LOS DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. ANÁLISIS DE SU PROTECCIÓN EN MÉXICO

GUILLERMO A. TENORIO CUETO
Y MARÍA RIVERO DEL PASO

SUMARIO: I. *Nota introductoria.* II. *La intimidad y la privacidad en relación con el concepto jurídico de dato y sus distinciones.* III. *Los principios rectores de la protección de datos.* IV. *Los tipos de consentimiento el aviso de privacidad.* V. *Los llamados derechos ARCO y su protección.* VI. *La transferencia de datos.* VII. *Los procedimientos de protección de datos personales en posesión de los particulares.* VIII. *Las sanciones de carácter pecuniario y penales.* IX. *Conclusión*

Resumen: Los datos personales deben ser protegidos por la importancia que significan para su titular. La salvaguarda de los mismos ha sido consagrada recientemente en el derecho positivo de distintos países, siendo México uno de ellos. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares

establece a cargo de sujetos particulares obligaciones respecto la forma en la que deben tratarse los datos personales a los que tengan acceso y consagra los denominados derechos ARCO, mediante los cuales los particulares pueden exigir el acceso, rectificación, cancelación y oposición al tratamiento de los mismos. El estudio propuesto realiza un análisis crítico de la situación imperante en materia de datos personales en nuestro país proponiendo una revisión conceptual del marco regulatorio.

Palabras clave: Datos Personales, Privacidad, Protección de Datos.

Abstract: Personal data have to be protected for the importance these represent for its owner. The safekeeping of personal data has been recently incorporated in applicable law of different countries, including Mexico. The Mexican Federal Law for Protection of Personal Data in Possession of Particular establishes on behalf of particulars several obligations regarding the from in which they treat the personal data to which they have access. This law also considers the ARCO rights; pursuant to which particulars may request the Access, Rectification, Cancelation, and Opposition to the treatment of their personal data. Moreover, such legal disposition states state different type of penalizations by means of which particulars may be sanctioned.

Key Words: Personal Data, Privacy, Protection of Personal Data.

I. NOTA INTRODUCTORIA

Los avances tecnológicos demandan del derecho una herramienta que permita garantizar la salvaguarda de los datos personales que son almacenados. Los avances en la ciencia hacen que cada vez, con mayor facilidad, personas y entes públicos y privados tomen decisiones con base en estadística. Sin embargo, la misma tecnología permite que haya filtraciones de dicha información, de manera intencional o accidental. El escape de dicha información resulta en la vulneración de la privacidad y control de los individuos de cuya información se trate.[1]

Recientemente, en algunos países se han adoptado ordenamientos jurídicos que protegen específicamente la información personal y rigen las bases con las que ésta debe ser tratada. Desde 2002 en México, a través de la Ley Federal de Transparencia y Acceso a la Información Pública Federal, se establecieron ciertos límites respecto del tratamiento de la información personal. Sin embargo, dicho ordenamiento sólo se refiere al tratamiento de datos personales por los llamados sujetos obligados[2] y por supuesto descuidando un adecuado tratamiento legislativo del marco jurídico internacional para datos personales.

En consecuencia de lo anterior, hasta el año 2010, los entes privados y demás sujetos distintos de los llamados sujetos obligados, no encontraban un cuerpo jurídico único y específico respecto al uso de datos personales, salvo por las disposiciones dispersas en otros ordenamientos jurídicos[3] y el reconocimiento

[1]Cfr. Téllez Váldez, Julio, *Derecho informático*, 3ª. Ed. Mc Graw Hill, México, 2004, p. 61. Al respecto el autor refiere que "los datos no son vulnerables per se sino según la aplicación de la que puedan ser objeto, la cual puede ser variada….convirtiéndose de esta manera en un instrumento de opresión y mercantilismo".

[2]El artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental refiere como sujetos obligados a: a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal; d) Los órganos constitucionales autónomos; e) Los tribunales administrativos federales, y f) Cualquier otro órgano federal".

[3]Habría que recordar que ya existían normas que protegían los datos perso

a este derecho incluido desde 2006 en el artículo sexto constitucional[4] y posteriormente por la reforma al artículo 16 constitucional del 1º de junio de 2009.[5] Es pertinente aclarar que la reforma al sexto supondrá el fundamento de protección de datos para los entes públicos, mientras que la del 2009 supondrá el auténtico fundamento para la protección de datos en posesión de los particulares.

En este sentido, siguiendo la tendencia internacional, durante septiembre de 2001 se presentó en la Cámara de Diputados una iniciativa sobre un Proyecto de Decreto para la expedición de una Ley de Protección de Datos Personales. Casi ocho años después, la Comisión de Presupuesto y Cuenta Pública analizó la iniciativa con el propósito de evaluar el impacto de la creación de la Comisión Nacional de Datos Personales, contemplada en el proyecto.

El primero de junio del 2009 se adicionó un segundo párrafo al texto de la Constitución que preveía la protección de los datos en posesión de los particulares. El 13 de abril de 2010 fue aprobado el dictamen[6] y se ordenó remitir el expediente relativo a esta iniciativa a la cámara revisora. Dos días después, la Cámara de Senadores recibió la minuta y el día 27 del mismo mes, la misma aprobó el decreto que crea la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

La Ley pretende establecer las bases que rijan la recolección, almacenamiento, consulta, transferencia, actualización y nales como era el caso de la materia de protección al consumidor o las del sector financiero.

