CJI/doc.541/17 corr.1

LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES

(presentado por la doctora Ana Elizabeth Villalta Vizcarra)

I MANDATO

Tomando en cuenta que el Comité Jurídico Interamericano delegó a la suscrita para que asistiera en representación de dicho Comité a varias reuniones de la Red Iberoamericana de Protección de Datos (RIPD), donde se ha estudiado el tema de Protección de Datos Personales, llegando hasta la elaboración de Estándares de Protección de Datos Personales, con el objeto de poder contar con reglas homogéneas para la región.

En ese sentido, se presenta el siguiente Informe en el Nonagésimo Primero Periodo Ordinario de Sesiones del Comité Jurídico Interamericano a celebrarse en Río de Janeiro, Brasil del 7 al 16 de agosto de 2017.

II. ANTECEDENTES

El Comité Jurídico Interamericano (CJI), formuló una propuesta de Principios de Privacidad y Protección de Datos Personales para las Américas, con la finalidad de instar a los Estados Miembros de la OEA a que se adopten medidas para respetar la privacidad, la reputación y la dignidad de las personas y especialmente que los Estados consideren la conveniencia de formular y adoptar leyes sobre la protección de datos personales y el derecho a la privacidad.

La Asamblea General de la OEA en su cuadragésimo cuarto período ordinario de sesiones, llevado en cabo en Asunción, Paraguay en junio de 2014, en su resolución AG/RES. 2842 (XLIV-O/14), encomendó al Comité Jurídico Interamericano "formule propuestas a la Comisión de Asuntos Jurídicos y Políticos sobre las distintas formas de regular la protección de Datos Personales, incluyendo un Proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia".

El Relator del tema nombrado por el CJI llegó a la conclusión que lo más productivo era la elaboración de una Guía Legislativa para los Estados Miembros que se basaría en los 12 Principios adoptados por el Comité Jurídico sobre esta materia con algunas modificaciones que tomarían en cuenta los diversos conjuntos de directrices preparados por la Unión Europea, la OCDE, APEC, entre otros, dando una orientación más amplia a los Estados con la finalidad de facilitar la elaboración de leyes nacionales, aprovechando las experiencias y logros de otras regiones pero teniendo en cuenta la situación de la nuestra y lo adelantos tecnológicos.

Estos Principios se fundamentan en normas reconocidas a nivel internacional y su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación en forma ilícita de los datos personales. Las normas nacionales que se implementen para la protección de datos personales deben tener una finalidad legítima y los datos deben procesarse de una manera justa, legal y no discriminatoria. Debiendo asegurarse que las personas que recopilan, procesan, usan y difunden datos personales lo hagan de forma apropiada y con el debido respeto de los derechos de las personas.

Se debe buscar un equilibrio entre el Derecho de Acceso a la Información y el Derecho a la Protección de Datos Personales. Es decir, se debe buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales y su derecho a tener acceso a los datos, así como el derecho que tienen las personas y organizaciones en el uso razonable de datos personales con fines comerciales legítimos y de una manera segura y protegida.

Los Principios sobre Protección de Datos Personales tienen un ámbito de aplicación tanto en los sectores públicos como privados, es decir, datos recopilados y procesados por entidades públicas y privadas pero no aplica para los datos personales utilizados por las personas en el contexto exclusivo de su vida privada.

En cuanto al concepto de Privacidad, este se basa en los derechos fundamentales del honor, la dignidad, la intimidad, la propia imagen, así como en la libertad de expresión, pensamiento, opinión y asociación. Muchos de ellos regulados en los Instrumentos Internacionales de Derechos Humanos y en los textos constitucionales o Leyes Fundamentales de los Estados Miembros de la OEA.

En el Sistema Interamericano, estos derechos están claramente establecidos en la Declaración Americana de los Derechos y Deberes del Hombre de 30 de abril de 1948 en su artículo V, y en la Convención Americana sobre Derechos Humanos conocida como “Pacto de San José” de 22 de noviembre 1969 en sus artículos 11 y 13. Así mismo la Corte Interamericana de Derechos Humanos se ha referido a ellos en varias de sus Sentencias, como el Caso de las Masacres de Ituango *vs*. Colombia y el Caso Atala Riffo *vs*. Chile, entre otros.

