Anuario Jurídico y Económico Escurialense, **XLVIII (2015) 159-180 / ISSN: 1133-3677**

El Derecho a la Intimidad y la Protección de Datos en la era de la Seguridad global. Principios constitucionales versus riesgos tecnológicos

The Right to Privacy and Data Protection in the Age of Global Security. Constitutional principles versus technological risks

Dra. Teresa Maria GERALDES DA CUNHA LOPES
Universidad Michoacana de San Nicolás de Hidalgo
Michoacán (México)
tdacunhalopes@gmail.com

"The constitutional right to privacy,
a right that many believe has little to do with privacy
and nothing to do with the Constitution".

Jed Rubenfeld in "The Right to Privacy", Yale Law School Legal Repository (*1/1/ 1989)*

Resumen: Los avances en las tecnologías de la información y de la comunicación (TIC's) están revolucionando prácticamente todos los aspectos de la vida y facilitan el acceso a la información de una forma exponencial. Por una parte, esto exige que las administraciones públicas, proveedores de Internet, etc., hagan una reingeniería de sus procesos con el fin de beneficiarse de las TIC. Por otro lado, esto significa que tienen que facilitar el acceso de los ciudadanos a su información personal y estar plenamente en el cumplimiento de los derechos constitucionales a la privacidad y a la protección de datos personales. Estamos, por tanto, ante el comienzo de una revolución que va a redefinir el Estado de Derecho y de un cambio en los conceptos de soberanía del Estado como consecuencia de las nuevas preocupaciones por la seguridad internacional y el uso regular de las bases de datos que permiten almacenamiento masivo de información o redes que permiten comunicaciones rápidas y seguras.

Abstract: Advances in information and communication technologies are revolutionizing virtually every aspect of life and facilitating access to information in an exponential way. On one hand, this calls for public administrations, Internet providers, etc, to reengineer their processes so as to benefit from ICT while, on the other, it means they have to facilitate citizen access to their personal information and be fully in compliance with Constitutional rights to Privacy and to Data Protection Laws. We are, therefore, facing the beginning of a revolution which will redefine the rule of law and a change in state sovereignty, concepts; as a consecuence of new international security concerns and regular use of databases which allow massive storage of information or networks which allow fast and secure communications.

Palabras clave: Seguridad, Privacidad, Derecho a la Intimidad, Protección Datos, Derecho Constitucional.

Keywords: Security, Privacy, Right to Privacy, Data Protection, Constitutional Law.

Sumario:

Introducción.

I. Los nuevos riesgos y amenazas al Derecho a la Intimidad y a la Protección de Datos en Internet.

II. El Derecho al Control de la Información Personal ("The Right to Control Information about oneself") y la Protección al Derecho de Autonomía Informática.

2.1. *El Derecho al Control de la Información Personal ("The Right to Control information about oneself") y la Protección al Derecho de Autonomía Informática en el Common Law norteamericano*.

2.2. *En el Derecho Comunitario (UE).*

2.3. *En el Derecho Mexicano*.

III. Estudio de caso: los criterios jurisprudenciales de la SCJN sobre la "Ley de Geolocalización" y los límites a los Derechos Fundamentales versus Seguridad Nacional.

IV. Reflexiones Finales.

V. Referencias Bibliográficas.

Recibido: julio 2014.
Aceptado: septiembre 2014.

INTRODUCCIÓN

Las estructuras de la Sociedad de la Información y del Conocimiento, cuya arquitectura se apoya sobre la difusión y masificación de las tecnologías de la información y de la comunicación, están revolucionando prácticamente todos los aspectos de la vida y facilitan el acceso a la información de una forma exponencial.

Estamos, por tanto, ante una revolución que va a redefinir el Estado de derecho, provocada por elementos, tan diferentes en su naturaleza, como por ejemplo: un cambio en los conceptos de soberanía del Estado, las nuevas preocupaciones por la seguridad internacional y el uso regular de las bases de datos que permiten almacenamiento masivo de información o redes que permiten comunicaciones rápidas y seguras. Creemos que el establecimiento de sistemas de gestión electrónica constituye un elemento decisivo en el aumento de la calidad de las relaciones entre las administraciones y los ciudadanos y entre los entes privados y los usuarios.

Tales sistemas elevan el nivel de eficiencia de los servicios públicos, aumentan el grado de interactividad con los ciudadanos, al elevar el potencial de la participación democrática y la eficiencia del Estado de Derecho asegurando mejoras en la calidad de los servicios y de vida, además de ser un factor importante en la estructuración de la economía moderna.

Sin embargo, los sistemas electrónicos de gestión implican la recolección, procesamiento y transmisión de datos personales. Por esta razón, es absolutamente necesario detectar posibles problemas relativos a los riesgos y violaciones a los Derechos Fundamentales de la Intimidad y de la Protección de Datos en la S.I.C.

En consecuencia, debemos evaluar los riesgos involucrados y estudiar las soluciones adecuadas, no sólo dentro de los parámetros técnicos, sino con instrumentos jurídicos y con los protocolos de ejecución judiciales correspondientes.

En este artículo, sobre la base del método comparativo analizaremos los temas importantes en el derecho constitucional comparado, analizando el alcance de la constitucionalización de la privacidad y comparando los sistemas normativos de protección de datos de la UE , EE.UU y México, que distinguen entre privacidad entendida como control de una persona sobre la información y la privacidad entendida como la capacidad de la persona para ejercer su autonomía informativa y controlar frente a las decisiones administrativas del Estado y a los proveedores de Internet el uso de sus datos personales .

I. LOS NUEVOS RIESGOS Y AMENAZAS AL DERECHO A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS EN INTERNET

Las Constituciones reconocen el Derecho a la Intimidad que implica, como han reconocido la Suprema Corte norteamericana, la Corte de Justicia Europea o la Suprema Corte en México, la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los otros, necesario para mantener una calidad mínima de la vida humana. Además, también han constitucionalizado el derecho a la protección de los datos de carácter personal que garantiza a los individuos un poder de disposición y control sobre ellos. Sin embargo, la utilización de las nuevas tecnologías puede facilitar la vulneración de la Intimidad de las personas.