[4]Cfr.Tenorio Cueto, Guillermo, *La constitucionalización del acceso a la información pública gubernamental*, en Bejar Rivera, Luis José (coord.) Derecho Administrativo. Perspectivas contemporáneas, Porrúa-Universidad Panamericana, México 2010, pp. 146 y 147.

[5]La reforma citada adicionó un segundo párrafo al artículo 16 de la constitución el cual refiere que: "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 tercero".

[6]Es importante aclarar que se dictaminaron siete iniciativas de Ley de Datos Personales en la Cámara de Diputados y una más en la Cámara de Senadores.

eliminación de datos; con el propósito de proteger la intimidad, defender la privacidad, la dignidad, el derecho a la información, tutelar el honor, la propia imagen o perfil personal y el derecho a la identidad. Es decir, garantiza el derecho a no ser molestado, lo que en términos anglosajones conocemos como "*the right to privacy*".[7]

II. LA INTIMIDAD Y LA PRIVACIDAD EN RELACIÓN CON EL CONCEPTO JURÍDICO DE DATO Y SUS DISTINCIONES

Ordinariamente cuando hablamos del término intimidad lo tenemos referido a un espacio de protección personal en el que difícilmente permitimos el acceso a ninguna otra persona. Es más, algunos autores consideran a lo íntimo como "aquel ámbito de pensamientos de cada cual, de la forma de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será…",[8] para otros, la intimidad es un ámbito jurídico que radica su origen en la propia dignidad del ser humano teniendo por ende, que ser protegida y tutelada como un derecho fundamental[9] consistiendo la misma en aquel espacio vital asemejado "… a la vida retirada o anónima, a la vida interior o espiritual de la persona".[10]

Pero no sólo la doctrina ha trabajado el tema de la intimidad. Los diversos sistemas jurídicos han incorporado la protec

[7]Cfr. Warren, S. y Brandeis, L., *The right to privacy*, *Harvard Law Review*, 1890, traducción al castellano por Pendas, Beningno y Baselga, Pilar, Civitas, Madrid, 1995.

[8]Cfr. Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, IFAI, Cuadernos de transparencia no.6, México, p. 15.

[9]Así lo ha entendido el Tribunal Constitucional Español al referir que el derecho de intimidad personal previsto en el artículo 18 de la Constitución Española, deriva de la dignidad de la persona (STC 231/1998)

10Cfr. Carrillo, Marc, *El derecho a no ser molestado*, Thomson Aranzadi, Navarra, 2003, p 44. Para autores como José María Desantes, la intimidad será "...aquella zona espiritual del hombre que considera inespecífica, distinta a cualquier otra, independientemente de que lo sea, y por tanto, exclusivamente suya, que tan sólo el puede libremente revelar". Desantes Guanter, José María, *Derecho a la información*, Coso, Valencia, 2004, p. 243

ción de este derecho. En ese sentido el sistema jurídico anglosajón americano lo define de manera clara como: "la potestad del titular a vivir solo y a no ser molestado, que permite al individuo decidir soberanamente sobre su independencia personal".[11] Para los sistemas continentales o mejor llamados de *civil law*, este derecho se materializa en la disposición "... de la vida personal, o el reconocimiento a favor de una persona de una zona de actividad que le es propia y respecto de la cual es dueña de impedir el acceso a otros, salvo que medie su previo consentimiento".[12] De igual manera el tratamiento dado en Europa recoge un principio fundamental del tratamiento de datos el cual es la autodeterminación informativa que consiste en el control y manejo de la información personal de manera autónoma e independiente por parte de los individuos.[13]

En nuestro sistema jurídico mexicano, ni el texto de la Constitución, ni las leyes ordinarias hacen referencia al derecho a la intimidad, por el contrario sólo se hace referencia al término privacidad. Intimidad y privacidad, parecieran ser lo mismo, pero es claro que el tratamiento jurídico a uno y a otro es completamente distinto. La privacidad adquiere su dimensión en función de entenderla como aquel espacio de la vida humana "donde impera una transparencia relativa",[14] es decir, donde cabe la posibilidad de la presencia de otro ser humano, donde la opacidad de la actuación no es total o donde es posible una interacción comunicativa.[15]

Ello nos lleva a proponer que mientras en el ámbito de lo íntimo, la protección de la información debiera ser total, en el ámbito de lo privado existiría un velo de protección por parte del individuo más deslucido, en donde la participación de "otro" u "otros", se vuelve fundamental para su conceptualización. A

[11] *Ibidem*.

[12] *Ibidem*.

[13] Sólo como referencia se pueden consultar las sentencias del Tribunal Constitucional Español 53/1985, 254/1993 y 11/1998, en donde se recoge a cabalidad este principio orientador de la materia de datos personales.

[14] Cfr. Garzón Valdés, Ernesto, *op. cit*., p. 18.

