HORNELAS PINEDA, Carlos Manuel. La protección de datos personales y la sociedad del control. *Revista In Jure Anáhuac Mayab* [online]. 2014, año 2, núm. 4, ISSN 2007-6045. Pp. 135-153.

LA PROTECCIÓN DE DATOS PERSONALES Y LA SOCIEDAD DEL CONTROL

PROTECTION OF PERSONAL DATA AND CONTROL SOCIETY

Carlos Manuel HORNELAS PINEDA*

Un paranoico es alguien que sabe un poco de lo que está pasando.
William S. Burroughs

RESUMEN. El incremento del uso de diversos dispositivos electrónicos posibilita intromisiones no deseadas a los datos personales de los individuos, lo cual plantea una infracción al derecho a la privacidad. Organismos tanto privados como públicos tienen acceso a datos personales a través de la tecnología digital que redundan en su propio beneficio y sirven como instrumentos de control social.
Palabras Clave: Datos personales, derecho a la privacidad, internet, videovigilancia, control social

ABSTRACT. The increased use of electronic devices has made it possible to access individuals' personal data, violating their right to privacy. Through digital technology, public and private companies use that personal information to obtain economic benefits or as social control techniques.
Keywords: Personal data, Right to Privacy, Internet, electronic surveillance, social control

I. Introducción.

En la actualidad una triple mirada acecha. Somos observados por ojos públicos, a través de cámaras de videovigilancia colocadas por el gobierno para cuidar la seguridad de los ciudadanos. Nos escrutan, asimismo, ojos privados que escudriñan lo que hacemos en el

* Maestro en Comunicación Institucional, Profesor / Investigador de la Escuela de Comunicación y Alumno del Doctorado de Gobierno y Gestión de Políticas Públicas de la Universidad Anáhuac Mayab. Mérida, Yucatán. carlos.hornelas@anahuac.mx 942-4800 ext. 563

supermercado, en las oficinas en las que trabajamos, en las tiendas de conveniencia o al interior de las escuelas. Lo hacen a través de diversos dispositivos para monitorizar: cámaras, pantallas, espejos, actividad en la red, entre otros. Finalmente, ojos indiscretos atentan contra la intimidad de las personas: cualquier ciudadano puede tomar una fotografía con algún dispositivo inteligente y la puede subir y publicar en la red casi de manera simultánea sin que lo notemos o consintamos. Algunos pueden pensar que la vida privada ha cedido terreno o que simplemente se han difuminado las fronteras entre lo público y lo privado.

Mientras gozamos de las bondades de la tecnología moderna, de esto que se ha llamado la Sociedad de la Información, también debemos cuestionarnos si el precio de comodidades se da a cuenta de la renuncia a la pretendida privacidad. Del extremo contrario al de la seguridad se encuentra el control y la vigilancia. Las intromisiones y prácticas de espionaje de la privacidad individual podrían ser objeto de una revisión profunda desde el punto de vista democrático. La tecnología también puede verse como fuente de producción de nuevas formas de acotamiento de la vida privada, incluso en el ámbito laboral, donde los medios informáticos son empleados so pretexto de aumentar la productividad y terminan siendo banco de información detallada de las actividades y rendimiento de los sujetos que los empleadores pueden revisar.

II. La protección de datos personales en México.

La protección de datos personales en el país es una preocupación relativamente reciente, que puede remontarse a una década atrás, con la promulgación de la primera Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en 2002. A partir de entonces la sociedad civil ha presionado por aumentar la lista de sujetos obligados a presentar información sobre áreas que gracias a la discreción de sus autoridades era frecuentemente negada. Como efecto colateral, en los años recientes la atención al tema ha girado hacia la protección de datos personales en manos de particulares.

La literatura en materia de transparencia se ha incrementado considerablemente en los últimos años. Sobre todo el área académica ve en este nuevo objeto de estudio una interesante intersección para el derecho, la gestión de políticas públicas, la sociología y la comunicación.

La problemática legal de la definición de los datos personales en México inicia con la ambigüedad con la cual se refiere a ellos desde diversos puntos de vista para el

profesional del derecho. Los datos personales pueden entenderse bien como una extensión o parte de su personalidad, colocándolos de este modo como un derecho de la persona y en el caso de su reconocimiento a través del artículo sexto constitucional, un derecho fundamental.

Asimismo los datos personales se relacionan con los conceptos de derecho de imagen, derecho de réplica, derecho a la autodeterminación informativa, Derecho a la Privacidad e intimidad y particularmente a la capacidad de oponer recursos ante las instancias correspondientes para el acceso, rectificación, cancelación y oposición de información inexacta que obre en las bases de datos de instituciones y /o empresas.

Un leve vistazo a la evolución histórica de las modificaciones de los artículos 6° y 16° Constitucionales puede dar cuenta de la transformación del concepto dentro del marco jurídico, así como, dependiendo del momento coyuntural, el legislador ha añadido fracciones a dichos artículos en respuesta a circunstancias políticas específicas.

La protección de datos personales en México tiene como antecedente obligado la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada el 11 de junio del año 2002 en el Diario Oficial de la Federación. Esta disposición debe entenderse como el cumplimiento de un compromiso contraído durante su campaña por el entonces Presidente de la República, Vicente Fox Quesada. Surge como una alternativa para proteger el derecho del ciudadano contra los actos de la autoridad que hacían opaco su proceder en algunos temas, en particular el de la rendición de cuentas; así como todos aquellos relacionados con el erario y la discrecionalidad para ejercer el gasto público.