Las nuevas tecnologías permiten acceder y agregar datos personales dispersos que de esta manera faciliten un perfil de la persona afectada, cosa difícilmente realizable sin ellas, al menos no sin abonar unos costes muy elevados. También permiten poder conocer las actividades realizadas al navegar por Internet, saber si se visita una página u otra o si se compra determinado producto, o cuáles son nuestras preferencias políticas y nuestro círculo de relaciones sociales, laborales y familiares. Todo eso sin que la persona afectada tenga conocimiento de ello y sin dejar, prácticamente, ningún rastro o huella de esta vigilancia continua. En este contexto , el individuo no puede realizar ningún control sobre esos datos ni sobre el uso primario o derivado que de ellos se realiza.Para contrarrestar los riesgos inherentes a la evolución de las estructuras de la Sociedad de la Información y del Conocimiento y, al mismo tiempo, para aprovechar las posibilidades reales de la misma, deben establecerse algunos nuevos principios generales si se desea que los ciudadanos de esta nueva Telepolis estén mejor protegidos y tengan mayor (y real) control sobre su entorno.

Dicho control es esencial si los individuos van a ejercitar una responsabilidad efectiva para su propia protección y deben estar mejor preparados para ejercitar apropiadamente la autodeterminación informativa, no sólo a través del ejercicio de los derechos ARCO, sino también con el fortalecimiento del habeas data con

las nuevas posibilidades abiertas por el derecho al olvido en Internet y por la aplicación de medidas de seguridad jurídica y de seguridad informática para contrarrestar las posibilidades abiertas por las RFID (en particular la geolocalización) y por la identificación con datos biométricos.

Hemos entrado en una era de masificación de la recolección y almacenamiento de datos, conocida por los expertos como "Big Data"[1] o sea en la revolución de los datos masivos .En el momento actual, los datos ya no son analizados (ni pensados) como algo estático cuya utilidad deja de existir cuando la función para la cual fueron recabados, almacenados y tratados se realiza. Tal como lo afirman Mayer-Schönbergen y Cukier[2]: "Los datos se convirtieron en una materia prima [...]. Los datos pueden reutilizarse inteligentemente para convertirse en un manantial de innovación y servicios nuevos. Los datos pueden revelar secretos a quienes tengan la humildad, el deseo y las herramientas de escuchar". Nuestro cotidiano, es un medioambiente hiperconectado, en el cual el individuo está sumergido en un océano de información y es la fuente primera de datos. En este punto, es necesario introducir la diferencia entre "digitalización" y "datificación", contextos y conceptos muchas veces confundidos en un sólo. Los datos, son por ende cualquier tipo de información que pueda ser transformado en un código binario, lo cual va mucho más allá de las definiciones jurídicas de los corporii normativos vigentes.

El nivel que presenta los riesgos más evidentes para el ejercicio de nuestros derechos y libertades es el de la masificación de datos y de las posibilidades de geolocalización y, por ende de producción de biopolíticas de seguridad.

II. EL DERECHO AL CONTROL DE LA INFORMACIÓN PERSONAL ("THE RIGHT TO CONTROL INFORMATION ABOUT ONESELF") Y LA PROTECCIÓN AL DERECHO DE AUTONOMÍA INFORMÁTICA

En el momento actual de la conceptualización del Derecho a la Intimidad, se identifica a éste con la llamada *libertad informática*, por el advenimiento de las nuevas tecnologías de la información y la comunicación (TIC), pero sobre todo, por el ejercicio pleno de las libertades fundamentales del individuo, de principio para poder acceder a todo tipo de información (almacenada y tratada manual o informáticamente) sea cual fuere la persona que la tenga

[1] "Big Data" es una expresión anglosajona que hace referencia a los sistemas que manipulan enormes cantidades de datos. Podría traducirse al castellano como "datificación masiva", pero la mayoría de los autores usa el término inglés.

[2] MAYER-SCHÖNBERGEN y CUKIER, *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt, 2013.

(natural, jurídica, pública o privada), siempre que sea sobre sí mismo o que le concierne, a efectos inmediatos de consultar o revisarla, y fruto de aquéllas facultades, solicitar, sí fuere del caso, la rectificación o la cancelación de la información, si resulta inexacta o incorrecta (fundamentación teórica del Habeas Data).

2.1. *El Derecho al Control de la Información Personal ("The Right to Control information about oneself") y la Protección al Derecho de Autonomía Informática en el Common Law norteamericano*

Pese a argumentación generalizada *contrario sensu,* este derecho de control de la información de sí mismo, expresamente ya se halla previsto en el ensayo de Warren y Brandeis, tal como lo denotábamos al hacer referencia al aspecto negativo (facultades de exclusión: *The right to let alone*), como el aspecto positivo de autocontrol de la información, basado en que el *Common Law* garantizaba por desde aquélla época el derecho a toda persona a decidir hasta qué punto pueden ser comunicados a otros pensamientos, sentimientos y emociones.

Estas facultades de la *Privacy*, como ya vimos con anterioridad, no son absolutas, sino limitadas por el propio *Common Law,* como ya lo referimos y como se desprende de la decisión judicial Barrows VS. Bell, ante las exigencias del bienestar general o de la equidad y estas a título enunciativo son:

1. El Derecho a la Intimidad no impide la publicación de aquello que es de interés público o general.

2. El Derecho a la Intimidad no prohíbe la información sobre un tema, aun siendo éste de naturaleza privada, si la publicación se hace en las circunstancias en que, conforme a la ley de difamación y libelo, sería calificada de información privilegiada.

3. El derecho no otorgaría, probablemente, ninguna reparación por violación de la Intimidad cuando la publicación se haga en forma oral y sin causar daños especiales.

