “La guía de Colaboración” [... además existen reportes que afirman que autoridades como el Instituto Nacional Electoral pueden haber enviado este tipo de pedido con el objetivo de acceder a los datos personales de usuarios de servicios de telecomunicaciones (Murray y Zuckerman, 2015:s/p, citados por Rodríguez, 2013:33).

El artículo 190 en sus tres primeras fracciones establece las obligaciones de los concesionarios de colaborar con la geolocalización de los equipos de comunicación móvil, así como de conservar un registro y control de

comunicaciones con una serie de datos del usuario, así como de entregar dicho registro en caso de que la autoridad se lo solicite. Al respecto Fernando García (2016), apunta: que el lenguaje utilizado en el artículo 190 sección III es altamente ambiguo en cuanto a las autoridades que están facultadas para acceder a los datos retenidos. Este artículo autoriza la entrega de datos retenidos a “las autoridades a que se refiere el artículo 189 de esta ley que así lo requieran”. El artículo 189 de la LFTR crea la obligación de las compañías de telecomunicaciones y proveedores de servicios en línea, de aplicaciones y de contenidos, de atender “todo mandamiento por escrito, fundado y motivado de la autoridad competente”, y se menciona, entre otros, a las “instancias de seguridad y procuración de justicia” sin establecer de manera clara cuáles son las autoridades que entran en esas categorías.

Así mismo, la conservación hasta por dos años a que se refiere el artículo 190, restringe el derecho de cancelación que tienen los usuarios de los servicios de telecomunicaciones al imponer a los concesionarios la no cancelación de los mismos durante ese periodo, por lo que la Ley Federal de Telecomunicaciones y Radiodifusión a través de dicha disposición omite especificar las causas de excepción a la cancelación, tal y como lo dispone el artículo 16 constitucional y que proceden por causas de seguridad nacional, de orden público, seguridad y salud públicas.

Tomando en consideración los argumentos de la Suprema Corte de Justicia de la Nación en el sentido de que los datos de tráfico y que son los enumerados exhaustivamente en el artículo 190, forman parte de las comunicaciones estaríamos en presencia de una violación al derecho a la inviolabilidad de las comunicaciones.

Por lo que hace al principio de proporcionalidad, que es el que prevé que sólo serán objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido, es posible afirmar que la LFTR impone la recolección de más datos de los que

necesitaría la autoridad para lograr el objetivo de perseguir delitos (fin que, como ya se dijo, además, no está señalado). Vale la pena preguntarse si es necesario recabar los más de veinte datos que exige la ley para que las autoridades competentes cumplan su función (Calero, 2014: s/p).

Con relación a los datos de tráfico es importante dejar sentado que la fracción II del artículo 190 de la ley Federal de telecomunicaciones, no obstante que describe una lista exhaustiva de datos a conservar por parte de las compañías de telefonía móvil, la cual resulta por cierto excesivamente amplia, no especifica cuáles son los datos que las compañías telefónicas deben conservar para efectos de transferir para causas criminales, por lo que de acuerdo a la teoría del mosaico cualquier dato por irrelevante que resulte puede ser determinante para definir el perfil de un individuo.

Otro aspecto de gran relevancia es la omisión de los artículos 189 y 190 en sus distintas fracciones, es la observancia del principio de previsibilidad como parte del proceso de conservación de datos, la existencia de un recurso efectivo para inconformarse con las infracciones cometidas por las “autoridades competentes” en el desarrollo del mismo al ver vulnerados sus derechos humanos, ya que como considera Maritza Rodríguez:

El cumplimiento de este principio, por lo tanto, requiere que cada estado prohíba o limite la vigilancia de las comunicaciones acompañadas de una sanción contra el gobierno y la compensación de personas afectadas (Rodríguez, 2013:21).

3.7 LA POSTURA DE LOS ORGANOS GARANTES ANTE LA RETENCIÓN DE DATOS PERSONALES EN PODER DE LAS COMPAÑÍAS DE TELEFONÍA CELULAR

En la actualidad México cuenta con once órganos garantes reconocidos legalmente, lo cual, de acuerdo a Calero Sánchez (2014), representa que el legislador demuestra desconfianza de la labor del Ejecutivo, por lo que ha determinado que materias como la evaluación de la educación y de los programas sociales, las telecomunicaciones, la competencia económica, la procuración de

justicia, dejen de ser parte de la administración pública, para ser realizadas por los órganos con autonomía, siendo muchos de ellos garantes de derechos fundamentales como es el caso del IFAI, (actualmente INAI Instituto de Acceso a la Información pública), el cual tiene a su cargo la obligación de garantizar los derechos de acceso a la información y protección de datos personales.

Bajo estos términos, la legislación dota a los órganos garantes de autonomía, presupuesto y herramientas legales como son las figuras jurídicas consistentes en la acción de inconstitucionalidad y la controversia constitucional.

El artículo 105 de la Constitución determina que tienen la facultad de interponer la acción de inconstitucionalidad: los senadores, Diputados Federales y Diputados locales, el Ejecutivo Federal, el Fiscal Federal de la República, los Partidos Políticos y los órganos garantes como son, La Comisión Nacional de Derechos Humanos y el Instituto Nacional de Acceso a la Información Pública, a través de la Procuraduría General de la República o con el aval del 33% de los integrantes de cualquiera de las Cámaras.

Así, la Suprema Corte de Justicia de la Nación es la facultada por las leyes para resolver la inconstitucionalidad de los artículos 189 y 190 en sus fracciones I, II y III, por lo tanto el INAI como la CNDH como órganos garantes están autorizados para solicitar a la Suprema Corte que resuelva sobre dicha materia en el caso de que se vean violentados derechos fundamentales.

Existen posturas sobre la falta de autonomía de los órganos garantes como es el caso de la analista Calero Sánchez, quien considera que en muchos casos, dichas Instituciones se erigen como mero “defensor de las políticas públicas del Ejecutivo”, lo anterior, tomando en cuenta el proyecto de dictamen de reforma constitucional en materia de transparencia y en el cual las comisiones responsables de la Cámara de Diputados señalaron que los organismos constitucionales autónomos fueron creados para coadyuvar con las instituciones del Estado, y estos han evolucionado para convertirse en mecanismos que dan solución a las diferentes problemáticas que enfrenta la sociedad; aunado a ello tienen dentro de

su naturaleza la creación de lazos de confianza entre la sociedad y el accionar gubernamental (Calero, 2013: s/p).