Posteriormente, el 20 de julio de 2007 se da a conocer en el Diario Oficial de la Federación la modificación al artículo sexto constitucional, por la cual se incorporan los principios y criterios básicos que deberán regir el acceso a la información como derecho fundamental. Como se detalla a continuación:

> A. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: (Adicionado mediante decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007. Reubicado mediante decreto publicado en el Diario Oficial de la Federación el 11 de junio de 2013, convirtiéndose en apartado a.)

> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. (Adicionada mediante decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007.)
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. (Adicionado mediante decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007.)
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos. (Adicionada mediante decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007.)
>
> IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciaran ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión. "(Adicionada mediante decreto publicado en el Diario Oficial de la Federación el 20 de julio de 2007.)

Para los efectos de esta exposición, las fracciones II y III cobran una relevancia específica. En lo que se refiere la fracción segunda, se puede pensar que una de las acepciones que tienen los datos personales dentro de nuestra Carta Magna eleva a derecho fundamental la protección a la privacidad.

El caso de la fracción tercera, admite que la titularidad de los datos personales le pertenece a la persona, valga la redundancia, porque se podría decir, son una extensión de su personalidad que lo identifican; y por lo tanto, no es propiedad de quien los tenga en posesión. Razón por la cual, el afectado podrá solicitar la rectificación de sus datos cuando estime conveniente.

En el año 2007, en el marco de la nueva reforma electoral vigente, se fijaron condiciones específicas para la propaganda política de los candidatos a puestos de elección popular a través de los medios de comunicación masiva. En particular, los

concernientes a la radiodifusión, condicionando su difusión exclusivamente a los llamados tiempos del estado. Asimismo hubo una prohibición expresa de la realización de las llamadas "campañas negras" con el fin de denigrar, discriminar y/o zaherir a candidatos adversarios políticos. En ese orden de ideas, se añadió al artículo sexto constitucional el siguiente señalamiento "el derecho de réplica será ejercido en los términos dispuestos por la ley". Con esta incorporación se abre la posibilidad de que el afectado pueda solicitar una réplica a un medio de comunicación si la información que difunde es inexacta, lo cual lo ubica como una especie de rectificación.

Para el año 2009, se añaden una serie de fracciones al artículo 16 constitucional en diversas ocasiones. Desde el primer párrafo, se puede apreciar la protección a la esfera íntima de la persona cuando se afirma 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." Esto constituye un claro señalamiento de aquello que ha sido llamado Derecho a la Privacidad y/o derecho a la intimidad.

El segundo párrafo, por ejemplo establece la protección de datos personales de la siguiente manera:

> 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.

Este párrafo en particular es la inspiración para el acrónimo con el cual la doctrina internacional se refiere a estos derechos, se les ha llamado derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Más adelante acota:

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la

> comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.
>
> Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración.
>
> La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

El 30 de abril del 2009, en el Diario Oficial de la Federación se publicó una adición al artículo 73 constitucional, el cual señala en su fracción XXIX-O las facultades exclusivas del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares. Lo cual equivale a admitir que esa materia es solamente de carácter federal.

Asimismo, establece que tiene facultad:

> XVII. Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.[144]

El 5 de junio de 2010 se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Si la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental ya vela por los datos del ciudadano común y corriente ante los actos de abuso de autoridad, esta ley de reciente creación los datos personales en posesión de particulares, es decir, en aquellos casos en los que las bases de datos a las que se hace referencia no sean de carácter oficial ni estén soportadas por alguna dependencia del Estado.

De lo anterior se deduce que si un determinado particular, por ejemplo, una empresa o una compañía de bienes y servicios, mantiene una base de datos personales de sus clientes, deberá regirse por los principios y normas establecidas a nivel federal en

[144] Fracción reformada DOF 11-06-2013.

materia de datos personales en posesión de particulares, por el Congreso de la Unión y las leyes que determinen su momento. Asimismo esto quiere decir que las autoridades locales al interior de los estados no tienen ninguna competencia en materia de datos personales tratándose de particulares. Las autoridades locales tienen competencia solamente en lo que se refiere a los datos personales en posesión de las autoridades correspondientes. El órgano garante a nivel federal es el Instituto Federal de Acceso la Información y Protección de datos: IFAI.

Como se ha señalado anteriormente la legislación en materia de protección de datos personales tiene como antecedente obligado la ley federal de transparencia y acceso a la información pública gubernamental. En ese sentido, cabe mencionar que mientras que esta ley garantiza el acceso a la información, también incluye una serie de reservas al principio de máxima publicidad. Dicha ley plantea una diferencia entre la información reservada y la de carácter confidencial. Se entiende a la información reservada como aquella en manos de la autoridad que no puede ser divulgada a partir de un supuesto de seguridad nacional o una causa mayor. Mientras que la información de carácter confidencial engloba a los datos personales, de los cuales, se dice, requieren el consentimiento de los individuos para su difusión, distribución o comercialización.

Así, pues, la ley federal de transparencia y acceso a la información pública gubernamental en su artículo cuarto de la fracción III señala como objetivo de la ley: "garantizar la protección de los datos personales en posesión de los sujetos obligados".