[15] *Ibidem*.

manera de ejemplo, para clarificar la diferenciación podríamos decir que lo pensado sobre un tema forma parte de mi intimidad, mientras lo expresado puede formar parte de la privacidad o bien, si es en condiciones públicas, de la publicidad. Lejos de lo que pudiera pensarse, el perfil de un portal como *Facebook*, obedece en principio a un ámbito privado y no público, pues en principio sólo los amigos más cercanos estarán en posibilidad de observar lo comunicado, pudiendo comentarlo entre ellos, pero no debiendo extrapolarlo fuera del ámbito del perfil.

El único marco legal donde figura una definición de la privacidad en México es la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal,[16] donde la vida privada se entiende como "... aquella que no está dedicada a una actividad pública y, que por ende, es intrascendente y sin impacto en la sociedad de manera directa y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta".[17] Es claro que esta definición de nuestro marco legal no aclara una distinción entre intimidad y privacidad y aglutina los conceptos confundiéndolos.

Lo cierto es que estos dos conceptos son fundamentales para entender el marco de protección de los datos personales. El tratamiento jurídico del mismo nos arroja dos posibilidades de datos, por un lado los datos personales que supone cualquier información concerniente a una persona determinada y por otro los llamados datos personales sensibles, los cuales son aquellos

[16]Cabría hacer la aclaración que en el ámbito jurisprudencial, la Suprema Corte de Justicia de la Nación en su sentencia 4002/2007 estableció la diferencia entre intimidad y vida privada señalando que: "... mientras [la vida privada] constituye el ámbito privado reservado para la propia persona y del que quedan excluidos los demás; la intimidad se constituye con los extremos más personales de la vida y el entorno personal, cuyo conocimiento está restringido a los integrantes de la unidad familiar…. Así se tiene que vida privada e intimidad son derechos distintos…" SCJN 4002/2007.

[17]Artículo 9 de la Ley de Responsabilidad civil para la protección del derecho a la vida privada, el honor y la propia imagen en el Distrito Federal.

que "...afecten la esfera más íntima de su titular o cuya utilización indebida, pueda dar origen a discriminación o conlleve un riesgo grave para este".[18]

Como se puede apreciar los datos personales siguen la suerte de los dos conceptos relacionados en este apartado. Aún y cuando no haya una clara definición del concepto de intimidad, la ley recoge esta idea cuando hace la distinción. En ese sentido entenderemos que serán datos personales o de la vida privada, todos aquellos que no estén enumerados dentro del catálogo de datos llamados sensibles o de la vida íntima. Este catálogo enumerado por la misma ley hace referencia a datos que permitan "revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual".[19]

Una legislación en materia de datos personales de asumir por consiguiente que los datos emanados tanto de la vida íntima como privada de las personas constituyen información,[20] la cual al ser transmitida de manera conexa nos puede indicar un perfil personal que constituiría, en términos económicos, un bien inmaterial,[21] susceptible de ser transmitido para obtener un beneficio en función de su explotación, aprovechamiento, uso u otra finalidad particular establecida por quien los maneje.

Cabe señalar que el dato en sí mismo carece de contenido, es decir, aún y cuando exista un contenido material, el mismo pierde relevancia de protección en función de su aislamiento. La protección de datos siempre es en plural pues es, en dicha pluralidad, donde encontramos un marco de actuación jurídica

[18]Artículo 3 fracción VI de la Ley Federal de protección de datos personales en posesión de los particulares. Autores como Osvaldo Gozaíni refiere que los datos sensibles "se dividen en dos campos: uno refiere al objeto de protección propiamente dicho; el otro a la garantía que tutela estos datos y el nivel de protección que merecen de acuerdo al grado de sensibilidad que se le atribuye…", Gozaíni, Osvaldo, *Habeas Data, protección de datos personales*, Rubinzal-Culzoni Editores, Buenos Aires, p. 233.

[19]*Ibidem*.

[20]Cfr. Téllez, Julio, *op. cit*., p. 58.

[21]*Ibidem*.

para tutelar. Por dar un ejemplo que ilustre lo anterior habría que pensar en un número telefónico el cual, en sí mismo, es un dato, aislado y sin posibilidad de convertirse en un elemento de protección. Pensemos ahora en el mismo número telefónico en relación con un nombre, es decir, el número telefónico de "x" persona, en este caso tenemos un par de datos vinculados que nos permiten una mínima identificación personal, digna ya de protección.

Como se refirió con anterioridad, el conjunto de datos produce una cierta información, información que provoca que una persona pueda ser identificada o identificable o bien que dicha información revele un aspecto de intimidad del sujeto, el cual deberá tener en sus manos un instrumento jurídico que le permita el control, rectificación, cancelación o aceptación del manejo de los mismos.

III. LOS PRINCIPIOS RECTORES DE LA PROTECCIÓN DE DATOS

La protección en el manejo de los datos no debe considerarse una protección sin una guía determinada. Dicha guía deberá estar ceñida por los principios rectores de la protección de los datos personales, los cuales son licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.[22]

Estos principios se articulan y actualizan en cada ocasión donde el particular proporcione a un tercero, sus datos. Dicha entrega y manejo de los mismos, deberá ajustarse a los principios referidos. En ese sentido, el derecho a la protección de datos "…reconoce a la persona un poder de control sobre la información personal que le concierne, sobre su utilización y destino para evitar utilizaciones ilícitas".[23]

[22]Artículo 6 de la Ley Federal de Protección de Datos Personales en Posesión de los articulares.