Inicialmente debemos mencionar que La Suprema Corte de Justicia de la Nación, en el año de 2014, se pronunció al resolver la acción de inconstitucionalidad 32/2012, Interpuesta por la Comisión Nacional de Derechos Humanos, deliberando con una mayoría de 8 votos, a favor de una geolocalización de los equipos de comunicación móvil, vinculados a delitos considerados graves, que no se realice de un modo irrestricto y con desapego a los preceptos constitucionales (SCJN, 32/2012/ <http://www2.scjn.gob.mx>).

Las primeras reacciones por parte de los teóricos ante la implementación de la geolocalización como herramienta de Procuración de Justicia, tuvo sus primeros cuestionamientos, como nos explica Macedo:

Dicha geolocalización no es permisible en todos los casos porque su autorización requiere de una justificación (de acuerdo con el caso en cuestión) o de un freno de su uso, dadas las limitaciones establecidas. El que el Estado esté obligado a controlar el crimen, a fin de proteger a la sociedad, no implica una contradicción respecto a los derechos humanos, por el contrario son dos tareas relevantes y conciliables en una Democracia Constitucional (Macedo, 2015:163).

A partir de la promulgación de la Ley Federal de Telecomunicaciones y Radiodifusión el 14 de julio del 2014, 219 organizaciones civiles se posicionaron para pedir acción de inconstitucionalidad en contra de los artículos 189 y 190 fracciones I, II y III, argumentando violaciones a la privacidad y protección de datos personales, sin embargo con cuatro votos a favor y tres en contra, el entonces Instituto Federal de Acceso a la Información Pública, (IFAI actualmente INAI) resolvió uno de los asuntos de mayor importancia de su vida institucional, al no ejercer la acción de inconstitucionalidad en contra de los artículos en análisis ante la Suprema Corte de Justicia de la Nación, facultad que entre otras le fue otorgada a raíz de la reforma constitucional en materia de acceso a la información con

relación a la promulgación de leyes o tratados internacionales que vulneraran los derechos de acceso a la información y protección de datos personales.

Dicha decisión debilitó considerablemente la confianza Institucional con que dicho organismo había sido creado, socavando el reconocimiento social e internacional de la política de transparencia y acceso a la información en México. Como reconoce Salazar Rebolledo (2015): “La decisión en torno a la promoción de una acción de inconstitucionalidad contra la Ley Telecom, provee un ejemplo ilustrativo de cómo se construye, se conserva o se pierde la confianza y la legitimidad institucional”.

Los argumentos finales esgrimidos para fundamentar tal decisión fueron retomados por la comisionada Ximena Puente en los siguientes puntos:

1. Legitimación activa. Puede darse el caso que el Instituto no esté legitimado para perseguir la declaración de inconstitucionalidad. El IFAI solo está legitimado para interponerla contra normas que vulneren el derecho de acceso a la información pública y la protección de datos personales, por tanto la demanda que se pretende iniciar puede ser desestimada por falta de legitimación, por estar relacionada con materia de seguridad y justicia.
2. Improcedencia por estar en trámite otra acción de inconstitucionalidad. Actualmente está en trámite una acción de inconstitucionalidad interpuesta por el IFAI en contra del artículo 303 del Código Nacional de Procedimientos Penales, cuyo contenido está altamente relacionado con el contenido en discusión de la ley Telecom. De ese modo se considera que la resolución que tome la SCJN respecto a esa disposición, también se aplicará a los contenidos de la Ley Telecom.
3. Improcedencia de la acción de inconstitucionalidad, en virtud de que la misma descansa en omisiones legislativas, se argumenta con base a jurisprudencias anteriores, que la SCJN solo puede actuar como legislador negativo pero no puede obligar a emitir una norma por motivo de omisión.
4. La Geolocalización y la entrega de datos sí reúnen los requisitos exigidos en el artículo 16 constitucional, de tal modo, si se adopta una visión sistémica de la disposición normativa, no resultan en un riesgo para la seguridad e intimidad de las personas. Se alega que, contrario a lo señalado, la disposición normativa sí

establece de manera precisa la autoridad competente, el mandamiento, el papel de los concesionarios, y los mecanismos ante los que se puede acudir en casos de excesos en la medida.

5. El derecho a la intimidad no es un derecho absoluto. Sus restricciones deben estar previstas en la ley siempre y cuando se persiga un fin legítimo y las injerencias no sean abusivas o arbitrarias. En el caso de la Ley Telecom el fin que se persigue es la seguridad pública.
6. La medida de geolocalización no es una violación al derecho a la privacidad. Según votaciones previas de la SCJN, ésta es un instrumento que “da efectividad a la persecución de determinados delitos, sin que pueda estimarse lesiva de derechos fundamentales” pues tiene por objeto la localización de equipos de comunicación y no de personas individualmente determinadas.
7. La conservación de un registro y control de las comunicaciones de telefonía celular no supone una violación al derecho a la privacidad, ello basado en que la Ley Telecom establece expresamente las excepciones a la protección de datos, “sin que sea necesario que se definan mayores parámetros respecto de la misma”.
8. La entrega de datos contenidos en el registro no supone una violación al derecho a la privacidad. Una acción de inconstitucionalidad no puede promoverse con base en las “suposiciones o expectativas sobre la forma en que será aplicada una norma en un caso concreto” (Salazar, 2015, s/p).

En efecto, como mencionó el INAI en los argumentos esgrimidos para no interponer la acción de inconstitucionalidad en contra del 189 y 190 fracciones I, II y III; producto de la reforma del 2014, ya había ejercido (el INAI en mayo 2014 y la CNDH en Abril del 2014) de manera independiente, su derecho a la acción de Inconstitucionalidad ante la Suprema Corte de Justicia, a fin de impugnar el Código Nacional de Procedimientos Penales promulgado el 5 de marzo del 2014.

La Corte resolvió la acumulación de los casos (10/2014 y 11/2014) en un mismo expediente, al considerar que ambas impugnaciones coincidían en la solicitud de inconstitucionalidad respecto del artículo 303 del citado Código Nacional el cual otorga al Ministerio Público la facultad para la localización en tiempo real de los teléfonos celulares y cualquier otro dispositivo con acceso a

servicios de telecomunicaciones, así como a la conservación de datos contenidos en redes y equipos informáticos hasta por el plazo de 90 días.

Por lo que respecta al INAI, este solamente impugnó el citado artículo 303, mientras que la CNDH impugnó 14 de los artículos que integran el Código Nacional, relacionados con el debido proceso (132, 147, 148, 153, 242, 249, 251, 266, 268, 355 y 434 e incluido por supuesto el 303), al considerarlos violatorios de derechos fundamentales 4.

El argumento se basaba en la violación a los derechos fundamentales de legalidad, seguridad jurídica y privacidad que señalaba el artículo 303 que a la letra establece: “cuando exista denuncia o querella, y bajo su más estricta responsabilidad, el Procurador o el servidor público en quien se delegue la facultad, solicitará a los concesionarios o permisionario o comercializadoras del servicio de telecomunicaciones o comunicación vía satélite, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con los hechos que se investigan en términos de las disposiciones aplicables”.