En el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares afirma que "para los efectos de esta ley, se entenderá por: […] II. Bases de datos: el conjunto ordenado de datos personales referentes a una persona identificada o identificable." Más adelante, el mismo artículos los define como "V. Datos personales: cualquier información concerniente a una persona física identificada o identificable."

Sin embargo debe reconocerse el contexto de esta óptica con la cual opera dicha definición. Si bien un dato de un sujeto pueden ser, por ejemplo su estatura o su complexión, por sí solas estas medidas no constituyen un dato personal sino hasta el momento en que se asocien y establezcan de modo efectivo la posibilidad de identificar a un sujeto por su complexión, estatura, género, origen étnico, etcétera.

Por esa razón se habla de bases de datos en lugar de, simplemente datos. Mientras, en el mismo artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares diferencia los datos personales sensibles y los define como:

> VI. […] aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Cabe mencionar que la revelación de datos sensibles se castiga con una pena fijada como el doble de la que corresponde a la revelación de datos personales.

En el artículo sexto de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares se señala que "Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la ley".

Para tal efecto, se dice, los particulares deberán exhibir un aviso de privacidad en sus instalaciones, que le informe al ciudadano cómo se almacenarán los datos, con qué fines, hasta qué período y definirá a un responsable para la custodia y resguardo de estos datos personales.

Como puede colegirse la comprensión del tema gira en torno a las colindancias de derechos, en primer lugar; las diferentes acepciones de los datos personales a las que se hace referencia, en segundo; las motivaciones políticas que propician las modificaciones a los artículos que las elevan a derechos fundamentales. Asimismo, la evolución de las modificaciones a los artículos constitucionales permite vislumbrar que la explicación o parte de ella se encuentra a través de estos momentos históricos que articulan tanto las apreciaciones teóricas que les respaldan como su traducción a la práctica cotidiana.

III. Caracterización de los usuarios de internet en México.

De acuerdo con la Asociación Mexicana de Internet (AMIPCI), en el reporte presentado el pasado 17 de mayo de 2013 en el marco de la conmemoración del día internacional de Internet, titulado "Hábitos de los usuarios de Internet en México 2013" se da a conocer un crecimiento del 10% de usuarios desde-2012 al 2013, de tal modo que la cifra alcanzada es de 45,1 millones de usuarios.[145]

[145] Véase en http://www.merca20.com/wp-content/uploads/whitepapers/redes-sociales-whitepaper-2013.pdf, consultado el 21 de mayo de 2014.

El estudio establece que existe una equidad en el empleo de internet dado que 51% de los usuarios son hombres y 49% mujeres. Asimismo, casi el 30% de los internautas en México se encuentra entre los rangos de 25 a 44 años. Durante 2013 el tiempo promedio de conexión diaria del internauta mexicano fue de 5 horas y un minuto, 67 minutos más que en 2012.

Las tres principales actividades que desempeña el internauta mexicano son: envía/ recibe correo electrónico 87%; búsqueda de información 84% e ingreso a redes sociales 82%. También se especifica que 9 de cada 10 internautas mexicanos entran a una red social.

Los usuarios de mayor uso de las redes sociales son los consumidores de 25 a 34 años, alrededor del 50% afirman estar enlazados todo el día; 42% del segmento de 18 a 24 años las revisan de 6 a 9 veces al día y en general se conectan regularmente en las noches.[146] Las redes sociales más populares son: Facebook, Twitter y Youtube, en ese orden. Aunque hay ligeras variaciones de preferencia entre una y otra dependiendo de los usuarios por las diferentes edades de los usuarios.

Los usuarios de internet en México ingresan a las redes sociales desde su teléfono celular inteligente, su *tablet*, la computadora de escritorio o la computadora portátil. Aquí también se encuentran distribuidos por edad. Por ejemplo, los usuarios jóvenes de 18 a 24 años de edad lo hacen regularmente a través de computadoras portátiles, mientras que los de 25 a 34 años se conectan más a través de sus celulares inteligentes.

El advenimiento de las redes sociales virtuales como una de las actividades más socorridas por los internautas presupone diversos problemas de orden teórico, conceptual y práctico en relación con la protección de datos personales. El uso intensivo y exponencialmente en crecimiento del internet, en particular de las redes sociales virtuales, plantea interrogantes a propósito de las patidifusas fronteras entre la intimidad y la propensión a compartir datos a través de estas plataformas. Muy pocas personas en la red son conscientes de que al subir contenido o compartir información sus acciones pueden ser consideradas posibles infracciones a los derechos de imagen, a la seguridad de las personas, al secreto o sigilo en distintas clases de procedimientos así como en un espectro bastante amplio que rodea la llamada protección de datos personales para instituciones, empresas, organismos sociales y particulares.

Los datos personales en las redes sociales virtuales tienen colindancia con una serie de derechos que implican una problemática ya de suyo específica como: el derecho

[146] *Ídem.*

a la imagen, el derecho a la intimidad, el Derecho a la Privacidad, el derecho a la autodeterminación informativa, el derecho de réplica, el derecho de autor y el llamado "derecho al olvido" entre otros. A esto habrá que añadir que las redes sociales virtuales más populares no son nacionales y en ocasiones las compañías que las operan no tienen oficinas en nuestro país. Esto hace que los llamados derechos ARCO (acrónimo de Acceso, Rectificación, Cancelación y Oposición) sean más difíciles de hacer valer.