[23]Cfr. Herrán Ortiz, Ana Isabel, *El derecho a la protección de datos personales en las sociedad de la información*, Universidad De Deusto, Bilbao, 2003, p.20.

En efecto, el primero de los principios concierne a la licitud en el manejo de los datos proporcionados. El referido principio, asume que el depositante de los datos debe contar con la certeza de que el responsable de los mismos llevará a cabo un uso legítimo de los datos proporcionados, es decir que "… no será posible su utilización para fines incompatibles con los inicialmente determinados…".[24]

De igual manera que sucede con la licitud, el principio de consentimiento es medular y una piedra angular del tratamiento legítimo de los datos personales. El consentimiento puede darse de dos maneras fundamentales: expresa o tácitamente. En uno y otro caso, contamos con una participación de la voluntad, mediante la cual, se acepta o no el manejo de la información por parte del responsable. En ese sentido debemos entender por consentimiento expreso, aquél mediante una expresión verbal, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos, proporcione al responsable la aceptación del manejo de los datos personales. Por el contrario, se entenderá que el consentimiento es tácito, cuando el responsable del manejo ha puesto a disposición del titular de los datos "un aviso de privacidad" y este último no ha objetado o manifestado una negativa para el manejo.[25] En ese sentido los datos deben utilizarse únicamente para el fin consentido por el titular y en caso de que se pretenda usarlos con un propósito distinto, el responsable deberá consentir nuevamente conforme a los requisitos del consentimiento según el tipo de información de que se trate. En el siguiente apartado se profundizará sobre este principio y sus repercusiones.

Con base en el principio de calidad, la ley impone a cargo del responsable la obligación de procurar que los datos personales contenidos en las bases de datos sean correctos, actualizados y utilizados para los fines para los que fueron recabados.[26] Asi

[24] *Idem*, p. 25.

[25] Artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[26] Nos parece importante referir que dichos atributos del principio de calidad

mismo, es obligación del responsable cancelar los datos cuando éstos cumplan su propósito. Este principio de calidad asume que los datos deberán "...ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para que los que fueron recogidos o para los que se traten posteriormente…".[27] Dicho principio de calidad en la protección de los datos personales corresponde al responsable de la base de datos, siendo a cargo de éste, el establecer los medios y mecanismos necesarios para evitar la violación de los sistemas que contengan los datos.

El principio de proporcionalidad supone que la recaudación de los datos deberá estar limitada por los fines para los cuales son recabados los mismos, de suerte que este principio establece "... la necesidad de que la información personal sea adecuada, pertinente, y no excesiva con los fines para los que se recabe y trate personalmente".[28] Este principio no sólo impacta en la recaudación, sino por el contrario también se asume en el tratamiento de los datos. Es claro que una información inexacta impediría que la misma fuera tratada de manera adecuada, en ese sentido la actualización de los datos es ser un elemento que completa el principio de proporcionalidad pues la información incompleta o inexacta, es información obsoleta.[29]

El último de los principios referidos en el texto de la ley es el principio de responsabilidad, el cual encuentra su eje de actuación en el debido manejo de los datos proporcionados. Este principio implica el establecimiento de "... medidas de seguridad, administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o

---

deben asumir definiciones precisas. En ese sentido entendemos que un dato será correcto cuando los mismos han sido otorgados por el titular y hasta que no comunique lo contrario respecto a ello y se mantendrá actualizado, de igual manera, hasta que se sepa que ya no lo está. Por su parte, cuando el titular otorga más datos de los necesarios para el fin que busca el responsable o éste obtiene lo mismo del titular, se considerará un dato excesivo, pues será innecesario para el fin perseguido por el titular.

[27] Cfr. Herrán Ortiz, Ana Isabel, *op. cit.*, p.25

[28] *Idem*.

[29] *Idem*.

el uso, acceso o tratamiento no autorizado",[30] bajo la condicionante de ser sancionado por la misma legislación. Este principio ordena a todo tratante de datos a no adoptar medidas menores a las que adoptaría tratándose del manejo de su información. El tratante se obliga a preveer medidas contra cualquier riesgo, las consecuencias emanadas de la vulneración de cara a los titulares y sobre todo, actualizar su desarrollo tecnológico de cara a posibles vulneraciones de seguridad.[31]

IV. LOS TIPOS DE CONSENTIMIENTO Y EL AVISO DE PRIVACIDAD

Una vez revisados los principios que irradian toda la protección de datos en posesión de los particulares, nos avocaremos a revisar con precisión los tipos de consentimiento y sus consecuencias teniendo en consideración el llamado "aviso de privacidad" que todo responsable deberá colocar a disposición de los titulares de los datos.

Los datos deben obtenerse informando claramente a los titulares sobre los fines y usos de los mismos. El consentimiento32 del titular para el uso de los datos personales puede expresarse de manera verbal, escrita, por medios electrónicos, ópticos o por signos inequívocos. No obstante se considera aceptación tácita cuando se revele algún dato personal habiendo puesto a disposición del titular un aviso de privacidad.