En esta impugnación, la corte sostuvo la constitucionalidad bajo la justificación de la necesidad de la geolocalización para combatir los delitos considerados como graves, por lo que no existen derechos absolutos y, en todo caso, la geolocalización como una medida del derecho a la privacidad es válida.

Ahora bien, tomando en consideración los criterios jurisprudenciales del rubro “Controversias constitucionales y acciones de inconstitucionalidad. Criterios para determinar la invalidez indirecta de las normas, en el ejercicio donde la invalidez se origina a partir de la extensión de los efectos de la invalidez de otra norma” (jurisprudencia P./J. 53/2010), Flores Pacheco explica:

4Como se mencionó anteriormente en mayo del 2012, la Comisión Nacional de Derechos Humanos ya había presentado una acción de inconstitucionalidad ante la SCJN respecto a la reforma a la entonces vigente Ley Federal de Telecomunicaciones debido a la adición hecha al artículo 40 bis, que determinaba la obligación de los operadores de telecomunicaciones a colaborar mediante la localización en tiempo real de los equipos de telefonía móvil y la cual fue declarada infundada declarando la validez de las disposiciones impugnadas argumentando que en la geolocalización existe una búsqueda que se refiere a los equipos de comunicación móvil y no a personas, es decir, no se dirige a buscar personas sino un instrumento del delito (Acción de Inconstitucionalidad 32/2012).

Sin embargo, aunque no fue impugnada vía acción de inconstitucionalidad por ninguno de los sujetos constitucionalmente legitimados para ello, en caso de que la Suprema Corte de Justicia de la Nación determinara la invalidez del cuestionado artículo 303, podría hacer extensiva la invalidez a algunos artículos de la Ley de Telecomunicaciones y Radiodifusión, mediante un ejercicio indirecto de validez de normas (Flores,2016:s/p).

No obstante lo anterior, si así hubiera sido, la resolución de la Suprema Corte podría concluir en dos sentidos, declarando la constitucionalidad o bien declarando la inconstitucionalidad de los preceptos impugnados en este caso el 189 y 190 de la ley Federal de Telecomunicaciones y radiodifusión por lo que el órgano garante debió considerar evidentemente tal posibilidad de que la acción de inconstitucionalidad fuera invalidada, ya que si bien si hubiese ocurrido al contrario y se hubiera declarado inconstitucional el artículo 303 del Código Nacional de Procedimientos Penales, dicha invalidez habría sido extensiva al 189 y 190; sin embargo en caso contrario la resolución de la Corte fortalecería todas las disposiciones en discusión, razonamiento elemental que el órgano garante como celoso guardián de la privacidad y el derecho a la protección de datos personales debió prever para hacer frente a las reformas de La nueva Ley Federal de Telecomunicaciones y Radiodifusión del 2014.

Ante la incapacidad de respuesta por parte del INAI, posterior a la reforma de la LFTR, la organización Red por la Defensa por los Derechos Digitales, a través

de su representante legal, demandó el amparo y protección de la justicia federal respecto de los artículos 189 y 190 fracciones I, II, y III de la Ley Federal de Telecomunicaciones y Radiodifusión publicados con fecha 14 de Julio del 2014; “Los quejosos manifestaron sustancialmente, que los referidos preceptos legales transgreden en su perjuicio los derechos humanos a la intimidad, inviolabilidad de las comunicaciones privadas a la protección de datos personales, libertad de expresión y seguridad jurídica, en virtud de que permiten a las autoridades acceder a datos personales de los usuarios de telecomunicaciones, a conservar un registro de datos sobre las comunicaciones de los usuarios e imponen la obligación a las concesionarias o autorizadas de aportar la localización geográfica en tiempo real de los dispositivos móviles de los usuarios de redes de telecomunicaciones” (Amparo en revisión 964/2015 [5]).

Con fecha 24 de noviembre del 2014 la Juez segunda de Distrito en materia Especializada en Competencia Económica y Radiodifusión y Telecomunicaciones en el Distrito Federal sobreseyó en el juicio y negó el amparo a dicha asociación.

Inconformes con la negativa de amparo, los quejosos, (RD3), interpusieron el recurso de revisión ante el Tribunal Colegiado en materia Especializada en Competencia Económica, Radiodifusión y Telecomunicaciones, el cual, en sesión de 9 de junio de 2015, el Tribunal Colegiado resolvió en el sentido de confirmar el sobreseimiento dictado por la Juez de distrito y declararse incompetente para analizar los agravios planteados por los recurrentes, por lo que reservó la jurisdicción a la Suprema Corte de Justicia de la Nación, la cual, al considerar que no existían causas de improcedencia entró al estudio de los agravios expuestos por los promoventes.

La litis básicamente se concretó a determinar si los artículos 189 y 190, fracciones I, II y III resultaban contrarios a los derechos humanos: de legalidad y seguridad jurídica; a la protección de datos personales; y a la inviolabilidad de las comunicaciones, resolviendo en el sentido de confirmar la sentencia recurrida, negando el amparo solicitado contra los artículos en cuestión (Amparo en revisión 964/2015 [5]).

Como parte de la resolución al Amparo en revisión 964/2015 interpuesto por parte de la Asociación Red en Defensa por los Derechos Digitales en contra de los artículos 189 y 190 de la Ley Federal de Telecomunicaciones la segunda sala de la Suprema Corte de Justicia decidió el 23 de septiembre del 2014, que las instancias de seguridad podrán pedir la geolocalización inmediata de un usuario mediante la autorización judicial por parte de un juez de control por escrito y en la cual se funden las causas legales de la solicitud, las autoridades competentes para tal efecto serán la Procuraduría General de la República y las procuradurías estatales, la Policía Federal bajo el mando del Ministerio Público o los servidores públicos que deleguen esta facultad. Además de las autoridades competentes en los casos de amenazas inminentes a que se refiere la Ley de Seguridad Nacional. Los datos a solicitar serían el nombre y domicilio del usuario, tipo de comunicación, origen y destino, fecha y hora y duración de la comunicación, siempre que haya la petición de un juez. No se entregará la información cuando se trate de asuntos de carácter electoral, fiscal, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Algunas autoridades y otras voceras han esbozado su oposición al requisito de autorización judicial para llevar a cabo la geolocalización en tiempo real aduciendo que de exigirse tal requisito se entorpecerían las investigaciones que dependen de su rapidez para ser efectivas. No obstante, mediante un mecanismo de emergencia es posible permitir el acceso a los datos de geolocalización en tiempo real de manera inmediata sin prescindir del control judicial, indispensable para prevenir o evitar el abuso de este tipo de medida. Así en ciertos casos la autoridad podrá acceder a la geolocalización en tiempo real de manera inmediata, siempre y cuando, simultáneamente se haga la solicitud al juez de control. Si el juez autoriza la medida se retrotraerían los efectos y se entendería que la medida estuvo autorizada desde un primer momento. En caso contrario, existiría un mecanismo de detección de un uso abusivo de la medida y se dispondría lo conducente, como puede ser la destrucción de los datos y la vista a las autoridades competentes para esclarecer las posibles responsabilidades que amerite el caso (García-Gaytán; 2016, s/p).