México no cuenta en su Constitución Política con la definición del llamado *Habeas Data* como ocurre como en el caso de algunos países latinoamericanos como Argentina en el cual admite la posibilidad de solicitud de un amparo a la autoridad correspondiente ante dichas violaciones. En el caso mexicano, el ciudadano se deberá dirigir ante el depositario de la información que requiere retirar o rectificar y en caso de serle negado su derecho, puede acudir ante los institutos de transparencia estatales si se trata de sujetos obligados, es decir entes públicos, o bien ante el IFAI si se trata de datos personales en posesión de particulares.

Por consiguiente, aunque la Ley Federal de Protección de Datos Personales y su reglamento tienen procedimientos específicos para la reclamación, tal pareciera que en la práctica dicha protección se reduce a la emisión de un aviso de privacidad como advertencia a los usuarios.

Entonces la reflexión gira alrededor del sujeto responsable de los datos en la empresa o compañía y alberga una serie de cuestionamientos sin resolver, por ejemplo ¿deberá existir sólo una persona responsable?, ¿No será mejor distribuir privilegios de consulta, acceso y distribución por niveles jerárquicos a varios responsables?

Para las redes sociales virtuales el llenado del formulario en línea que solicita incorporarse en cualesquiera de estas compañías, a cambio de un espacio público en la red funciona de facto como un contrato de adhesión que al presionar el botón "aceptar" otorga un claro consentimiento del sujeto para que la empresa en cuestión utilice sus datos personales en el modo que estime más conveniente a partir de ese momento. Además, en la inmensa mayoría de los casos las empresas no tienen sede en México lo cual hace de internet una cuestión extra-territorial.

Como puede apreciarse existe la posibilidad real de que diversos agentes sociales que van desde las instituciones públicas hasta las empresas trasnacionales intervengan directamente en ellas para su propio interés, con el detrimento de las libertades y derechos de la población en general.

Una reflexión sobre el marco de protección de una de las cuestiones más sensibles de la persona humana, como lo son sus datos personales, se hace necesaria. Delimitar y caracterizar aquello que puede ser objeto de protección es un debate actual que debe nutrirse de los aportes transdisciplinarios de la comunicación, el derecho y la política pública.

A medida que los usuarios son cada vez más demandantes de servicios otorgados a través de internet tales como la búsqueda de información, el entretenimiento, trámites oficiales o de consulta a órganos gubernamentales, las transacciones comerciales y el contacto con otros individuos empleando plataformas de redes sociales virtuales, sigue siendo un asunto pendiente el marco de regulación específico sobre la privacidad.

IV. La sociedad del control y a vigilancia.

A. *En la red, ¿somos la araña o la mosca?*

Los avances logrados en las Tecnologías de la Información y Comunicación (TIC)[147], constituyen la infraestructura de una plataforma global en línea que procesa y da tratamiento simultáneo a datos personales de los usuarios, que finalmente terminan con o sin su consentimiento tanto en manos del Estado, instituciones privadas, empresas comerciales o terceras personas, sirviendo de insumo para sus diferentes propósitos.

En la Sociedad de la Información las TIC actuales abarcan desde chips de memoria altamente eficiente; la convergencia de las comunicaciones digitales; la capacidad ilimitada de almacenamiento; el procesamiento ultrarrápido de altos niveles de información; los dispositivos móviles multipropósito; las redes sociales virtuales; el reconocimiento automatizado de rasgos faciales[148]; la geolocalización de datos y dispositivos en "tiempo real"; así como un incremento en la vigilancia, supervisión y monitoreo del flujo y contenido de correos electrónicos; ataques cibernéticos; escudriñamiento de características biométricas o genéticas; computación en la nube;

[147] Las TIC se definen como sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación entre dos o más interlocutores. Por lo tanto, las TIC son algo más que informática y computadoras, puesto que no funcionan como sistemas aislados, sino en conexión con otras mediante una red. También son algo más que tecnologías de emisión y difusión (como televisión y radio), puesto que no sólo dan cuenta de la divulgación de la información, sino que además permiten una comunicación interactiva. El actual proceso de "convergencia de TIC" (es decir, la fusión de las tecnologías de información y divulgación, las tecnologías de la comunicación y las soluciones informáticas) tiende a la coalescencia de tres caminos tecnológicos separados en un único sistema que, de forma simplificada, se denomina TIC (o la "red de redes"). *Cfr*. ONU- CEPAL. *Los Caminos Hacia Una Sociedad de la Información en América Latina y El Caribe*, Bávaro, Punta Cana, República Dominicana, 29 al 31 de enero de 2003[http://www.itu.int/wsis/docs/rc/bavaro/eclac-es.pdf] Consultado el 14 de enero de 2014, página 3.

[148] *Cfr*. "Reconocimiento facial", en *Biometría. Métodos biométricos*, Disponible en línea [http://www.biometria.gov.ar/metodos-biometricos/facial.aspx] consultado el 10 de febrero de 2014.

técnicas de visualización de datos a través de dispositivos digitales; dispositivos de identificación de radiofrecuencia (RFID[149]); hasta artefactos diminutos para la medición de características físicas de los individuos. Todos los cuales tienen en común el uso y / o tratamiento de datos personales.