En relación al consentimiento tácito, es necesario señalar los requisitos o las condiciones con base en las que se considerará que se puso a disposición del titular el aviso de privacidad, pues así podría tenerse mucha mayor certeza de que no se vulnera el principio de información y consentimiento. La autorización en el manejo de datos, podrá ser revocada por el titular de los mis

[30]Artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[31]*Idem*.

[32]Para Marcela Basterra el consentimiento es "el elemento determinante para que sea lícita la recolección de datos". Basterra, Marcela, *Protección de Datos Personales*, Ediar, Buenos Aires, 2008, p. 373.

mos, en cualquier momento de acuerdo con los mecanismos y procedimientos señalados para ello por el responsable.

La facultad del responsable para determinar la forma de revocación del consentimiento crea un obstáculo en relación con este principio, pues corresponde al titular determinar momento a momento cómo se utiliza su información y éste debe poder ejercer ese derecho libremente y en cualquier momento. En ese sentido, cabe aclarar que los derechos denominados ARCO (Acceso, Rectificación, Cancelación y Oposición) no suponen la revocación del consentimiento en virtud de que los mismos inciden directamente en el tratamiento y no en el consentimiento.

De igual manera es importante señalar que, tratándose de datos sensibles, el consentimiento debe ser expreso y por escrito. Las bases de datos con este tipo de información no podrán crearse sin que exista justificación y fines legítimos, concretos y acordes con las actividades o fines del responsable. Es imperante establecer que la regla general debiera ser que no es factible el manejo de datos sensible salvo que esté su tratamiento consentido expresamente y por escrito.[33]

La ley federal señala diversas excepciones al requisito de obtener el consentimiento por parte del titular las cuales son:

a) Estén previstos por ley

b) Datos que figuren en fuentes de acceso público

c) Datos personales que se sometan a un procedimiento previo de disociación

d) Tengan el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable

e)Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.

f) Sean indispensables para la atención médica, prevención, diagnóstico, prestación de asistencia sanitaria, tratamien

[33]En ese sentido valdría citar como una referencia internacional, la directiva 94/46/CE de la Unión Europea, la cual prohíbe el manejo de los datos denominados sensibles, excepto cuando haya sido consentido explícitamente su tratamiento por el titular Artículo 8.1 de la Directiva 95/46/CE.

tos médicos o gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, mientras que el tratamiento de datos se realice por una persona sujeta a secreto profesional o equivalente.

g) Se dicte resolución de autoridad competente.[34]

Todas estas excepciones implican el manejo de datos sin el previo consentimiento del titular. En ese sentido la obligación del responsable que maneja los datos no se exime del cumplimiento de los principios de la protección, por el contrario, sigue estando obligado a un manejo adecuado de la información en su poder.

Este consentimiento no podría darse, si previamente el titular de los datos no conoce el tratamiento que el responsable otorgará a los mismos, es decir que para obtener el consentimiento de una persona no sólo en la entrega, sino en el manejo y disposición de los datos, es necesario que se ponga a su disposición, la información necesaria que le indique cual será el destino de la información que proporciona. Todo particular responsable en el manejo de datos deberá hacer del conocimiento del titular el llamado "aviso de privacidad".

El aviso de privacidad es el instrumento a través del cual el responsable en el manejo de los datos pone a consideración del titular de los mismos, los alcances del manejo de datos que realizará, en virtud del consentimiento del titular. La ley lo define como el "documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo tratamiento de sus datos personales".[35] Dicho aviso de privacidad podrá ser completo o simplificado.[36]

[34]Artículo 10 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[35]Ibidem, artículo 3º.

[36]Se entenderá un aviso de privacidad completo aquel que reúna los seis elementos de información enumerados en el artículo 16 de la ley. Por su parte será simplificado cuando recibidos los datos por alguna de las vías previstas por el artículo 17 fracción II, la información de manejo de datos sólo se limite en un primer momento a las dos primeras fracciones del artículo 16 y se provean los mecanismos para que el

El llamado aviso de privacidad permite al titular de los datos no sólo el quehacer del responsable con los datos, sino saber quien es el responsable, que finalidad tendrá el tratamiento de los datos, el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, transferencias que se lleven a cabo con los datos y procedimientos cuando se verifique el cambio del contenido del aviso de privacidad.

En todo momento el aviso de privacidad debe preceder al consentimiento, es decir que éste se encontrará viciado de origen si no existe el conocimiento del titular del mencionado aviso. Si el responsable de la obtención de los datos se hace de ellos por otra vía diferente al titular, inmediatamente los obtenga deberá enviar por cualquier medio al titular el aviso de privacidad para que éste, asuma que, el manejo de sus datos está en manos de un tercero y en su caso efectuar la negativa del consentimiento y el ejercicio de algún derecho respecto a ellos.

Este aviso de privacidad siempre deberá ponerse a disposición del titular por el medio que sea oportuno a través del formato que sea necesario, es decir que la ley no otorga ningún resquicio de posibilidad de que este aviso no se haga del conocimiento del titular. En ese sentido si los datos son recogidos en al vía pública, el responsable antes de recolectarlos deberá entregar al titular el aviso de privacidad, si los datos son obtenidos mediante medios electrónicos, por esa vía el responsable deberá hacer entrega del aviso, si los datos son recabados telefónicamente, el responsable deberá previamente informar al titular del aviso de privacidad. Como podemos darnos cuenta, cada responsable del manejo de datos deberá establecer en sus diversos procedimientos de obtención de los mismos, los mecanismos pertinentes y oportunos para obtener el consentimiento del titular.