Los artículos 189 y 190 fracciones I, II y III no señalan con precisión qué autoridades pueden hacer requerimientos a las concesionarias autorizadas, Sin embargo, la Corte, mediante el Amparo en Revisión 964/2015, dictado por la Segunda Sala, ha intentado solucionar el problema que se refiere a “la autoridad competente”, al resolver que, las únicas autoridades facultadas para tener acceso a los datos retenidos, son los Fiscales Federales y estatales, la Policía Federal y el Centro de Investigación y Seguridad Nacional.

A pesar de la definición de las autoridades señaladas, los riesgos de abuso son latentes, considerando la crisis institucional y organizacional por la que constantemente atraviesan las autoridades facultadas para la intervención. Por lo que no obstante reconocer la Suprema Corte los riesgos de abuso que implican las disposiciones en análisis estas disposiciones han sido validadas, bajo argumentos endebles e inconsistentes.

La Suprema Corte de Justicia, como se hizo referencia en la página 82 de la presente investigación, mediante la resolución 1621/2010, sostiene que el derecho a la inviolabilidad de las comunicaciones protege tanto el contenido de las comunicaciones como los datos relacionados con dichas comunicaciones, considerando que, si bien los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones, ofrecen información sobre las circunstancias en que se ha producido la comunicación, señalando que el registro de los números marcados o la duración de la llamada telefónica llevado a cabo sin observar las debidas garantías para restringir el derecho fundamental al secreto a las comunicaciones, puede provocar su vulneración (México, Suprema Corte de Justicia, Amparo Directo en Revisión 1621/2010).

Sin embargo, la propia corte ha declarado, que el artículo 190 fracciones I, II y III de la Ley de Telecomunicaciones y Radiodifusión, es constitucional, mediante la afirmación de que la retención de datos no implica una vulneración al derecho a la inviolabilidad de las comunicaciones (Segunda Sala, Suprema corte, Amparo en Revisión 964/2015).

La resolución contempla la obligación de contar con una orden judicial para poder tener acceso a los metadatos almacenados por parte de las compañías de telefonía móvil, salvo la geolocalización en tiempo real, la cual no requiere de dicha orden judicial, lo cual resulta absolutamente contradictorio.

Desde el criterio establecido en la resolución 32/2012, la Corte no ha variado mucho su concepción respecto a la geolocalización al sostener que esta sucedía en un solo momento y por lo cual no implicaba una invasión a la privacidad; sin embargo, el tiempo ha comprobado que se trata de un monitoreo constante y continuo de un sujeto perfectamente identificable, que mediante la conjunción de datos es capaz de revelar aspectos altamente sensibles de su vida. Dicha ligereza en la interpretación de la Corte se agudiza ante la ausencia de autorización judicial para su utilización bajo la excusa de utilizarla como mecanismo emergente para el esclarecimiento de una situación determinada, lo que revela una falta de justificación constitucional en su regulación.

La postura de la Suprema Corte ha sido vacilante, imprecisa e incluso contradictoria al adoptar por un lado medidas que parecen positivas como es el caso de su consideración en el sentido de que el acceso y análisis de la información almacenada en teléfonos móviles sin orden judicial implica una violación al derecho de inviolabilidad de las comunicaciones privadas; en el mismo sentido protege los metadatos en poder de las compañías de telefonía celular, al determinar imprescindible la autorización judicial previa; no obstante que la eliminación de la autorización judicial para efectos de obtención de datos de localización en tiempo real, va en contrasentido a la protección de los derechos fundamentales que parecen reflejar las decisiones relativas a los metadatos y los datos de conservación.

La postura del INAI de igual manera ha sido incongruente al argumentar que anteriormente a la reforma de julio del 2014, ya se había promovido acción de inconstitucionalidad respecto al artículo 303 del CNPP, toda vez que dicha acción no constituye en todo caso un impedimento para promover la correspondiente en contra del 189 y 190 fracciones I, II y III de la LFTR; incluso tal decisión hubiese

fortalecido en todo caso la primera resolución de acción de inconstitucionalidad respecto al 303 en caso de haber declarado la inconstitucionalidad.

Con base en lo anterior, la abstención de la mayoría de los comisionados del INAI en este sentido, reflejó una debilidad Institucional y falta de compromiso para cumplir con los objetivos para los cuales fue creado, la Protección de Datos del gobernado frente a las Instituciones.

No obstante lo anterior, el papel que ha llevado a cabo la sociedad organizada en esta nueva era de participación ciudadana ha demostrado la persistencia por defender la privacidad del gobernado, a decir del Director de la Organización Red por la Defensa de los Derechos Digitales:

“se presenta ahora una petición a la Comisión Interamericana de Derechos Humanos, la cual resolverá respecto de la admisibilidad de la petición. Si la CIDH considera que los artículos 189 y 190 de la LFTR se viola el derecho a la privacidad reconocido en la Convención Americana de Derechos Humanos, se podrá entonces someter el caso ante la Corte, cuyas sentencias son obligatorias para México” (<https://fayerwayer.com> consultado el 27 de febrero del 2017).

A pesar de los intentos de la Corte por aclarar los procedimientos para la geolocalización en tiempo real y la conservación de datos personales, los artículos 189 y 190 fracciones I, II y III no son lo suficientemente precisos para determinar cuáles son las autoridades que pueden solicitar la colaboración de las empresas para fines de seguridad y justicia, llevar a cabo el monitoreo en tiempo real o bien acceder a los metadatos de las comunicaciones. Tampoco se precisan los casos en que las autoridades pueden ser autorizadas para la intervención.

CONCLUSIONES FINALES

1. El texto de los artículos 189 y 190 fracciones I, II y III refleja los vacíos legales por los que atraviesa la legislación mexicana en general, y en específico en relación a la materia de vigilancia y conservación de datos la cual se encuentra dispersa en distintos ordenamientos, por lo que las disposiciones en análisis carecen de solidez, claridad y precisión. En tal virtud, se hace indispensable una Ley de conservación de datos que unifique y defina todos los aspectos concernientes a los distintos tipos de comunicaciones: metadatos, datos de geolocalización, comunicación en tiempo real y datos almacenados, y que refleje una consistencia a efecto de salvaguardar los derechos fundamentales.