A partir del advenimiento de las nuevas tecnologías de la información y la comunicación se ha adoptado una presunción básica acerca de la protección de datos personales basada en una moderna interpretación del Derecho a la Privacidad. Establece que cada persona tiene cualidades atributos o características únicas e irrepetibles distintas a todos los demás que configuran en su conjunto los elementos de su persona.

En ese sentido, la protección de datos personales se equipara con el derecho a la personalidad. Siendo entonces estos elementos constituyentes de la persona y que en conjunto permiten su plena identificación, es completamente razonable que se convierta en una prerrogativa individual su divulgación o reserva del modo en que más le convenga o interese, es decir, que en última instancia sea quien ejerza el control sobre sus propios datos, o bien consienta su tratamiento a terceros.

No obstante, en la actualidad hay un incremento sustancial de métodos cibernéticos o informáticos intrusivos e indetectables que pueden utilizarse para identificar, analizar, evaluar o crear perfiles individualizados de personas, que sirven como insumo a terceros, vulnerando con ello sus derechos fundamentales, y, peor aún, exponiendo su seguridad, dado que dicha información puede resultar hasta en acciones de localización y ubicación física para fines de todo tipo[150].

B. *Nosotros: la mercancía y los consumidores.*

Desde el punto de vista comercial, la tecnología permite la creación de perfiles personalizados de consumo y preferencias basados en la acumulación de información referenciada en los datos personales que delinean tendencias[151]. A modo de ejemplo, las

[149] *Cfr.* Alexandres Fernández, Sadot (*et. al.*), "RFID: La tecnología de Identificación por Radio Frecuencia", en *Anales de mecánica y electricidad*, Enero-Febrero 2006, Disponible en línea [http://dialnet.unirioja.es/servlet/articulo?codigo=1448367&orden=62874&info=link] páginas 47-52 Consultado el 30 de enero de 2014

[150] @ADN Político, *Sitio web revela datos personales...¿están los tuyos?,* en ADN Político, 7 noviembre de 2013, Disponible en línea [http://www.adnpolitico.com/gobierno/2013/11/07/tu-ife-curp-y-domicilio-estan-disponibles-en-un-sitio-web] Consultado 14 de enero de 2014

[151] "Precisamente la información de carácter personal ha sido necesaria en el proceso evolutivo de las tecnologías de la información y las telecomunicaciones y, sobre todo, de los servicios que se prestan a través de ellas. Una de las facetas de esa necesidad es, evidentemente, económica. Las empresas requieren de la creación de bases de datos que les permitan tener un mejor perfil de sus clientes y en el caso de las telecomunicaciones, sobre todo en lo que concierne a los prestadores de servicios, las bases de datos tienen un carácter esencial". Arellano Toledo, Wilma "Privacidad y protección de datos en internet: España, la Unión

compañías que operan a través de la nube conocen con precisión la última compra de música realizada en línea, y con–datos tan específicos como el número de la tarjeta de crédito, la dirección asociada para la facturación, el importe y fecha del consumo, el gusto por un determinado género musical y los dispositivos en los cuales se ha descargado la melodía[152].

Asimismo, la computadora del vehículo guarda el número de viajes, las trayectorias recorridas, su duración. En el caso de los *Smartphones* que comparten información con las redes sociales virtuales suelen sugerir encuentros con personas "interesantes" que son amistades potenciales, basados en los pasatiempos favoritos publicados como el tipo de lecturas, películas, lugares o intereses comunes. E incluso podrían enviar un aviso de alerta cuando detectan que se encuentran próximos, a partir del uso de instrumentos de geolocalización. La mayor parte de las redes sociales virtuales, por ejemplo, establecen como condición indispensable para intercambiar información, que las personas abandonen el anonimato en sus interacciones.

A fin de posicionar los productos y servicios, el procesamiento de datos ha sustituido en parte a las encuestas personales que proporcionaban estadísticas fiables sobre preferencias de consumo y a través del tratamiento de datos personales han logrado personalizar ofertas a clientes potenciales. Además dicha información es capaz de detectar tendencias y fluctuaciones, por pequeñas que sean, a lo largo del tiempo, toda vez que se acumula progresivamente y la muestra se incrementa exponencialmente, dándole estabilidad y aumentando con ello su nivel de confiabilidad.

La empresa Google[153] reúne datos del individuo en sus bases de datos para la creación de perfiles que logren automatizar la personalización de publicidad y mejorar las técnicas mercadológicas para su beneficio económico y su venta a terceros. Es posible medir el impacto de las comunicaciones móviles, las tendencias de su uso, interacciones

---

Europea y México" en Tenorio Cueto, Guillermo (Coordinador) 2012. *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*. Editorial Porrúa México. Universidad Panamericana páginas 143- 168-

[152] ADN político, *El IFAI indaga presunto espionaje en dispositivos móviles*, Disponible en línea [http://www.adnpolitico.com/gobierno/2013/07/05/el-ifai-indaga-presunto-espionaje-en-dispositivos-moviles], consultado el 14 de enero de 2014. El espionaje, según esta nota se realiza a través de un software que se autoinstala llamado Fin Fisher: Es un programa que puede infiltrase en computadoras, teléfonos celulares y otros dispositivos móviles mediante un archivo adjunto en un mensaje. Así el controlador del software puede tener acceso a datos personales como directorios telefónicos, conversaciones en audio o en texto y fotografías de los usuarios de cada equipo.