---

otorgante pueda conocer el texto completo del aviso de privacidad.

V. LOS LLAMADOS DERECHOS ARCO Y SU PROTECCIÓN

Una materialización del derecho a la información consiste en el desarrollo de los derechos de acceso, rectificación, cancelación y oposición (o derechos ARCO) donde aquél constituye su fundamento.[37] En efecto el derecho a la información se colma en esa obligación de informar[38] y cuando nos referimos a la protección de datos el derecho a la información obliga al responsable a informar sobre los datos que obran en su poder, pero de igual manera otorgan al titular de dichos datos a determinar que manejo quiere que se haga con ellos. Esto es conocido como la autodeterminación informativa.[39]

Lo cierto es que cada uno de estos derechos cobra entidad propia y asume para sí diversas consecuencias legales respecto al tratamiento de los datos personales. En ese sentido, el primero de ellos, el derecho de acceso termina por completar el inacabado derecho de acceso a la información en México. Desde el año 2001, el derecho de acceso informativo se había materializado a través de una de las partes de acceso que son las entidades públicas, teniendo en consecuencia una ley de acceso a la información pública que incluía un apartado de manejo de datos personales, pero siempre referido a entidades públicas. Una de las grandes carencias durante todo este tiempo es que el derecho de acceso a la información no encontraba plenitud pues quedaba trunco en el acceso a la información de los datos que manejan los particulares. Así pues, el derecho de información se obtiene en una doble vía respecto a los particulares, por un lado el dere

[37]Cfr. Herrán Ortiz, Ana Isabel, *op. cit*., p.30

[38]Cfr. Desantes Guanter, José María, *Derecho a la información*, Coso, Valencia, 2004, p. 74.

[39]Cfr. Delón Vázquez, Mánelic, *El proceso de protección de datos personales*, Universidad Panamericana, México, 2011, p. 24. Al respecto el autor refiere que a través de ella el individuo puede "proteger su esfera de intimidad en cuanto al tratamiento de sus datos personales… ya que teniendo el control de aquellos datos que se encuentran en poder de otras personas, tiene la posibilidad de manejar que aspectos de su vida quiere que queden expuestos a la mirada ajena y cuales no y quienes la pueden manipular".

cho de obtener información para determinados fines a partir de la recopilación de datos y bajo un marco legal adecuado y por otro, el derecho de acceder a la fuente que es responsable del manejo de los datos.[40]

Dice la legislación que cualquier particular tendrá el derecho de acceder a sus datos personales que obren en poder del responsable, lo que significa que el primero de los llamados derecho ARCO, producirá como consecuencia lógica que en caso de no permitir el acceso, el titular de los datos estará facultado para accionar los mecanismos legales necesarios para lograr el acceso. Mecanismos que inician con la solicitud de protección de datos ante el Instituto de Acceso a la Información y Protección de Datos.

El segundo de los derechos es el de rectificación. Es claro que este derecho es concomitante al de acceso, pues sin este último no habría posibilidad de accionar ninguno de los tres restantes. No obstante, al igual que sucede con el acceso, implica consecuencias jurídicas diversas. La rectificación supone la "modificación de las informaciones personales erróneas o incompletas",[41] lo que conduce a que el responsable esté obligado a la rectificación cuando el titular lo solicite.

Este derecho de rectificación impacta en la esfera del titular directamente al ofrecer una información equívoca. En ese sentido, el titular tiene un derecho a obligar al responsable a rectificar el dato, el cual puede ser: a) erróneo o inexacto, es decir aquel dato que, pretendiendo asumir alguna referencia informativa por su inexactitud no completa adecuadamente la información; b) equívoco, cuando la información referida proveniente del dato conduce a diversas interpretaciones poco claras o; c) incompleto, es decir una información parcialmente cierta.[42]

[40]Cfr. Herrán Ortiz, Ana Isabel, *op. cit*., p. 31.

[41]Cfr. Rebollo Delgado, Lucrecio, *Derechos fundamentales y protección de datos*, Dykinson, Madrid, 2004, p. 155.

[42]Cfr. Bertelsen Repetto, Raúl, *Tratamiento de datos personales y protección de la vida privada*, Universidad de los Andes, Cuadernos de extensión jurídica no. 5, Santiago de Chile, 2001, pp. 43 y 44.

Es claro que en los tres casos planteados encontraríamos algunas diferencias pues en estricto sentido, hablamos de rectificación sólo en el caso de los datos erróneos o inexactos, pues en los otros dos tenemos el deber de hablar de un derecho de complementación o aclaración, los cuales no existen en la legislación.[43] De cualquier manera, debería entenderse *in extenso* el derecho para estos dos supuestos, pues en última instancia si bien no es una rectificación de datos supondrá una rectificación de información vinculada con una persona.