En cuanto a legislación nacional secundaria, varios de los Estados Miembros de la Organización de los Estados Americanos han adoptado normas con respecto a la privacidad y a la protección de datos personales.

De igual manera la mayoría de dichos ordenamientos jurídicos han establecido que el derecho a la privacidad no es absoluto y que puede tener limitaciones razonables. En ese sentido, existen otros derechos fundamentales a los que se ha hecho referencia como los de libertad de expresión, libertad de información, libertad de asociación, que también están consagrados en los Instrumentos Internacionales de Derechos Humanos y así tenemos que en ámbito interamericano la Declaración

Americana de los Derechos y Deberes del Hombre de 30 abril de 1948 se refiere a ellos en su artículo IV y la Convención Americana sobre Derechos Humanos o Pacto de San José de 22 de noviembre 1969 en su artículo 13.

Los "Datos Personales" implican toda aquella información inherente a una persona, que permiten identificarla, abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta, es decir, la información de una persona física identificada o identificable, como por ejemplo: nombre, apellidos, correo electrónico, estado civil, profesión, numero de documento de identidad, entre otros.

Los "Datos Personales" Sensibles, son aquellos que de divulgarse de manera indebida afectarían la esfera más íntima del ser humano o provocarle un riesgo grave, como por ejemplo, el origen racial o étnico, el estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia u orientación sexual, entre otros.

El "Controlador de Datos" es la persona física o jurídica, entidad pública o privada, organismo u organización que solo o conjuntamente se encarga del almacenamiento, el procesamiento, el uso, la protección y la difusión de los datos y en algunas circunstancias pueden convertirse en recopiladores de datos.

El "Procesador de Datos" es la persona física o jurídica, entidad pública o privada, organismo u organización que solo o conjuntamente procesa los datos en cuestión, abarcando toda operación o conjunto de operaciones que se realizan con datos personales, como recopilación, registro, almacenamiento, recuperación, divulgación o transferencia.

La "Autoridad Responsable de la Protección de Datos", es la que se encarga de establecer y hacer cumplir leyes, normas, requisitos relativos a la protección de datos personales a fin de mantener una uniformidad; esta autoridad puede variar según la legislación de los Estados Miembros.

"Titular de los Datos", es la persona cuyos datos personales se recopilan, procesan, almacenan, utilizan o difunden, es decir, es la persona a quien corresponden los datos personales.

Con relación a lo anterior, se cuenta con una Guía de Principios que fueron expuestos por él relator del Comité Jurídico Interamericano en este tema siendo estos los siguientes:

Los "Principios de la OEA" sobre la Protección de la Privacidad y los Datos Personales

Primer Principio: Propósitos Legítimos y Justos

"Los Datos Personales deben ser recopilados solamente para fines legítimos y por medios justos y legales".

Este Principio debe respetarse en todo proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales.

La legitimidad excluye la recopilación arbitraria y caprichosa de los datos personales, implicando la existencia de una estructura jurídica y transparente a la cual pueda tener acceso la persona cuyos datos se estén recopilando, se debe indicar claramente los fines para los cuales se recopilan los datos, a fin de que la persona pueda saber cómo se recopilaran, usarán o divulgarán los datos.

En cuanto a los medios justos y legales, excluye la obtención de datos personales por medio de fraude, engaño o pretextos falsos, su recopilación debe ser compatible con los requisitos jurídicos pertinentes como con las expectativas razonables de las personas basadas en su relación con el controlador de datos y con los avisos dados a las personas en el momento en que se recopilen los datos.

Segundo Principio: Claridad y Consentimiento

"Se deben especificar los fines para los cuales se recopilan los datos personales en el momento en que se recopilen. Como regla general, los datos personales solamente deben ser recopilados con el consentimiento de la persona a que se refieran".

Este Principio se fundamenta en la transparencia y en el consentimiento. Lo que significa que los fines para los cuales se recopilan los datos personales deben especificarse claramente desde su inicio, debiendo informar a las personas sobre las prácticas y políticas de las entidades o personas que recopilan los datos personales, a fin de que puedan tomar una decisión clara con respecto al suministro de tales datos.