4. El Derecho a la Intimidad decae con la publicación de los hechos por el individuo, o con su consentimiento. Esto es una aplicación de la ley de propiedad literaria y artística.

5. La veracidad de lo que se publica no supone una defensa. Se impide la publicación incorrecta de la vida privada y el que pueda ser descrita.

6. La ausencia de *"malicia*" en quien hace público algo no constituye defensa.

En forma sintética estos principios, son recogidos por el *Office of Science and Technology of the Executive Office of the President* de los EE.UU, cuando en 1967 emite un concepto sobre la *Privacy* en los siguientes términos: "*el derecho a la vida privada es el derecho del individuo de decidir por sí mismo en qué medida compartirá con otros sus pensamientos, sus sentimientos y los hechos de su vida privada"*[3].

Posteriormente aparecen los trabajos de *WESTIN* en 1967 (*Privacy and Freedom*) y de *SHATTUCK*, en 1977 (*Rights of Privacy*), sobre el derecho al control de la información referente a uno mismo, autores que han tenido el mérito de poner de relieve una progresiva tendencia a concebir la *Privacy* como el poder de ejercer un control sobre las informaciones que puedan afectar al individuo.

Los estudios de Westin y Shattuck se fundan en el impacto de las nuevas tecnologías de la información (TI), el avance de los sistemas informáticos basados en los computadores, en las libertades fundamentales e Intimidad y en el derecho de acceso a la información.

Desde la segunda mitad del siglo XX se pone en evidencia la irrupción de las tecnologías, la informática no sólo en la potencial vulnerabilidad de los Derechos y Libertades que con ella se posibilitan sino en la igualmente potenciada protección que con aquellas puede logarse si se actúa conforme al *Common Law*. Con el paso del tiempo, son más los argumentos a favor del riesgo, la ampliación del grado de vulnerabilidad y la amenaza que representan estas nuevas tecnologías y la informática que los argumentos proteccionistas, y así quedará plasmado en las diferentes legislaciones y Constitucionales del mundo.

Entendemos que el derecho al control de la información referente a uno mismo, en los dos autores citados, se refería a las personas jurídicas colectivas (privadas o públicas), lo cual plantea la posibilidad del derecho al control de la información (*information control*) de las personas jurídicas y no sólo las personas físicas o naturales, como había sido la tesis dominante hasta ese momento de la evolución del aquél derecho y de los derechos fundamentales en general.

Parafraseando a Westin*, ¿*qué facultades comprendía ese derecho a controlar la información uno mismo? De la radiografía de hechos, sucesos, derechos y avances tecnológicos de la sociedad Norteamérica de aquella época descritas en su libro *Seguridades legales para identidad absoluta.*

> *"Este tipo de entidad al ser racional y autónoma es por sí (per se), no por otro, es decir, es persona (personare). De alguna manera es substancial;*

[3] Ver sitio web del *Office of Science and Technology of the Executive Office of the President.*

y todo lo substancial es un supuesto, y el supuesto es sujeto, y si éste es racional y autónomo, sin duda alguna tiene que ser sujeto de derechos y deberes. Luego la persona jurídica es una entidad que se expresa jurídicamente como sujeto de derechos y deberes". (...)"Los derechos fundamentales son aquellos que fundan la legitimidad del orden jurídico, por tratarse del reconocimiento que el sistema legal positivo hace unos bienes que son necesarios para la dignidad de la vida humana puesta en relación social. Estos derechos son necesarios, no contingentes tanto para el orden social justo, como para el despliegue jurídico adecuado de la persona. Tuvo el sistema ius filosófico que acudir al origen remoto de tales derechos en el ius naturale que era exclusivo para la persona humana. Luego vino un concepto más depurado, que se fundaba no tanto en la naturaleza humana, sino que se centraba en la dignidad de la persona y surgió el criterio de los derechos individuales del hombre, que luego admitió la socialidad y solidaridad de éste, de suerte que desembocó en los derechos colectivos de las personas, y aquí se encuadra, por vez primera, la titularidad de las personas jurídicas como sujeto de derechos fundamentales, como expresión mancomunada de la idea social de los seres humanos, que tienden a vincularse por medio del derecho, en lugar de disociarse en aras de una mal entendida individualidad. Con el advenimiento de la segunda generación de Derechos Humanos -que incluye lo social como sujeto de derecho- se consolida hoy, en la vigencia plena de la llamada tercera generación de Derechos Humanos (derechos de los pueblos y reconocimiento de la humanidad como gran persona jurídica sujeto de derecho universales), es contra evidente afirmar que sólo los individuos considerados aisladamente son titulares de los derechos fundamentales, porque ello supone negar toda una evolución jurídica trascendente, en el sentido de que el hombre se realiza como persona también en forma colectiva, y para ello necesita de la protección jurídica tanto desde su dimensión universal, como de su aspecto en sociedades autónomas".

Estando pues claramente establecido que las personas jurídicas son titulares de derechos fundamentales, y por lo tanto de la acción de tutela, resulta necesario precisar, adicionalmente, que de manera específica son titulares del derecho de Habeas Data. Un ejemplo concreto es el derecho al honor y al buen nombre. Las personas naturales que conforman la persona jurídica se verían afectadas si el todo que las vincula no es titular del buen nombre como derecho. Hay un interés social que legitima la acción de reconocimiento, por parte del Estado y de la sociedad civil, del buen nombre que ha adquirido un ente colectivo, porque ello necesariamente refleja el trabajo de las personas humanas en desarrollar la perfección de un ideal común objetivo. Si las personas jurídicas

son titulares del derecho fundamental al buen nombre, en consecuencia lo son también del derecho al Habeas Data, toda vez que este último derecho, existe justamente como garantía de aquel y del Derecho a la Intimidad personal y familiar. De esta manera, el Habeas Data viene a ser como una garantía de estos dos derechos, siendo por lo tanto accesorio de ellos al *garantizar la Intimidad en una sociedad de la información y del conocimiento.*

En la parte pertinente, al derecho a controlar la información sobre uno mismo y el ejercicio subsecuente de las facultades que éste engendra en entronque con el *Habeas Data*, la *Privacy Act*[4], sostiene que las instituciones o órganos que tienen bajo su responsabilidad un sistema de registros (entendiendo como registro, una unidad de información personal tratada, almacenada y registrada informáticamente con el consentimiento expreso de la persona concernida) deberá permitir al individuo examinar y tomar nota del registro a él concerniente y permitirle solicitar modificaciones.