2.- La normatividad mexicana, y en concreto el texto del artículo 189 de la LFTR carece de criterios objetivos para definir las autoridades legitimadas para tener acceso a los datos a conservar, puesto que no determina alguna autoridad específica a la que deba someterse tal decisión de conservación.

La Ley Federal de Telecomunicaciones se refiere a “Autoridades competentes” como aquellas que tienen a su cargo la seguridad nacional, la procuración de justicia y la administración de justicia, lo que genera que cualquiera de éstas puede, sin que medie mandato alguno, solicitar los datos personales de los usuarios de telecomunicaciones.

Como la misma denominación lo indica, la autoridad “competente” debe consistir en una autoridad judicial independiente e imparcial que cuente con los

conocimientos tecnológicos adecuados para garantizar que el Estado está actuando dentro de la legalidad y la observación de los derechos humanos de quien resulte vigilado.

Bajo el término “instancias de seguridad y justicia” como lo expone el texto del artículo 189 de la LFTR, engloba un sinnúmero de autoridades y servidores públicos que impide esclarecer con exactitud a cuáles se refiere.

En este sentido, se plantea un déficit de la normatividad mexicana ante la falta de precisión para definir a las autoridades competentes facultadas para el acceso a los datos objeto de conservación en apego a la finalidad perseguida y las limitaciones a las cuales estarían sujetas, a fin de evitar abuso de poder y por tanto violaciones a los derechos humanos.

Así mismo, en este caso no obsta que la Suprema Corte ha intentado solucionar esta deficiencia, señalando a Ministerios públicos locales y federales, Policía Federal y Procurador General de la República como facultados para tal efecto, en virtud de que la falta de coordinación y la corrupción que invade a las autoridades que señala, que comúnmente se ven involucradas con grupos criminales, impide garantizar un tratamiento adecuado de los datos personales de los individuos.

3. Los principios de proporcionalidad y finalidad implican reducir al mínimo la afectación a los derechos fundamentales, es decir, que sea estrictamente necesaria la medida de conservación de datos por parte de los sujetos obligados, así como el actuar de la autoridad judicial para esclarecer una investigación, así mismo se hace indispensable que el beneficio obtenido por el fin perseguido sea mayor que el perjuicio ocasionado en la esfera privada del individuo sometido a la vigilancia, esto es, que el estado justifique su actuar minimizando en lo posible en riesgo de afectación, de tal manera que ya se hayan agotado todos aquellos recursos existentes con que cuenta la autoridad para el esclarecimiento de un delito antes de invadir la privacidad con dichas medidas.

Los artículos 189 y 190 fracciones I, II y III omiten especificar cuál es la finalidad u objetivo de la retención de los datos personales, por lo que no establecen dichas causas. No obstante que se puede deducir que es la persecución de los delitos, no especifican cuáles son los tipos penales considerados como “graves” para la procedencia de la retención, lo anterior constituye un atentado a los principios de finalidad y proporcionalidad que sustentan el derecho a la protección de datos personales.

La Ley de Seguridad nacional en México autoriza al Centro de Investigación y Seguridad Nacional (CISEN) a interceptar comunicaciones privadas cuando exista una “amenaza inminente a la seguridad nacional” sin embargo el término de seguridad Nacional está en crisis lo que representa un contexto ambiguo para poder determinar cuándo procede la vigilancia y cuando no.

El concepto “seguridad nacional” como justificante para llevar a cabo la conservación de datos y la geolocalización, resulta un término sumamente ambiguo, el cual la legislación mexicana no ha logrado puntualizar, la seguridad nacional incluye todo y a la vez nada, por lo que deriva en la ausencia de justificación en el abuso de poder de las Instituciones facultadas para vigilar a la sociedad.

4. Los datos que integran una comunicación de telefonía celular, deben estar protegidos por el derecho a la inviolabilidad de las comunicaciones y por el de protección de datos personales establecido en los artículos 6 y 16 constitucionales, ya que su retención definitivamente sí afecta la intimidad de la persona y su derecho a la autodeterminación informativa como bienes jurídicos protegidos por el derecho a la protección de datos; no se trata de conservación o geolocalización de algo intangible o de objetos, como en su momento lo sostuvo la Corte, sino de personas, seres humanos, en su esfera privada.

El considerar por parte de la Suprema Corte que la geolocalización no busca personas sino equipos móviles como instrumento del delito resulta absurdo, ya que de los datos que se desprendan de los equipos móviles, evidentemente siguiendo

la teoría del mosaico, se puede llegar a configurar un perfil que defina la vida privada de una persona, la cual resulta sospechosa de la comisión de un delito a priori, esto es, todos somos sospechosos de la comisión de un delito mientras no se compruebe lo contrario, contradiciendo los principios constitucionales del debido proceso.

5.- Las compañías de telefonía celular carecen de las políticas necesarias para una adecuada conservación de datos que garantice al usuario que su información está siendo debidamente resguardada a fin de evitar abusos de poder por parte de las autoridades que la requieran.

Podemos afirmar que las compañías de telefonía celular no solo carecen de los procedimientos adecuados que aseguren seguridad y certeza en el tratamiento de los datos personales frente a terceros y en particular frente al Estado, sino que adolecen de los medios de defensa pertinentes que permitan al usuario del servicio, oponerse o inconformarse con el tratamiento y transmisión de dichos datos, ante las autoridades judiciales.

6. Los argumentos del INAI para justificar la omisión del ejercicio de la acción de inconstitucionalidad resultan antiprogresistas, débiles e incongruentes, pues el haber impugnado el 303 del CNPP no constituye un impedimento para impugnar el 189 y 190 fracciones I, II y III, cuyo contenido era más amplio que el primero ya que, al declararse inconstitucional abarcaba obviamente el contenido del 303.

El INAI como Institución garante de los datos personales, carece de autonomía e independencia para ponderar la protección de datos personales de las personas frente a un interés público, por lo que su actuar deja en el tintero su calidad como protectora de los ciudadanos frente a la divulgación de la información de que son titulares y que el gobierno ha recabado y posee de manera originaria para otras finalidades.

La abstención de la acción de inconstitucionalidad respecto a los artículos 189 y 190 fracciones I, II y III de la LFTR bajo la excusa de haber ejercido una anterior acción de inconstitucionalidad respecto al artículo 303 del Código Nacional

de Procedimientos Penales, no es suficiente para asumir que no había necesidad de hacerlo, lo anterior si consideramos que como órgano garante de los datos personales, su obligación consiste en agotar los mecanismos legales que la ley le otorga para anticipar y revertir la afectación que de la vulneración del derecho de protección de datos de carácter personal puedan resultar.