[153] *Cfr*. Rueda, Nicolás, "Google pagará multa por rastrear sin permiso a usuarios de Safari", en *MediaTelecom*, publicado el 19 de noviembre de 2013, Disponible en línea [http://www.mediatelecom.com.mx/index.php/tecnologia/internet/item/54373-google-pagara-multa-por-rastrear-sin-permiso-a-usuarios-de-safari], Consultado el 19 de noviembre de 2013

entre usuarios de ciertos sitios o páginas de internet, preferencias sociales de uso y consumo a través de diversos dispositivos.

De esta manera la colecta de datos personales se convierte en un modo de sistematizar verdaderas bases de datos simultáneas y "vivas" que se actualizan constantemente sin la intervención de las empresas para ingresar la información que sirve de insumo. Son, precisamente los usuarios de estos servicios en línea, quienes realizan la tarea de subir todos estos datos a la nube voluntariamente a cambio de los servicios prometidos. La mayor parte de las ocasiones las personas ignoran que su información es fuente de riqueza, así como también las políticas de tratamiento de datos de las empresas que les brindan el servicio. En el último de los casos, algunos individuos ven esta práctica como un mal necesario a fin de obtener servicios que son calificados de "gratuitos" como el correo electrónico o una página personal en las redes sociales virtuales. Así las cosas, los datos personales de cada individuo se convierten en mercancías valiosas a disposición de diferentes actores en el mercado, algunos de ellos anónimos.

Estas mercancías han sido adquiridas, por así decirlo, sin trabajo alguno para la empresa que las comercia en la mayoría de los casos sin el consentimiento de las personas, o bien en detrimento de la privacidad de las mismas. En este sentido, la relación mercantil se negocia desde una posición asimétrica en la cual la empresa difunde un engaño inicial consistente en hacer pasar como gratuitos los servicios que ofrece y que la información recabada sólo tendrá fines estadísticos para la mejora continua. Entonces se erige en una posición de ventaja sobre las personas, que en el momento de la transacción carecen de medios de contrapeso consintiendo contratos de adhesión preestablecidos y no negociables. Esta práctica es considerada desleal desde el momento en que una de las partes o actores no disponen de la misma información que la otra sobre el objeto de la transacción comercial, lo cual contraviene en última instancia el principio de equidad en el mercado. Hay quienes opinan que en la actualidad es posible que las empresas en línea tengan más información sobre nosotros que el propio Estado[154].

C. *La sociedad de la vigilancia.*

Después de los atentados del 9/11 en Nueva York, los esfuerzos para prevenir situaciones similares resultaron en el desarrollo e implementación de tecnologías de vanguardia para la observación y vigilancia de amenazas potenciales a la seguridad, las

[154] Terra Noticias, *Sitio web ofrece datos del IFE de forma gratuita*, 7 noviembre de 2013, Disponible en línea [http://noticias.terra.com.mx/mexico/sitiowebofrecedatosdelifedeformagratuita,313074f2d4332410VgnVCM3000009af154d0RCRD.html] Consultado 14 de enero de 2014

cuales se integraron a sistemas de alerta a determinadas autoridades, constituyendo un protocolo de acción para estos casos. Si J. Edgar Hoover viviera en esta época sería completamente feliz. Cada internauta ha construido minuciosamente un expediente detallado con toda la información que antes sólo podía ser obtenida mediante horas de vigilancia y mecanismos de inteligencia que integraban una red de informantes encubiertos[155]. Lo mejor de todo es que ha proporcionado sus datos voluntariamente, sin coacción alguna.

Estos esfuerzos han logrado edificar redes a través de cámaras de altas especificaciones interconectadas con bases de datos en línea, de manera simultánea, por ejemplo, para el monitoreo de tránsito de pasajeros en aeropuertos. De tal modo que, si eventualmente un rostro le es familiar al sistema por antecedentes que configuren una posible amenaza, sean detectados al momento para emitir una advertencia a las autoridades a fin de que sea neutralizada en el menor tiempo posible. En este sentido se ha implementado software especializado que mediante la captura de imágenes de las cámaras instaladas, registran la comunicación no verbal así como las posturas intimidantes y gestos desafiantes de las personas y con base en el análisis simultáneo podrían dar cuenta de potenciales comportamientos agresivos, muestras de ansiedad o casos sospechosos que serían catalogados por el mismo software como amenazadores. Los comportamientos, entonces, ya pueden clasificarse dentro de normas preestablecidas por los organismos de control, quienes deciden qué es normal. Podría pensarse que esta tarea hace más fácil el trabajo a los dispositivos de cómputo porque finalmente impone un principio de homogeneización del comportamiento humano, al menos para el procesamiento de la máquina.