Es necesario enfatizar que en EUA, tal como en México hasta las recientes reformas constitucionales entre el 2009-2012, el Derecho a la Protección de Datos está íntimamente imbricado en la normatividad interna sobre el acceso a la información pública. Una reformulación del Privacy Act fue introducida en el *Freedom of Information Act*[5] (FOIA), promulgado por el Presidente Lyndon B. Johnson el 6 de Septiembre del 1966 al cual fueron adicionadas enmiendas en el 1996, 2002 y 2007. Durante el periodo comprendido entre 1982 y 1995, estuvo en vigor la *Executive Order 12,356* de 1982 del Presidente Ronald Reagan, que permitía a las Agencias Federales restringieren el acceso a la información bajo la excepción 1(Exemption 1). Esta Orden Ejecutiva fue revocada por el Presidente Clinton en 1995[6] . En 1996 es publicado el *The Electronic Freedom of Information Act Amendments*[7], y en noviembre de 2001,

[4] SCHWARTZ, P.M. & REIDENBERG, J.R., Data Privacy Law, 1996; REIDENBERG, J.R., *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); REIDENBERG, J.R., *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); REIDENBERG, J.R. & GAMET-POL, F., *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105 (1995); REIDENBERG, J. et al., *The Privacy Debate: To What Extent Should Traditionally "Private" Communications Remain Private on the Internet?,* 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 329 (1995); REIDENBERG, J.R., *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 FED. COMM. L.J. 195 (1992); REIDENBERG, J.R., *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services,* 60 FORDHAM L. REV. S137 (1992).

[5] Public Law 89-554, 80 Stat. 383; Amended 1996, 2002, 2007

[6] Véase a este respecto, "*FOIA Post: FOIA Amended by Intelligence Authorization Ac*t". United States Department of Justice Office of Information and Privacy. 2002. http://www.usdoj.gov/oip/foiapost/2002foiapost38.htm.

[7] Para el panorama actualizado del sistema normativo en materia de Acceso a la Información ver el Portal del Departamento de Justicia http://www.usdoj.gov/oip/

el Presidente Bush firma la *Executive Order 13233*, con serias restricciones al Acceso a la Información, que será revocada por el Presidente Barack Obama por la *Executive Order 13489* de 21 de enero de 2009. En 2002 es promulgado por Georges Bush el *Intelligence Authorization Act* y en el 31 de diciembre de 2007 el *OPEN Government Act,* cuyas estipulaciones son semejantes a la LFTAIG mexicana y recogen los principios de quinta generación.

Sin embargo, este andamiaje jurídico garantista ha sido colocado frente a una política de seguridad que ha explorado las áreas grises al límite, bajo interpretaciones sui generis producidas por el Departamento de Justicia, en particular durante el primer período de la Presidencia de Obama, culminando una lenta transformación de los Estados-Unidos en lo que muchos llaman un nuevo estado totalitario informacional. De Daniel Ellsberg, pasando por Julian Assange, Bradley Manning y ahora Edward Snowden, Estados-Unidos se ha progresivamente transformado en un estado totalitario cibernético con objetivos y métodos que nos recuerdan la antigua Unión Soviética y en que la primazia de la ciberseguridad y la obsesión por la guerra contra el enemigo invisible (post 9/11) tienen precedencia sobre las garantías constitucionales**.**

2.2. *En el Derecho Comunitario (UE)*

Entre el 1995 y el momento actual, las autoridades legislativas y ejecutivas de la Unión Europea (UE) publicaron diversos textos legislativos en materia de Protección de Datos, cuyos principales son: la Directiva 95/46/CE; y la Directiva 97/66/CE[8]; y las cuales sirven como base para las demás directivas, que son las siguientes: la Directiva 2000/31/CE; la Directiva 2001/497/CE; la Directiva 2002/58/CE; la Directiva 2004/48/CE; la Directiva 2009/136/CE; y la Directiva 2012/0011 (COD).

Actualmente el grande debate en el terreno europeo se da sobre la cuestión de las violaciones al derecho fundamental a la intimidad y de rupturas de seguridad en ambientes en red. Un caso paradigmático es la cuestión de la protección de datos de los usuarios de las redes sociales y de la invasión de su privacidad por las poderosas herramientas de los metabuscadores. La posición doctrinal (y la jurisdificación de estos derechos) en la UE se encuentra entre las recomendaciones del Grupo del Artículo 29, las posiciones enunciadas por el Abogado general[9], por ocasión de las sentencias del Tribunal europeo en el

[8] DA CUNHA LOPES, T.M.G., "La creación de una Política Europea de Protección de Datos Personales", Alfa-redi, 2012 [10 de Julio del 2017]. http://www.alfa-redi.org/node/8833.

[9] El texto de las conclusiones del Abogado General del 25 de junio del 2013 puede ser consultado en la dirección http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=es&mode=req&dir=&occ=first&part=1&cid=991239.

caso Google y la redefinición de los alcances y límites del derecho al olvido, en la sentencia final de la Corte de Justicia sobre el Asunto C-131/12[10]. Este caso plantea la cuestión de conceder (o no) a los usuarios de Internet la posibilidad de suprimir los datos personales (como imágenes, textos, opiniones, documentos oficiales, certificados y cualquier otro tipo de datos personales que describen los comportamientos y acciones pasadas) de la lista de resultados servida por los motores de búsqueda o publicados en sitios web, redes sociales, blogs, etc.[11].