El tercero de los derechos referidos en el texto legal es el de cancelación. Este derecho, al menos para la ley mexicana, asume un periodo de bloqueo, es decir, el derecho de cancelación no se da inmediatamente solicitada la misma. Es pertinente aclarar que este es un error, pues en todo caso debieran entenderse como derechos diferenciados, por un lado la cancelación y por otro el bloqueo, pues la cancelación debe dar lugar a la destrucción del dato, mediante el mecanismo pertinente, mientras que el bloqueo "consiste en la facultad de exigir que se suspenda temporalmente el tratamiento de datos que estén almacenados, es decir que se suspenda cualquier operación…destinada a utilizar los datos en cualquier forma".[44]

En la legislación mexicana el derecho de rectificación da lugar a un periodo de bloqueo,[45] el cual permite al responsable de los datos conservarlos, "…para efectos de responsabilidades nacidas del tratamiento",[46] es decir, dicha ley asume un periodo en el cual el dato saldrá del dominio del uso del responsable entrando en una especie de esfera de protección especial, en la cual sólo podrán ser tratados cuando se verifique la comprobación de una violación en su tratamiento y que de la misma, se desprenda una responsabilidad. El tiempo del bloqueo varía de acuerdo al plazo "...de prescripción las de las acciones derivadas de la rela

[43] *Idem*.

[44] *Idem*.

[45] Artículo 25 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[46] *Idem*.

ción jurídica que funda el tratamiento en los términos de la ley aplicable en la materia".[47]

A diferencia de lo que ocurre en otros sistemas jurídicos, en México se ha optado por establecer en qué casos no hay obligación de los responsables a cancelar los datos[48] teniendo por ejemplo, cuando se refieran a las partes de un contrato privado, deban ser tratados por disposición oficial, obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales o a perseguir delitos, o cuando sean necesarios dichos datos para proteger intereses jurídicamente tutelados del titular, para realizar una acción en función del interés público o bien sean necesarios para cumplir una obligación legalmente adquirida por el titular o sean objeto de tratamiento para la prevención o diagnóstico de un diagnóstico médico.[49]

De cualquier manera el derecho de cancelación agotará su existencia en el vencimiento del periodo de bloqueo establecido por la ley. Será un derecho exigible de aplicación condicionada pero que, al menos, permite el retiro de los datos a un estado que imposibilita su manejo.

El último de los denominados derechos ARCO es el de oposición. Dicho derecho consiste en una acción de negativa respecto al manejo de datos para determinados fines como pueden ser publicidad, investigación de mercado o encuestas de opinión.[50] A diferencia de la cancelación, en el mismo no se busca una supresión de los datos proporcionados, por el contrario se consiente en proporcionarlos, pero se limita u opone el titular al tratamiento para fines específicos. Desafortunadamente, la legislación mexicana no hace esta aclaración por lo que el dere

[47] *Idem*.

[48] En concreto nos referimos al caso Chileno, donde su ley 19.628 estable que los datos pueden ser cancelados si el almacenamiento carece de fundamento legal, si los datos tienen el carácter de caducos o si los mismos han sido proporcionados voluntariamente o se usan para comunicaciones comerciales. Cfr. Bertelsen Repetto, Raúl, *op. cit*., p. 44.

[49] Artículo 26 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[50] Cfr. Bertelsen Repetto, Raúl, *op. cit*., p. 46.

cho de oposición puede confundirse por un lado con el derecho de cancelación o bien con el derecho de bloqueo. Por la redacción del artículo 27 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el derecho de oposición queda ceñido a un bloqueo en el tratamiento de los datos, es decir que una vez solicitada la oposición el responsable debe mantenerlos en ese estado de esfera de protección de la cual hablábamos cuando nos referíamos al bloqueo de datos, y los mismos permanecer así por el tiempo que el titular estime. No serán cancelados pues la naturaleza de la oposición, según la ley, es impedir el tratamiento.

VI. LA TRANSFERENCIA DE DATOS

La salvaguarda de los datos a través de mecanismos jurídicos que protejan los derechos de acceso, rectificación cancelación y oposición estaría incompleta sino se hiciera hincapié en una debida protección de los mismos derechos cuando el responsable transfiere los datos del titular a un tercero, quien debiera asegurar el mismo tratamiento que el primer responsable ha dado a los mismos sea nacional o sea un tercero extranjero el que los maneje. A ello se le ha denominado la transferencia de los datos.

La primera regla establecida es que el responsable que pretenda transferir los datos a un tercero nacional o extranjero deberá "... comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento...",51 Con ello se garantiza extrapolar el nivel de protección, el cual "valorará atendiendo a todas las circunstancias que concurran en la concreta transferencia de que se trate"52 y por ello impedirá que el tratamiento sea menor al del país de origen. En ese sentido el aviso de privacidad, con las limitaciones y consecuencias del mismo viaja pegado a los datos proporcionados, evitando su orfandad legal y

[51]Artículo 36 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[52]Cfr. Herrán Ortiz, Ana Isabel, *op. cit.*, p. 40.

teniendo como consecuencia que el nivel de protección jurídico en otro responsable, disminuya en función de una regulación paupérrima en el ámbito del sistema jurídico de que se trate.