La presente investigación revela a través de la información recopilada una ausencia de comunicación y transmisión de información eficiente entre los sujetos obligados a la conservación de datos de sus usuarios, (operadora de telecomunicaciones) y el agente facultado para salvaguardar los derechos como es el INAI.

En el caso del sistema jurídico español, la Agencia de Protección de Datos juega un papel muy importante en la salvaguarda de estos derechos, en el caso de México, el INAI como el órgano garante tanto de transparencia como de protección de datos, revela una tendencia al servilismo en pro del sistema o del grupo en el poder.

La Suprema Corte de Justicia representa a través de sus criterios una postura antiprogresista y conservadora en virtud de que incurre en una notable contradicción al establecer como requisito indispensable la autorización judicial respecto de los datos almacenados por parte de las compañías de telefonía celular y no con respecto a los datos de geolocalización en tiempo real, lo que revela un estado de vulnerabilidad del individuo sujeto a ser vigilado y localizado frente a la decisión de una autoridad que pudiese ser incompetente y sin limitación alguna que potencialmente pudiera estar coludida con los grupos criminales para delinquir en contra de la ciudadanía.

No se trata de sacrificar la privacidad en pro de la seguridad, simplemente se trata de causar el menor daño posible en la esfera jurídica y social que rodea al gobernado a fin de aplicar dos derechos que pueden coexistir perfectamente si la normativa es clara y precisa en su redacción respetando los derechos fundamentales propios de una sociedad democrática.

La labor del Estado se reduce a un mero agente de control social, las libertades de los individuos están supeditadas a un comportamiento condicionado, (que presupone que todos son sospechosos de la comisión de delitos), pues gracias a la información de que dispone, puede anticipar la conducta de las personas, promoverlas o restringirlas de acuerdo con los intereses del gobierno en turno.

7. Otro aspecto no menos relevante, es el relacionado con la determinación de niveles de protección que puedan asegurar a los usuarios cuyos datos son conservados frente a riesgos de abuso o uso ilegal de los mismos en atentado a la confidencialidad; en el caso de México no contamos con un panorama muy alentador en cuanto a que, como se explicó en el capítulo segundo de la presente investigación, toda vez que no se garantiza un nivel alto de protección por parte de las operadoras en cuanto a la ausencia legal para precisar el destino de los datos recabados, no se asegura la destrucción de los mismos una vez cumplido su objetivo de colaboración con la justicia y, por tanto, el control de los mismos, que atendiendo a la colusión entre las Instituciones policiacas y de investigación con la delincuencia dejarían al usuario en completo estado de inseguridad e incertidumbre ante el enorme riesgo que implica el hecho de que sus datos sean captados por el crimen organizado, por citar un ejemplo.

En este sentido, es importante recalcar que la normatividad española ha legislado por medio de su reglamento de desarrollo de la Ley orgánica 25/2007 de 13 de diciembre, de protección de Datos de carácter personal en su artículo 81.4 en donde garantiza la “obligación de las operadoras a identificar al personal especialmente autorizado para acceder a los datos objeto de la ley, adoptar las medidas técnicas y organizativas que impiden la manipulación o uso para fines distintos de las comprendidas en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación y acceso no autorizados”.

10.- Los artículos 189 y 190 fracciones I, II y III vulneran el derecho a la protección de datos personales contemplado en los artículos 6 y 16 constitucionales en virtud de la afectación de la autodeterminación informativa como bien jurídico protegido por el mismo, puesto que hay una restricción al acceso, oposición, rectificación y cancelación de los datos personales en poder de las compañías de telefonía celular cuyos procedimientos no se encuentran debidamente precisados en dichas disposiciones, por lo que dejan al individuo en un estado de vulnerabilidad frente al tratamiento que tanto dichas compañías como las autoridades le puedan dar.

11. Es menester puntualizar que la pretensión de la presente investigación no consiste en la eliminación lisa y llana de las herramientas de conservación de datos y geolocalización, sino que los lineamientos para su implementación, estén claramente definidos y previstos en el texto de los artículos 189 y 190 fracciones I, II y III de la Ley Federal de Telecomunicaciones y Radiodifusión a fin de que se justifique plenamente la invasión, por un objetivo legítimo y evitar el riesgo de que en aras de erradicar la criminalidad, resulten más afectaciones que beneficios en perjuicio de la ciudadanía.

Se requiere de un andamiaje jurídico sólido que garantice que los datos personales se encuentran debidamente resguardados y que durante su retención se están cumpliendo los fines para los cuales fueron solicitados.

FUENTES DE CONSULTA

-Burke, Peter; (2002). De Gutenberg a Internet; Una Historia Social de los Medios de Comunicación; Editorial Taurus; Madrid.

-Trejo, García, Elma del Carmen; (2006). Regulación Jurídica en México; México.

-Sunstein, Cass; (2003). República.com. Internet, democracia y Libertad; Paidós, Barcelona.

-García, Tinajero, Leonel; (2011). Las Fronteras del derecho de la Información; Novum; México.

-Castells, Manuel; (2001). La Galaxia Internet; Reflexiones sobre Internet, Empresa y Sociedad; areté; Madrid.

Campuzano, Tomé; Herminia; (2000). Vida Privada y Datos Personales; Tecnos; Madrid.

-Castells, Manuel; (2000). La Era de la Información; Tomo III; Fin del Milenio; Siglo XXI; Madrid.

- Castells; Manuel; (2000). Local y Global; La Gestión de las Ciudades en la Era de la Información; Taurus; México.

-Turkle, Sherry; 1997, La Vida en Pantalla, La Construcción de la Identidad en la era del Internet; Paidós; Barcelona.

Scolari, Carlos; (2004). Hacer Clic, Hacia una semiótica de las Interacciones Digitales; Gedisa; Barcelona.

-Roszak, Theodore; (2005). El Culto a la Información; Un Tratado sobre Alta Tecnología, Inteligencia Artificial y el verdadero Arte de Pensar; Gedisa; Barcelona.

-Foucault, Michelle; (2006). Seguridad, territorio y Población; Fondo de Cultura Económica; Buenos Aires.

- Megías Quirós; José Justo; (2007) Coord., Sociedad de la Información; Derecho, libertad; comunidad; Aranzadi; Pamplona; págs. 95-120.

Held, D; Mac Grew, A; Goldvlatt, D; Perraton, J. (1999). Global Transformation Polity Press, Cambridge.

Arellano Toledo; Wilma; Coord., (2012). La Sociedad de la información en Iberoamérica; Estudios Multidisciplinarios; Porrúa; México.