Esta sentencia, que tendrá consecuencias de gran alcance, no sólo en su aplicación en el territorio de los 28 estados miembros, pero como referencia jurisprudencial para las decisiones futuras de nuestra Suprema Corte en casos afines. La sentencia refleja un renovado entusiasmo por los derechos fundamentales a la privacidad y protección de datos (que aplaudo) aunque tal vez a expensas del derecho a la libertad de expresión. Si bien la Corte es normalmente cauta en su enfoque de equilibrio entre los derechos fundamentales, tal precaución es el gran ausente en este juicio. La Corte reafirma el derecho a la protección de datos, en primer lugar, asegurando el amplio ámbito de aplicación de la Directiva. El fallo de la Corte al referirse directamente al artículo 10 del CEDH y al artículo 11 de la Carta de la UE , que protegen el derecho a difundir y recibir información en este sentido es bastante significativo. La Corte parece ser de la opinión que sólo el "interés público" puede superar a los derechos a la protección de datos personales y privacidad. Por lo tanto intermediarios como los buscadores, en este caso preciso Google, deben proteger la privacidad sobre la libertad de expresión, excepto en circunstancias limitadas.

2.3. *La Protección del Derecho a la Intimidad y a la Protección de Datos en México*

En el caso particular de México, resulta prioritario tratar el proceso de constitucionalización como una materia federal, lo que ha sido alcanzado en el 2009 con la reforma al art. 73 constitucional.

En nuestra opinión, dada la importancia, la trascendencia, el carácter global e internacional de la Internet, de las Tecnologías de Información y Comunicación y de las herramientas tecnológicas que pueden afectar las relaciones económicas y

[10] El texto integral de la Sentencia del Tribunal de Justicia de la UE puede ser leído en la dirección web http://ep00.epimg.net/descargables/2014/05/13/5ba6db7a62470eb16ac8feb397cf936d.pdf

[11] GOMES DE ANDRADE, N. N., "El olvido: El derecho a ser diferente… de uno mismo. Una reconsideración del derecho a ser olvidado", en Revista de Internet, *Derecho y Política*, Vol.1, nº 13 (2012) 67 y 83.

sociales, lo ideal u óptimo es que se elevara a nivel federal la materia informática, sea cual sea su ámbito de aplicación o la rama del Derecho en la que incida. En consecuencia, consideramos que la reforma de la Constitución Política de los Estados Unidos Mexicanos en su artículo 73 es un acto de transcendental importancia.

A su vez, la reforma del artículo 16 Constitucional establece que:

> "*Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento*".

Reinterpretando *contra sensu* tal declaración, se puede argumentar que solamente por medio de un mandato escrito y que suscriba una autoridad competente, es posible "molestar a una persona" siempre y cuando dicha autoridad funde y motive, legalmente, su proceder. Primeramente es necesario apuntar que el sentido del artículo 160. Constitucional es proteger a los individuos de cualquier perturbación que puedan sufrir, sin que exista de por medio, mandato legal alguno, es decir, excluir de todos aquellos que sin ser autoridades mandatadas, la posibilidad de molestar a un individuo. Ahora bien, esa molestia puede realizarse a través de diferentes actos entre los que se pueden encontrar atentados contra la Intimidad. Sin embargo, aun cuando el artículo 16 de la C.P.E.U.M. protege los derechos de los ciudadanos a la privacidad de sus hogares, de la información y las comunicaciones, dejaba lagunas sobre la protección del concepto moderno de datos personales, razón por la cual es de fundamental relevancia la adición de un segundo párrafo el 1 de junio del 2009:

> "*Artículo Único.- Se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que proceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan*

que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión".

Si bien tradicionalmente el primer párrafo del artículo 16 constitucional solamente se ha analizado desde la perspectiva de la legalidad de los actos de autoridad, la inviolabilidad del domicilio o de la protección de la libertad individual, en la actualidad tal artículo se puede interpretar plenamente en relación con todas las cuestiones inherentes a la persona, entre ellas, la Intimidad, específicamente la informática, y como consecuencia la protección de sus datos personales[12].

La primera, en términos históricos, ley secundaria en que aparecen protecciones específicas a la protección de datos es la LFTAIG. En su origen la LFTAIPG aparece como un instrumento necesario para incrementar la confianza de los ciudadanos mexicanos después de un largo período de secretismo y de corrupción bajo el reinado priista (PRI) de 1929 al 2000 y no como una legislación protectora de los derechos fundamentales a la privacidad, a la Intimidad y a la autodeterminación informática. En este sentido, los objetivos de la LFTAIG incluyen: dotar la administración pública de transparencia, otorgar a los ciudadanos la facultad de solicitar información pública a los poderes Ejecutivo, Legislativo y Judicial Federales y de contribuir a la democratización de la sociedad mexicana y a la instauración de un estado de derecho. El Capítulo IV de tal ordenamiento sostiene una serie de obligaciones para el sector público entre las que destacan en su artículo 20.No debemos obviar que los abusos relativos al tratamiento de datos personales provienen esencialmente del sector privado, por lo que esta Ley, al regular exclusivamente, las obligaciones de los sujetos de derecho público, no alcanza a prevenir las lesiones que pueda sufrir un individuo en su esfera personal por parte de este sector privado. Así, México ha promulgado recientemente una *Ley Federal de Protección de Datos Personales en Posesión de particulares que* fue publicada el día 5 de julio del 2010 en el D.O.F[13].

Sobre la cuestión de los Principios, recoge las directivas del Simposio de Viena sobre la necesidad de que la información fluya de forma regulada entre los países y sobre el derecho de los países firmantes de imponer regulaciones

[12] Cfr. OVALLE FAVELA, J., "Comentario al artículo 16", en *Derechos del pueblo mexicano. México a través de sus constituciones*, Porrúa Editor, México 62003, t. III, pp. 163 y ss.