En el caso del Estado de Yucatán, en meses recientes, se han instalado más de 500 cámaras de videovigilancia en diversos lugares de la ciudad, así como también en puntos estratégicos de ciertas vías de comunicación[156]. El sistema es capaz de entregar con nitidez imágenes de placas de automóviles desplazándose a 200 kilómetros por hora. La idea es que se emita automáticamente la infracción correspondiente por exceso de

[155] Gonzalbo (*Op. Cit.*) señala al respecto que: “Este sentido común dice que lo privado debe estar más o menos protegido, a salvo de cualquier intromisión, mientras que lo público debe ser visible, transparente; en la práctica, tengo la sensación de que ocurre lo contrario: del gobierno en adelante, las instituciones públicas resultan oscuras, no podemos saber lo que sucede en ellas, mientras que nuestra vida privada está sujeta a toda clase de controles y sistemas de vigilancia. Por eso se quiere leyes que garanticen la transparencia, el acceso a información pública, y se quiere también leyes que protegen la privacidad. (página 10)”

[156] *Cfr.* “Refuerzan vigilancia en vídeo en territorio yucateco" en *Diario de Yucatán*, publicado el 16 de enero de 2014, Disponible en línea [http://yucatan.com.mx/merida/policia/refuerzan-vigilancia-en-video-en-territorio-yucateco], consultado el 18 de enero de 2014

velocidad al titular del vehículo, recuperando el nombre de la base de datos con la que se cuenta.

Las dimensiones de la cantidad de datos personales que son procesados a través de estos portales se incrementan exponencialmente. Las comunicaciones digitales en línea enlazadas a través de satélites pueden ser monitoreadas, rastreadas, geolocalizadas, e incluso las personas pueden ser reconocidas automáticamente por sus rasgos faciales.

De acuerdo con los documentos filtrados a diversos medios por el ex-contratista de inteligencia, Edward Snowden[157], Estados Unidos, a través de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), habría puesto en marcha operaciones de escucha no autorizada alrededor del mundo a distintos objetivos de su particular interés, incluyendo en ellos a sus propios aliados. BBC Mundo, por su parte, publicó que el programa PRISM habría sido lanzado por NSA en 2007. A través de él se pueden captar correos electrónicos, videos, fotografías, actividad en redes sociales, llamadas de voz o de imagen y voz combinadas e incluso contraseñas y otros datos de los usuarios puestos en circulación a través de las empresas proveedoras del servicio de internet así como portales de servicios en red. Entre las compañías involucradas en el programa PRISM se encuentran Microsoft, su división Skype; Google y su división Youtube; Yahoo, Facebook, America On Line (AOL) de Warner Communications y Apple, entre otros.

Una asimetría nos coloca en el mismo escenario: por un lado el ciudadano común y corriente, y por otro, el Estado y su aparato. A través de la tecnología, sistemas inteligentes entregan reportes automatizados que de manera unilateral, puesto que ignoramos los indicadores e índices de la metodología empleada, pueden definir, categorizar y clasificar a las personas por su "nivel de riesgo" o "peligrosidad", basado en sus aficiones, lecturas, gustos, activismo a favor de ciertas causas, preferencias sexuales o contactos sociales. La hiperconectividad entonces se vuelca contra el ciudadano como una libertad positiva.

Nunca como ahora el Estado se informa a través de diversas tecnologías de vigilancia sobre los sujetos sociales[158] sin la posibilidad del error humano o la alteración del material por la influencia de emociones, sentimientos o cualquier otro rasgo de

[157] *Cómo espía EEUU., según Snowden*. BBC Mundo publicado el jueves 31 de octubre de 2013 [http://www.bbc.co.uk/mundo/noticias/2013/10/131031_eeuu_nsa_espionaje_tecnicas_az.shtml] Recuperado el 13 de octubre de 2013

[158] *Cfr.* "Snowden: NSA puede decodificar conversaciones privadas" en *Noticieros Televisa*, 14 diciembre 2013, Disponible en línea [http://noticieros.televisa.com/mundo/1312/snowden-nsa-puede-decodificar-conversaciones-privadas/] Consultado el 14 diciembre 2013

subjetividad que ocasionara un sesgo para el análisis. Desde el gobierno se dice que la observación sirve en última instancia a la consecución de la seguridad, la paz social y el bien común, incrementando su efectividad en los métodos empleados para la vigilancia y el control social. Sin embargo queda el resquicio para plantear una duda razonable ¿es esto una amenaza a las libertades individuales?

En un principio, la regulación de datos personales se centró en la relación entre el Estado y los individuos, dado que éste guarda minuciosos registros y bases de datos personales y tiene la capacidad real de limitar, coartar o intervenir en la libre esfera de acción de los ciudadanos de manera directa, inmediata y justificada. En una sociedad que se precie de ser democrática, el individuo debe tener la facultad de saber qué tipo de datos son almacenados por el Estado y con qué propósitos, durante qué período. Así como tener la capacidad de rectificarlos, oponerse a su divulgación, o cancelarlos en caso de no existir una razón necesaria para su acopio[159]. El control de los datos es una prerrogativa individual del sujeto que se extiende a su privacidad, y por tanto, que debe ser garante de la confidencialidad de sus comunicaciones, sin preocuparse porque puedan ser intervenidas o que admitan tecnológicamente intromisiones no consentidas.

REFERENCIAS.

ADN político, El IFAI indaga presunto espionaje en dispositivos móviles, Disponible en línea [http://www.adnpolitico.com/gobierno/2013/07/05/el-ifai-indaga-presunto-espionaje-en-dispositivos-moviles], consultado el 14 de enero de 2014

ALCÁNTARA, José F. Privacidad, propiedad Intelectual y el futuro de la libertad. Barcelona, España. El Cobre Ediciones. Colección Planta 29. 2008.