Byung-chul, Han; (2014). Psicopolítica, Neoliberalismo y Nuevas Tendencias de Poder, Barcelona, España, Herder.

Huerta, Ochoa, Carla; (2005). La Intervención Administrativa en el Estado Contemporáneo; Estudios en Homenaje a don Jorge Fernández Ruiz . Derecho Administrativo.

Bondi, Loretta; (2004). Beyond the Border Across the Atlantic, México's Foreign and Security, Post September 11th, Center for Transatlantic Relations, The Johns Hopkins University, Washington.

Laborie Iglesias, Mario; (2011). La Evolución del Concepto de Seguridad, Instituto Español de Estudios Estratégicos, Madrid.

Gilmore;(1977).The Ages of American law, Yale University Press; New Heaven.

Revenga, Sánchez, Miguel; (1995). El Imperio de la Política, Seguridad nacional y Secreto de Estado en el sistema constitucional norteamericano.

López, Portillo, Ernesto; (1998). Hacia una Ley de Seguridad nacional, UNAM; pdba.georgetown.edu.

De la selva, Alma Rosa; (2012). Brecha Digital y Sociedad de la Información y el Conocimiento en México; Infotec; México.

Davara, Rodríguez, Miguel Angel; (2008). La Protección de Datos y las Comunicaciones Electrónicas, En Ferrer Mac-Gregor, Eduardo y Zaldívar Lelo de Larrea, Arturo (Coords.). La ciencia del derecho procesal constitucional. México; UNAM IIJ.

Nahabetián Brunet; (2010). Conferencias; Fundación Ciencias de la Documentación; Protección de Datos Personales, un desafío de nuestro tiempo; Octubre 2011.

Lira Arteaga; Oscar Manuel; Cibercriminalidad; (2010). Fundamentos de investigación en México; Instituto Nacional de Ciencias Penales; México.

Pérez, Luño, Antonio Enrique; (2002). Intimidad y Protección; Dyckinson; Madrid.

Del Peso Navarro, Emilio; (2003). Servicios de la Sociedad de la Información, Comercio Electrónico y Protección de Datos, Díaz de los Santos, Madrid; p.103-125.

Lucas Marín, Antonio; (2009). La Nueva Comunicación; Colección Estructuras y Procesos; Trotta; Madrid.

Plaza, Crisanto; (2015). Ensayo sobre la Regulación Tecnológica, La Era Digital en Europa; Taurus; Madrid.

LLácer Matacás, (2012). María Rosa; La Autorización en el Tratamiento de Información Personal en la contratación de bienes y servicios; Colección I. Persona y familia; Monografías de Derecho Civil; Madrid.

Corbacho Abelaira, Fernando J.; (2006). Nuevas Tecnologías como Instrumento de Represión Penal; En Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 12/2006 3ª. Parte Doctrina. Edit. Aranzadi, S.A.U., izur Menor.

FUENTES HEMEROGRÁFICAS

- “Telecomunicaciones: Ley para un Estado Policial”, en Rev. Nexos; Red en Defensa de los Derechos Digitales; CDMX; julio 9 2014.

- Ideosema, (2004). Revista de Literatura, lingüística y semiótica; número 3, Vol. 1; Escuela de Lenguas y Literaturas Hispánicas; CDMX; 2004.

- Natalia Calero Sánchez; “El Nuevo IFAI, una caricatura de la Autonomía Constitucional”; en Rev. Transparencia, agosto; 2014.

- *GITS*, “Ciberseguridad, Privacidad del Internauta y Delitos Telemáticos”; 2015.

- Méndez, José Carlos; “Ley de Geolocalización: Persecución vs Seguridad”, enero; 2014.

-Gainza, Carolina; en Rev. de Sociología; No.17; Facultad de Ciencias Sociales de la Universidad de Chile; p. 124.

- Arellano, Toledo, Wilma; Ochoa Villicaña, Ana María; *Derechos de Privacidad e Información en la Sociedad de la Información y en el entorno TIC*; Revistas lus; vol. 7 No. 31; Puebla, ene/jun; 2013.

- Cassou Ruíz, Jorge Esteban; “Revista del Instituto de la Judicatura Federal”, Núm. 28; CDMX; 2009.

- “Telecomunicaciones: Ley para un Estado Policial”, en Rev. Nexos; Red en Defensa de los Derechos Digitales; CDMX, julio; 2014.

- Palacios, Surya *OPINIÓN*: “La Geolocalización de Celulares afecta a la privacidad”; en Rev. Idconline; CNN CDMX; 2014.

- Martínez, Martínez Evelio; “Galileo: La siguiente Generación de los Sistemas de localización por satélite”; Fundación Teledes; en Rev. Red, abril 2001.

-Aldo Macedo Fredy; “Aportaciones generales a las Ciencias Jurídicas”, Comentarios al Código Nacional de Procedimientos Penales; En Rev. *Iter Criminis*, Revista de Ciencias Penales; Num.9; Sexta Época; abril-junio; CDMX, 2015.

-Gonzáles, Encinar; José Juan; “Derecho Constitucional, España y Unión Europea”; Ariel, 2000; Barcelona.

ENLACES ELECTRÓNICOS

- Rodríguez Laínz, Jose Luis, (2012). “Hacia un nuevo entendimiento del concepto de gravedad del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas”, Juzgado de Instrucción número 4 de Córdoba Diario La Ley, Nº 7789, Sección doctrina, 2 de febrero de 2012, Año XXXIII, Ref. D-49, Editorial LA LEY: <http://diariolaley.laley.es>. Consultado el 15 de octubre del 2017.

- Rodríguez Laínz; José Luis, (2014). “Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones”; Magistrado Juzgado Instrucción 4 de Córdoba; Diario La Ley, Nº 8308, Sección Doctrina, 12 de mayo de 2014, Ref. D-148, Editorial LA LEY; <http://diariolaley.laley.es>. Consultado el 15 de octubre del 2017.

- Ormazábal Sánchez, Guillermo, (2008). “Los deberes de conservación de datos por parte de los operadores de telecomunicaciones y su aportación al proceso mediante requerimiento judicial”, (Reflexiones a la luz de la legislación española y de la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea) Diario La Ley, Nº 7055, Sección Doctrina, 13 de Noviembre de 2008, Año

XXIX, Ref. D-322, Editorial LA LEY; <http://diariolaley.laley.es>. Consultado el 15 de octubre del 2017.