[13] Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. D.O.F. ver: http://www.dof.gob.mx/nota_detalle. php?codigo=5150631& fecha=05/07/2010.

para el flujo de datos que pueda resultar contrario al orden público o a la seguridad nacional y establece la definición de "*dato personal*" en el art. 2 transitorio:

> *"Artículo segundo. Se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para quedar como sigue: Artículo 3.- Para los efectos de esta Ley se entenderá por: I. ... II. Datos personales: Cualquier información concerniente a una persona física identificada o identificable".*

Esos datos contienen rasgos distintivos que sólo conciernen a ese individuo y que lo hacen único. Tal como lo explica el propio IFAI, organismo de tutela:

> "*Entonces, la protección se realiza sobre el dato, de manera que éste no pueda ser tratado o elaborado, y convertido en información, nada más que para aquellos fines y por aquellas personas autorizadas para ello. Esta necesaria protección es un límite a la utilización de la informática ante el temor de que pueda agredir la Intimidad o privacidad de los ciudadanos, personal, familiar o socialmente, y que pueda coartar el ejercicio de sus derechos*".

Tanto en el espíritu como en la letra, es evidente que los legisladores mexicanos se apoyaron e inspiraron directamente en el marco normativo europeo, empezando por el Convenio No. 108 del Consejo Europeo, del cual retoma la perspectiva de protección de los Derechos Humanos, concretamente su objetivo de garantizar el derecho a la vida privada de los individuos, con respecto al tratamiento automatizado de los datos de carácter personal. Otro importante referente legislativo de la nueva normatividad mexicana es la *Directiva 95/46/CE.* Tal como lo enfatiza la exposición de motivos de la *Ley Federal de Protección de Datos en Posesión de Particulares*, la tendencia mundial apunta hacia la regulación jurídica de los datos personales, hecho que fundamenta en la presentación de un listado de cuarenta países que cuentan con regulación jurídica en el tema de Protección de Datos personales.

En resumen, podemos observar que existen referentes legales en materia de protección a la Intimidad y Privacidad, tanto en la Constitución de los Estados Unidos Mexicanos (C.P.E.U.M.), como en Leyes Federales así como en la legislación secundaria, y observamos la transcendencia constitucional de la Protección de Datos Personales, establecida por la reforma al art. 16 Const. A su vez, a reforma del 73 Const. y la nueva Ley Federal de Protección de Datos en Posesión de Particulares, subsanan las lagunas existentes en la LFTAIG.

Sin estas reformas, México quedaría fuera de los circuitos comerciales y de los flujos transfronterizos establecidos al interior del triángulo demarcado por los dos tratados de Libre Comercio, el primero con América del Norte y el segundo con la Unión Europea.

Finalmente, en la C.P.E.U.M., los artículos 7 y 16 establecen criterios tutelares de la privacidad e Intimidad de las personas. En el art.7 constitucional se prevé como límite a la libertad de imprenta el respeto a la vida privada. En el art.16 se regulan dos aspectos relevantes de la garantía protectora del Estado: la inviolabilidad domiciliaria y de las comunicaciones privadas y el Habeas Data.

III. ESTUDIO DE CASO: LOS CRITERIOS JURISPRUDENCIALES DE LA SCJN SOBRE LA "LEY DE GEOLOCALIZACIÓN" Y LOS LÍMITES A LOS DERECHOS FUNDAMENTALES VERSUS SEGURIDAD NACIONAL

En este debate sobre la cuestión de los principios constitucionales versus riesgos tecnológicos, el análisis de la acción de inconstitucionalidad sobre la "ley de Geolocalización" mexicana es extraordinariamente elocuente y permite, a través de la enumeración de los argumentos doctrinales y criterios jurisprudenciales evidenciar la complejidad del mismo.

Los Ministros de la SCJN avalaron, el jueves 16 de enero 2014, la llamada "Ley de geolocalización" de celulares, que coloca el problema de un equilibrio complejo entre derechos fundamentales y seguridad nacional. La discusión en la corte se inició después de una acción de inconstitucionalidad promovida por la Comisión Nacional de los Derechos Humanos (CNDH), contra las reformas al Código de Procedimientos Penales, el cual permite a la Procuraduría General de la República (Fiscalía) acceder directamente a la ubicación de teléfonos celulares en el cuadro de una investigación, sin que exista para tal un mandato judicial .Se trata de la Demanda de acción de inconstitucionalidad 32/2012, presentada ante la Suprema Corte de Justicia de la Nación, el 11 de mayo del 2013, en contra del artículo 133 Quáter del Código Federal de Procedimientos Penales y los artículos 16, fracción I, apartado D y 40 Bis de la Ley Federal de Telecomunicaciones.

Desde luego nos encontramos frente a un asunto en el que se alega la violación, como quiera que sea, del derecho fundamental a la privacidad que de acuerdo con el promovente de la acción, la CNDH está protegido por los artículos 14 y 16 de la Constitución. Sin, embargo, la decisión de la Corte es

contraria a la demanda de acción de inconstitucionalidad interpuesta por la CNDH ya que prevaleció la fuerza del argumento del principio de la proporcionalidad y la necesidad de acción en "tiempo real" del Ministerio Público, que al estar en la necesidad de rastrear y localizar el punto focal del origen de una llamada, lo tiene que hacer en tiempo real, elemento de vital importancia y fundamental para la eficiencia y resultados en la investigación, inclusive, en algunos casos, determinante para las posibilidades de sobrevivencia de la víctima.

A pesar de que la mayoría de los ministros se ha declarado a favor de que autoridades federales localicen teléfonos celulares relacionados con crímenes sin orden judicial, la Suprema Corte de Justicia de la Nación (SCJN) aceptó modificaciones al proyecto de resolución, bajo la ponencia de la Ministra Margarita Luna Ramos, en las cuales se incluyan las excepciones en las que esa facultad podrá utilizarse.