La persona por lo tanto, será capaz de dar su consentimiento libremente respecto de la recopilación de los datos personales de la forma y con los fines previstos, en ese sentido, el consentimiento de la persona debe basarse en información suficiente y clara, que no dé lugar a ninguna duda o ambigüedad. Para que el consentimiento sea válido, la persona debe contar con suficiente información sobre los detalles concretos de los datos que se recopilarán, la forma en que se recopilarán, los fines del procesamiento y toda divulgación que pueda efectuarse, a fin de que pueda realizar una elección real.

La persona no debe correr ningún riesgo de engaño, intimidación, coacción o consecuencias negativas si se niega a dar el consentimiento. La manifestación del consentimiento debe ser libre, inequívoca, específica e informada mediante la cual el titular consiente en el tratamiento de sus datos personales.

Tercer Principio: Pertinencia y Necesidad

"Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación".

Los datos personales deben ser correctos, exactos, completos y estar actualizados con respecto a los fines para los cuales se hayan recopilado, ya que la calidad de los datos son importantes para la protección de la privacidad, por lo que el recopilador o procesador de datos debe adoptar mecanismos para cerciorarse de que los datos personales sean correctos, exactos, completos y actualizados.

Los datos deben de ser pertinentes guardando una relación razonable con los fines para los cuales hayan sido recopilados. Es decir, no deben utilizarse para fines con los que no guarden ninguna relación.

Cuarto Principio: Uso Limitado y Retención

"Los datos personales deben ser mantenidos y utilizados solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente".

Los datos personales no deben utilizarse con fines que no sean compatibles con aquellos para los cuales se hayan recopilado, excepto con el consentimiento del titular de los datos o por mandato de ley.

Los datos personales solo pueden mantenerse el tiempo que sea necesario para el fin para el cual se hayan recopilado y de conformidad con lo dispuesto en las leyes nacionales pertinentes, ya que la retención innecesaria y excesiva de datos personales tiene evidentemente implicaciones para la privacidad por lo que los datos deben eliminarse cuando ya no se necesiten para su fin original o cuando lo dispongan las legislaciones nacionales.

No obstante lo anterior, un controlador de datos podría tener razones legales legítimas para retener datos durante un período determinado de tiempo como por ejemplo expedientes de pacientes, expedientes de empleados, expediente de alumnos, entre otros.

Quinto Principio: Deber de Confidencialidad

"Los datos personales no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que nos sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley".

Es un deber básico del controlador de datos el mantener la confidencialidad de los datos personales en un entorno seguro y controlado y que estos no se usen para fines que sean incompatibles con la finalidad original. Proteger la privacidad implica no solo mantener la seguridad de los datos personales, sino también permitir que los datos se usen y se divulguen para otros fines. Debe establecerse una relación de confianza entre el titular de los datos y el controlador de los datos.

Sexto Principio: Protección y Seguridad

“Los Datos Personales deben ser protegidos mediante salvaguardias razonables y adecuadas contra accesos no autorizados, pérdidas, destrucción, uso, modificación o divulgación”.

Los controladores de datos tienen el deber de tomar las medidas prácticas, técnicas y necesarias para proteger los datos personales que obren bajo su poder o custodia y cerciorarse que tales datos personales no sean objeto de pérdida, destrucción, acceso, uso, modificación o divulgación.

Los datos personales deben protegerse, por medio de salvaguardias razonablemente concebidas para prevenir que las personas sufran daños considerables como consecuencia del acceso no autorizado a los datos, o por su pérdida o destrucción. Para los datos personales más sensibles se requerirá un nivel más alto de protección.

Estas salvaguardias deben ser “razonables y adecuadas”, ante las amenazas cibernéticas y responder ante esa evolución. El reto consiste en proporcionar orientación válida a los controladores de datos, procurando al mismo tiempo que las normas sigan siendo tecnológicamente neutrales, y no se vuelvan obsoletas como consecuencia de los rápidos cambios tecnológicos.