ALEXANDRES FERNÁNDEZ, Sadot (*et al*.), "RFID: La tecnología de Identificación por Radio Frecuencia", en Anales de mecánica y electricidad, Enero-Febrero 2006, Disponible en línea [http://dialnet.unirioja.es/servlet/articulo?codigo=1448367&orden=62874&info=link] páginas 47-52 Consultado el 30 de enero de 2014

ARELLANO TOLEDO, Wilma. "Privacidad y protección de datos en internet: España, la Unión Europea y México" en Tenorio Cueto, Guillermo (Coordinador) *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*. México D.F. Editorial Porrúa-Universidad Panamericana 2012

[159] El Economista, *Desactivan web con datos personales*, Publicado el 7 de noviembre de 2103, Disponible en línea[http://eleconomista.com.mx/sociedad/2013/11/07/desactivan-web-datos-personales], Consultado el 20 de enero de 2014

Carta de los Derechos Fundamentales de La Unión Europea de 2010 [*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:es:pdf*]

Convención Americana Sobre Derechos Humanos (Pacto de San José) San José, Costa Rica 7 al 22 de noviembre de 1969 [*http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm*]

Convención de Roma para la protección de los Derechos Humanos y las Libertades Fundamentales de 1959 [*http://www.cjf.gob.mx/documentos/2011/HTML/DGDHEGyAI/Tortura/Textos%20internacionales/Soporte/Documentos/15.%20convenioProtec.Fundamentales.pdf*

Convención sobre los Derechos del Niño de 1989 [*http://www2.ohchr.org/spanish/law/crc.htm*]

Cómo espía EEUU., según Snowden. BBC Mundo, jueves 31 de octubre de 2013, [http://www.bbc.co.uk/mundo/noticias/2013/10/131031_eeuu_nsa_espionaje_tecnicas_az.shtml]

Declaración Universal de los Derechos Humanos [*http://www.un.org/es/documents/udhr/*]

El Economista, Desactivan web con datos personales, Publicado el 7 de noviembre de 2103, Disponible en línea [http://eleconomista.com.mx/sociedad/2013/11/07/desactivan-web-datos-personales]

Enciclopedia Jurídica Mexicana. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Tomo III D-E. Editorial Porrúa. México, 2002, Págs. 408 – 410.

ESCALANTE GONZALBO, Fernando. *El Derecho a la Privacidad*. Instituto Federal de Acceso a la Información Pública. Colección cuadernos de transparencia # 2. México D.F. 6ª edición. 2008

GAMBOA MONTEJANO, Claudia y AYALA CORDERO, Arturo. *Derecho de la Intimidad y el Honor vs. Derecho a la Información. Estudio Teórico Conceptual, Marco Jurídico a Nivel Federal y Estatal e Iniciativas presentadas en la materia en la LIX Legislatura*. México D.F. Edit. Centro de Documentación, Información y Análisis. Cámara de Diputados LX Legislatura. 2007 [*http://www.diputados.gob.mx/cedia/sia/spi/SPI-ISS-01-07.pdf*]

ONU- CEPAL. Los Caminos Hacia Una Sociedad de la Información en América Latina y El Caribe, Bávaro, Punta Cana, República Dominicana, 29 al 31 de enero de

2003[http://www.itu.int/wsis/docs/rc/bavaro/eclac-es.pdf] Consultado el 14 de enero de 2014.

Pacto Internacional de Derechos Civiles y Políticos de 1966 [*http://www2.ohchr.org/spanish/law/ccpr.htm*]

"Reconocimiento facial", en Biometría. Métodos biométricos, Disponible en línea [http://www.biometria.gov.ar/metodos-biometricos/facial.aspx] consultado el 10 de febrero de 2014.

"Refuerzan vigilancia en vídeo en territorio yucateco" en Diario de Yucatán, publicado el 16 de enero de 2014, Disponible en línea [http://yucatan.com.mx/merida/policia/refuerzan-vigilancia-en-video-en-territorio-yucateco]

RUEDA, Nicolás, "Google pagará multa por rastrear sin permiso a usuarios de Safari", en MediaTelecom, publicado el 19 de noviembre de 2013, Disponible en línea [http://www.mediatelecom.com.mx/index.php/tecnologia/internet/item/54373-google-pagara-multa-por-rastrear-sin-permiso-a-usuarios-de-safari], Consultado el 19 de noviembre de 2013

Terra Noticias, Sitio web ofrece datos del IFE de forma gratuita, 7 noviembre de 2013, Disponible en línea [http://noticias.terra.com.mx/mexico/sitiowebofrecedatosdelifedeformagratuita,313074f2d4332410VgnVCM3000009af154d0RCRD.html]

VELASCO SAN MARTÍN, Cristos. *Protección de datos personales en internet*. Revista Electrónica Entérate en Línea. Internet, Cómputo y Telecomunicaciones. Año 7 Núm. 74, Publicación Mensual, 27 de Noviembre de 2008.Universidad Nacional Autónoma de México. Dirección General de Servicios de Cómputo Académico [*http://www.enterate.unam.mx/Articulos/2003/enero/protecci.htm*]

http://noticieros.televisa.com/mundo/1312/snowden-nsa-puede-decodificar-conversaciones-privadas/

http://www.merca20.com/wp-content/uploads/whitepapers/redes-sociales-whitepaper-2013.pdf, consultado el 21 de mayo de 2014.

Recepción: 30 de abril de 2014.

Aceptación: 27 de junio de 2014.