-Ponce Rodríguez, Sergio, (2008). “La Conservación de los Datos por los Operadores de Servicios de Comunicaciones Electrónicas, Análisis de la --Ley 25/2007, de 18 de Octubre, sobre la Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones”, en Rev. Actualidad Jurídica Uría Menéndez; 19-2008. www.uria.com/documentos/publicaciones/1931/documentos/articulo/UM.pdf. Consultado 13 de octubre de 2016.

- Piedras, Ernesto, (2016). “Consideraciones sobre la Colaboración con la Justicia”, epiedras@the-ciu.net. Consultado el 12 de enero del 2016.

- Markku, Lawkka, (2000). “Criteria for a Privacy Supportig System”, <http://www.tlm.hut.fi/Research/Tessa/Papers/Lawkka-nordsec>. Consultado el 13 de diciembre 2015.

-www.sociedadinformacion.unam.mx/index.jsp?action=est; Observatorio de la Sociedad de la Información y del Conocimiento de la Universidad Autónoma de México en línea. Consultado el 10 de febrero 2016.

- www.gitsinformatica.com, (2003). “ciberseguridad gits, informática”. Consultado el 2 de marzo 2016.

- Araya Eduardo, (2005). en Rev. Agenda Pública; Universidad de Chile; Instituto de Asuntos Públicos; agendapublica.uchile.cl Año IV-No. 5, diciembre 2004/enero 2005. Consultado el 12 de marzo 2016.

-www.libertaddigital.com “Estados Unidos impulsó las medidas de control de datos aprobadas en la ley de internet española”. Consultado 20 de agosto del 2016.

- González Fernández; José Antonio, (1995). “La Seguridad Pública en México”; biblio.jurídicas.unam.mx. Consultado el 20 de agosto 2016.

- González, Ballesteros, Teodoro, (1987). “Los principios de la Protección de datos personales Garantías frente al poder político”;Madrid; www.quadernsdigital.net; Fecha de consulta 4 de enero del 2017.

-L.E. VIGGIOLA y E. Molina Quiroga, (1999). “Tutela de la autodeterminación informativa. Aproximación a una regulación eficaz en el tratamiento de datos personales”. Ponencia presentada al Congreso Internacional de “Derechos y Garantías en el siglo XXI” de la Asociación de Abogados de Buenos Aires, <http://www.aaba.org.ar/bi151302.htm>. Consultado el 5 de enero del 2017.

- ProtDataMxproteccióndatos.mx/wp/ 2011,Jurisprudencia de la Suprema Corte de Justicia de la Nación sobre Datos Personales y Comunicaciones Privadas en México; Semanario Judicial y su Gaceta XXVIII; septiembre 2008; Tesis I.3º.C695 C; p. 1253. Consultado el 10 de enero 2017.

- Marecos, Gamarra, Adriana, (2013). Observatorio Iberoamericano de Protección de Datos; <http://oiprodat.com/>. Consultado el 5 de febrero del 2017.

- Rodríguez, Maritza, (2013). “Los Principios Internacionales sobre la aplicación de los Derechos Humanos de Vigilancia; Análisis Comparado de las Leyes y prácticas de vigilancia en Latinoamérica”; neccesaryandproporcionate.org. Consultado el 5 de febrero 2017.

-ec.europa.eu/spain/pdf/ip0904-2.pdf. Declaración de la Comisión Europea, Directiva sobre la conservación de datos: Declaración de la Comisaria Malmstrom sobre la sentencia del Tribunal Europeo, 8 de abril del 2014. Consulta 5 de octubre del 2016. Consultado el 13 de marzo 2017.

La Directiva 2006/24/CE “Sobre Conservación de Datos de Tráfico en las Comunicaciones Electrónicas: Seguridad vs privacidad”.

www.lioc.edu/idp/3/dt/esp/villasau.pdf. Villasau, Mónica, En Rev. Internet, Derecho y Política; consulta 5 de octubre de 2016

-NP_GEOLOCALIZACION.pdf.noticiasjurídicas.com/.../3703, “Actualidad”, Fecha de consulta 05 de octubre del 2016. Agencia Española de Protección de Datos, fecha de consulta 5 de octubre del 2016.

-Article 29, Data Protection Working Party, consultado el 06 de octubre 2016. 81/11/EN; WP185.

-<http://www.boe.es>, Agencia Estatal Boletín Oficial del Estado; consulta 6 de octubre del 2016.

- Ponce Rodríguez Sergio, (2008). “La Conservación de Datos por los Operadores de Servicio de Comunicaciones Electrónicas”; www.uria.com/documentos/publicaciones/1931/documentos/articuloUM.pdf; En Rev. Actualidad jurídica Uría Menéndez/19-2008, p.71-77, fecha de consulta 10 de octubre 2016.

- Navarro, Jiménez, Gilberto, Ordenjurídico.gob.mx. “El Derecho a la Protección de Información Personal en México”, p.20, consultado el 24 de enero del 2017.

-<https://fayerwayer.com> 2016/05; consultado el 27 de febrero del 2017, Suprema Corte de México aprueba retención de metadatos. Consultado 13 de febrero del 2017

-SCJN; Amparo en Revisión 964/2015; AR-964-2015; consultado el 28 de febrero del 2016.

LEGISLACION

-Ley Federal de Telecomunicaciones y Radiodifusión, aprobada por el congreso mexicano con fecha 07 de Julio del 2014.

- www.diputados.gob.mx. Ley Federal de Protección de Datos Personales, consultado el 12 de febrero del 2015.

-www.diputados.gob.mx, Constitución Política de los Estados Unidos Mexicanos, consultado el 20 de marzo del 2016.

-www.diputados.gob.mx, Ley Federal de Seguridad Nacional. Consultado el 25 de mayo del 2015.

-www.dof.gob.mx, Ley General del Sistema Nacional de Seguridad Pública. Consultado el 15 de marzo del 2015.

-www.diputados.gob.mx, Ley General de Salud. Consultado el 18 de abril del 2015.

-<http://www.oas.org>. Tratado de la Convención Interamericana de Derechos Humanos.

-<http://www.boe.es/legislación> Constitución Española, Agencia Estatal Boletín Oficial del Estado.

-Ley Orgánica de 13 de diciembre 15/1999 de Protección de Datos de Carácter Personal.

-Ley de 25/2007, de 18 de octubre de Conservación de Datos Relativos a las comunicaciones electrónicas y a las Redes públicas de comunicaciones.

-Ley 30/1992 del 26 de noviembre, Agencia de Protección de datos en España.

-Código Penal Español, (Reforma junio de 2015).consultado el 9 de octubre del 2016.

-www.BOE.es, Ley de Enjuiciamiento Criminal vigente, consulta 10 de octubre de 2016. Consultado el 18 de octubre del 2016.

-www.BOE.es, Ley General de Telecomunicaciones 32/2003. Consultado el 19 de octubre del 2016.