Ocho de los 11 ministros votaron a favor del proyecto, pero con algunas diferencias de criterios que recuperan la división habitual entre tres grandes grupos doctrinales que se han venido dibujando, a partir del 2009, en cada contradicción de tesis o en cada acción de inconstitucionalidad: conservadores a ultranza que interpretan el derecho bajo el paradigma positivista, pragmáticos cuyos criterios jurisprudenciales conforman un terreno intermedio que ha permitido acuerdos importantes y avances jurisprudenciales y una minoría garantista, sin la cual la Corte no hubiera podido operar en el sentido transformador y diría yo, "civilizador" en estos últimos años. Cuatro ministros respaldaron el proyecto de la ponencia en sus términos, o sea en su versión "dura". Son ellos, Luis María Aguilar, Jorge Pardo Rebolledo, Alberto Pérez Dayán y Margarita Luna Ramos. Estos cuatro ministros consideran que la ley es una herramienta necesaria para combatir delitos graves como el secuestro y la extorsión, que aumentaron en el último año, y que la geolocalización no representa una violación a la intimidad porque localizar un teléfono celular no conlleva la intervención de llamadas o de sus mensajes.

Sin embargo, otros cuatro consideraron que era necesario que la Suprema Corte fijara los criterios que deberá seguir la PGR (Fiscalía), a fin de evitar abusos contra los ciudadanos. Arturo Zaldívar, uno de esos cuatro ministros , consideró que no basta con que la ley señale que la medida únicamente podrá emplearse cuando se trate de delincuencia organizada, narcotráfico, secuestro, amenazas y extorsión, sino que debe restringirse a "casos de urgencia", es decir, cuando peligre la vida o la integridad de una persona o el objeto del delito pueda desaparecer. Tres ministros se pronunciaron en contra -Olga Sánchez Cordero, Sergio Valls y José Ramón Cossío, -para quienes esta medida es inconstitucional porque viola el derecho humano a la privacidad. "La norma

es eminente y frontalmente inconstitucional por no contener los elementos para salvaguardar el derecho a la privacidad. (…) El punto de partida debe ser el derecho humano que protege la Constitución y no la facultad de investigación (de la PGR)", dijo Cossío[14]. Refutando esta posición, en la primera parte del análisis, algunos ministros establecieron una diferencia entre la geolocalización del origen de las llamadas, que implica una técnica de investigación judicial, y el seguimiento a una persona que conlleva aspectos legales sobre privacidad de que habría de interpretarse de manera integral. Un argumento relevante sobre la analogía que se podría establecer entre la "orden de cateo" y la "geolocalización" ha sido enunciado y desmontado por el Ministro Pérez Dayan:

> "*En el caso estamos frente a algo intangible, los datos de localización de un equipo de comunicación, desde donde se generó una llamada relacionada con alguno de los delitos a que se refiere la propia ley, es un tema de datos, es un tema intangible, sólo es la ubicación del lugar en donde se produjo o se está produciendo una llamada; es por lo que quisiera insistir que la denominación -objetos no alcanzaría a cubrir esta formalidad."*(…)[15].

O sea, al establecer esta distinción, se niega que lo que se persigue sea la localización material de un objeto, o la búsqueda de un objeto, ej. el celular. Lo que se busca es el dato intangible, la localización del lugar en el que se produjo o se está produciendo una llamada.

O una comunicación. La naturaleza de un dato intangible, por consecuencia, argumentó el Ministro Pérez Dayan implica que no se esté en el supuesto exacto de los cateos, el instrumento jurídico constitucional que permite localizar un objeto y que está cubierto por el supuesto específico del artículo 16, que obliga a pasar necesariamente por la formalidad prevista en el artículo constitucional citado y por ende por el escrutinio de un juez.

Contra esta posición se colocó el Ministro Gutiérrez Ortiz Mena, ya que parte del argumento de que esa actividad de localización de ese teléfono móvil se hace respecto de bienes que son disponibles en tanto que están en el espectro radioeléctrico, y que son solicitables a la empresa de telecomunicaciones

[14] Ver SCJN , Seguimiento de Asuntos Resueltos por el Pleno de la Suprema Corte de Justicia de la Nación, Acción de inconstitucionalidad 32/2012"Valida SCJN las normas que sustentan la geolocalización de los equipos de comunicación móvil vinculados a delitos considerados graves", consultado 4 de abril 2014 en http://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=139112&SeguimientoID=575

[15] Ídem.

en tanto registro de un dato de localización con independencia de la vinculación que se tiene con una persona o un derecho de alguna persona. El ministro Ortiz Mena, en una posición retomada en su resumen por el Presidente de la SCJN, Juan Silva Meza, propuso, en ese punto del debate en el pleno, un catálogo de las restricciones, condiciones, o sea de una interpretación conforme necesaria para que esta localización en esa caracterización: "que se hace pueda llevarse a cabo por quien está constitucionalmente facultado para llevar una investigación a partir de los artículos 21 y 102 constitucionales, que rigen también sin desdoro de la XIV y XVI, la actividad pública de la autoridad, ahí están y tienen que tener esa circunstancia, pero es una perspectiva que es armonizable"[16].

Creo que la propuesta de integralidad, o sea, interpretación conforme a partir de que se interprete a la luz de todos los principios constitucionales, de que se interprete a través del marco de derechos humanos de fuente internacional, de las sentencias obligatorias nuestras como Suprema Corte, y de las sentencias de la Corte Interamericana debería prevalecer.

VI. REFLEXIONES FINALES

Las circunstancias en que las personas interactúan entre sí se han alterado dramáticamente desde la década de 1980 de manera que se han transnacionalizado las prácticas sociales y políticas. Estos cambios fueron introducidos por un conjunto de circunstancias en que las relaciones locales, nacionales y globales estimuladas por la invención de nuevas tecnologías de la comunicación y de transporte, crearon la creciente interdependencia económica y el desarrollo de sistemas de gobernanza mundial que incorporan a los Estados, pero se extienden para allá (y a través) de los Estados-nación.