Para lo anterior, el titular de los datos deberá otorgar su consentimiento para permitir que el responsable, como parte del proceso de tratamiento de los datos pueda efectuar la transferencia de los mismos a terceros nacionales o extranjeros. Este consentimiento para la transferencia admite excepciones, las cuales están previstas por la ley y que son las siguientes:

a) Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

b) Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

c) Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

d) Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

e) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

f) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

g) Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.[53]

[53]Artículo 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

VII. LOS PROCEDIMIENTOS DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

La ley de datos personales cuenta con una sección adjetiva dividida en tres tipos de procedimientos. Por un lado un procedimiento llamado de protección de derechos, un segundo procedimiento llamado de verificación y un último denominado de imposición de sanciones.

Respecto a estos tres procedimientos es imperante precisar que no es propiamente un proceso de *Habeas Data*, sino se trata de procedimientos que, aunque de manera material se nutran de lo pretendido por el *habeas data* respecto a la protección de los datos, carece de la intervención jurisdiccional[54] y sólo se limitan a ser procedimientos administrativos de carácter conciliatorio y sancionador.

De igual manera el juicio de nulidad, previsto en el artículo 57 del ordenamiento legal, que pudiera llevarse a cabo respecto a la resolución proveniente del Instituto Federal de Acceso a la Información y Datos Personales, frente al Tribunal Federal de Justicia Fiscal y Administrativa, no es un proceso de *Habeas Data*, pues en este último caso no se está frente al ejercicio material del denominado proceso, sino ante la nulidad del acto del órgano administrativo que emitió la resolución.

Como se ha referido, el primero de los procedimientos de protección de datos,[55] mas no habeas data, es un procedimiento llevado ante el Instituto Federal de Acceso a la Información y Datos Personales mediante el cual, el titular de los datos presenta una solicitud de protección y el organismo deberá emitir una resolución sobre la misma, la cual tendrá como efectos, confirmar, revocar o modificar la respuesta del responsable.

[54]Cfr. Gozaíni, Osvaldo, *op. cit*., pp. 383-389. Al respecto el autor destaca que la garantía procesal del Habeas Data radicará justamente en su carácter de proceso judicial constitucional, es decir que independientemente de la materia de la que se nutre, el mismo deberá asumirse desde el juez constitucional.

[55]Artículo 45 y ss., de la Ley Federal de Datos Personales en Posesión de los Particulares.

Como se refirió anteriormente, la resolución del Instituto sólo dará pie a la impugnación del titular ante el Tribunal Federal de justicia Fiscal y Administrativa a efecto de que éste, emita si la resolución del Instituto es nula o no lo es. No hay competencia expresa para que dicho tribunal pueda resolver sobre el ejercicio de los derechos ARCO.

El segundo de los procedimientos es el de verificación,[56] el cual tendrá como finalidad la supervisión del responsable por parte del Instituto cuando aquel incumpla una resolución emitida por éste. Dicho procedimiento deja abierta la puerta para que el inicio del mismo sea de oficio o a petición de parte.

El tercero de los procedimientos es el de imposición de sanciones[57] el cual tiene como antecedente cualquiera de los otros dos y supondrá para el Instituto el observar el incumplimiento de alguno de los principios o disposiciones de la ley.

VIII. LAS SANCIONES DE CARÁCTER PECUNIARIO Y PENALES

No podía la ley eludirse de un apartado de sanciones pecuniarias y penales respecto al incumplimiento de la misma. En ese sentido la legislación establece diecinueve supuestos de conductas consideradas como infracciones[58] y dos tipos penales, los cuales verán duplicadas sus penas cuando se traten de datos sensibles.[59]

Sin ánimo de ser exhaustivo en la enumeración vale la pena detenerse a señalar y comentar algunas de las sanciones. La primera, objeto de referencia es la omisión del aviso de privacidad, la cual será sancionada con una infracción que podrá oscilar entre los 100 y los 160000 DSMGV en el Distrito Federal. Con ese mismo monto serán sancionados aquellos que no cumplan con la solicitud del titular para el ejercicio de los derechos ARCO o actuar con negligencia o dolo en la tramitación.

[56] *Ibidem*, artículo 59.
[57] *Ibidem*, artículo 61
[58] *Ibidem*, artículo 63
[59] *Ibidem*, artículos 67 y ss.

Otro tipo de sanción es la que se tasa con una infracción de 200 a 320,000 DSMGV en el Distrito Federal entre las cuales encontramos el incumplimiento con el deber de confidencialidad, el cambio sustancial de la finalidad o transferir los datos a terceros sin comunicar a éstos el aviso de privacidad.

IX. CONCLUSIÓN

El manejo de los datos en posesión de los particulares cobra vida en nuestro sistema jurídico a partir de la reforma del 2009 y la Ley Federal de protección de datos en posesión de los particulares en junio de 2010. Esta incorporación supone un cambio paradigmático en el tratamiento de los datos, incorporando a nuestro sistema jurídico la protección de los mismos a través del reconocimiento de los denominados derechos ARCO (….) y que desafortunadamente no establece procesos judiciales acordes con la reforma constitucional, dejando meros y simples procedimientos que no pueden alcanzar el ámbito jurisdiccional y que sólo se limitan a un ámbito de la justicia administrativa.

Recibido: 07-03-2011
Aprobado: 09-06-2011