Nuevos problemas globales asociados con el desarrollo económico, la energía nuclear, la salud, la ecología y los riesgos tecnológicos han surgido que tienden a unir juntos las oportunidades de vida de las personas en todos los países en las redes complejas de interdependencia. Las nuevas estructuras de interacción de las sociedades contemporáneas han aumentado la capacidad de las personas para conectarse y colaborar con otras personas más allá de su ubicación física inmediata. Ellas han abierto oportunidades para encontrar una gama mucho más diversa de personas, bienes, ideas y proyectos colectivos.

Al mismo tiempo, sin embargo, también debemos reconocer que el desarrollo de las conexiones transnacionales es a menudo involuntaria, a veces coercitiva y

[16] Ídem

sus "oportunidades" y posibilidades desigualmente distribuidas en función del país y de la esfera social en la que se encuentran las personas .El aumento de la movilidad de las personas, de los productos básicos y de las ideas es, pues, una característica central de esta nueva era de la interacción humana en la que las fronteras territoriales de la mayoría de los estados-nación son ahora porosas. Los límites de la nacionalidad se han desdibujado por la pluralización cultural, derivados de la migración, multiculturalismo étnico, la diversidad cultural de todo tipo, y las crecientes demandas de reconocimiento de las diferentes opciones de vida. Estos cambios son a menudo considerados, tal como lo propuso Castells en 1996, como un cambio en la democratización de las relaciones sociales y políticas de los espacios territoriales relativamente cerradas de los estados-nación para abrir, las relaciones en red que atraviesan el globo entero. Esta interpretación lineal, sin embargo, oculta una imagen mucho más ambivalente. Es verdad que muchas redes basadas en la comunicación en Internet son relativamente abiertas, a pesar de los diversos niveles de la censura estatal y la creciente prominencia de paywalls contenido. Pero, en su opuesto, muchas de las redes globales y transnacionales, que van desde grupos empresariales a las organizaciones criminales, son tan cerradas y jerárquicas como los estados territoriales, si no más.

Redes funcionales o redes de información nuevas, a menudo crean nuevos límites en que la participación depende del nivel educativo, de las credenciales sociales, del acceso a la tecnología y del control más amplio de los recursos materiales y culturales. Sin embargo, esta opacidad de las redes funcionales anudado a las estructuras securitarias de los estados en la era de la seguridad global, han dejado al individuo en una posición potencialmente débil en que el ejercicio de sus derechos fundamentales puede estar en recesión. El nivel que presenta los riesgos más evidentes para el ejercicio efectivo de derechos y libertades es, tal como ya lo vilos a lo largo de este artículo, el de la masificación de datos y de las posibilidades de geolocalización y, por ende de producción de biopolíticas de seguridad. Nuestra última barrera, la constitucionalización del principio de autodeterminación informática se derrumba frente al carácter difuso de la soberanía en la sociedad de la información. Es altura, por lo tanto, de pensar en un encuadramiento normativo y en órganos de tutela supranacionales.

VII. REFERENCIAS BIBLIOGRÁFICAS

- ACUÑA LLAMAS, F. J., "*Dos caminos hacía la protección integral de los datos personales en México*", en VILLANUEVA, E., y LUNA PLA, I. (eds.), *Derecho de acceso a la información pública: valoraciones iníciales*, UNAM, USAID, FKA, México 2004.

- CEVALLOS, D., *México: Transparency Law-A vaccine against corruption*, WL 6915685, June 12, 2003, 80.

- DADA ESCALANTE, P., "I*nformación contra Privacidad*", en *México entra a la era de la transparencia*, Instituto de Acceso a la Información (IFAI), México 2004, 4.

- D.O.F (Diario Oficial de la Federación), http://www.dof.gob.mx/

- GERALDES DA CUNHA LOPES, T. M., "*La Protección de Datos Personales en México*", Facultad de Derecho y Ciencias Sociales/CIJUS, 2010.

- GERALDES DA CUNHA LOPES, T. M., y MAGALLÓN HIGAREDA, S., *Legislaciones y Autoridades Reguladoras de las Entidades Federativas en Materia de Derecho de Acceso a la Información y Protección de Datos en México*, Facultad de Derecho y Ciencias Sociales/CIJUS, México 2010.

- GOMES DE ANDRADE, N. N., "El olvido: El derecho a ser diferente… de uno mismo. Una reconsideración del derecho a ser olvidado", en Revista de Internet *Derecho y Política* Vol. 1, nº 13 (2012) 67 y 83.

- MAYER-SCHÖNBERGEN y CUKIER, *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt, 2013.

- OVALLE FAVELA, J., "Comentario al artículo 16", en *Derechos del pueblo mexicano. México a través de sus constituciones*, Porrúa Editor, México 2003, t. III.

- REIDENBERG, J. R., *Privacy in the information economy: A fortress or frontier for individual rights*. *Fed. Comm. LJ*, *44*, 195 (1991).

- RYSDALL, R., "Protección de Datos y el Convenio Europeo de los Derechos Humanos. Discurso de apertura de la XIII Conferencia de Comisarios de Protección de Datos", en *Novática*, marzo de 1992.

- SCJN, Seguimiento de Asuntos Resueltos por el Pleno de la Suprema Corte de Justicia de la Nación, Acción de Inconstitucionalidad 32/2012 "Valida SCJN las normas que sustentan la geolocalización de los equipos de comunicación móvil vinculados a delitos considerados graves", consultado 4 de abril 2014 en http://www2.scjn.gob.mx/AsuntosRelevantes/pagina/SeguimientoAsuntosRelevantesPub.aspx?ID=139112&SeguimientoID=575

- SCHWARTZ, P., y REIDENBERG, J. R., "Data privacy law: a study of United States data protection", en *LEXIS Law* (1996).