En caso de violación de datos personales, los controladores de datos deberían tener la obligación legal de notificar a las personas cuyos datos han sido comprometidos, para que estas puedan tomar las medidas de protección más adecuadas, así como tener acceso a los datos a efecto de que se corrijan datos inexactos o el uso indebido de los mismos como consecuencia de su violación. Así mismo deben examinarse las políticas en materia de retención de datos y mejorar sus medidas de seguridad, como sería el caso que los controladores de datos tuviesen la obligación de cooperar con las fuerzas del orden en el ámbito penal y con otras autoridades.

Se deberían también imponer sanciones a los controladores de datos por incumplimiento a su deber de salvaguardar y proteger los mismos, tales sanciones deberían de ser proporcionales al grado de perjuicio o de riesgo. Todo esto debería ser objeto de regulación de las legislaciones nacionales.

Séptimo Principio: Fidelidad de los Datos

“Los Datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósito de su uso”.

Cuando se recopilan datos personales y se les retiene para seguir usándolos, el controlador de datos tiene la obligación de tomar medidas para que los datos se mantengan actualizados, completos y exactos, en la medida de lo necesario para los fines para los cuales se hayan recopilado y se usen, con la finalidad de que no menoscaben los derechos del Titular de los Datos.

Octavo Principio: Acceso y Corrección

"Se debe disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso a dichos datos y puedan también solicitar al controlador de datos que los modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso o corrección, deberían así mismo de especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional".

Los Titulares de Datos tienen derecho a tener acceso a los mismos a fin de que puedan impugnar su exactitud y solicitar al controlador de datos que modifique, revise, corrija o elimine los datos en cuestión y así poder ejercer el derecho a la rectificación.

Este derecho de acceso y corrección es una de las salvaguardias más importantes en el campo de la protección a la privacidad. El derecho de acceso a los datos personales mantenidos por un controlador de datos debe ser sencillo de ejercer, aunque a veces puede estar sujeto a excepciones y limitaciones, por lo que si a una persona se le deniega la solicitud de acceso, debe explicársele las razones de su denegación para que no se convierta en un acto arbitrario.

En el ordenamiento jurídico interno de algunos Estados Miembros de la OEA se reconoce el Recurso al *Habeas Data*, en virtud del cual el titular de datos puede entablar un juicio para prevenir un presunto abuso de sus datos personales o ponerle fin, este derecho se regula de distintas maneras en los Estados Miembros, incluso en algunos tiene rango constitucional.

Noveno Principio: Datos Personales Sensibles

"Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptible de causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información".

Los "datos personales sensibles" abarcan todos aquellos que puedan afectar los aspectos más íntimos de las personas. Según el contexto cultural, social o político, podrían incluirse los datos relacionados con su salud personal, preferencias sexuales, creencias religiosas, ideología política, origen racial o étnico, sexo, entre otros.

Si estos datos se manejan o se divulgan en forma indebida, podrían dar lugar a una intromisión profunda en la dignidad personal y en el honor de la persona afectada, pudiendo desencadenar una discriminación ilícita o arbitraria o causar un riesgo de graves perjuicios para la persona, la índole de la sensibilidad puede variar de un país a otro.

Los controladores de datos deben de saber determinar los riesgos más importantes para los titulares de los datos al divulgar los mismos, razón por la cual sería conveniente responsabilizarlos por la divulgación de datos sensibles.

Décimo Principio: Responsabilidad

"Los controladores de datos adoptarán e implementarán de manera responsable las medidas correspondientes para el cumplimiento de estos principios".

La protección efectiva al derecho a la privacidad y de los datos personales tiene su fundamento en la conducta responsable de los controladores de datos tanto de sectores públicos como privados, en ese sentido, los sistemas de protección de la privacidad deben reflejar un equilibrio apropiado entre la reglamentación gubernamental y la implementación efectiva por aquellos que tienen la responsabilidad directa de la recopilación, el uso, la retención y la difusión de datos personales.

Su buen uso depende de la capacidad de quienes recopilan, procesan y retienen datos personales para tomar decisiones responsables, éticas y disciplinadas acerca de los datos y su uso durante todo el ciclo de vida de los mismos. Estos custodios de datos deben actuar con la debida responsabilidad a favor de quienes les proporcionan y confían sus datos.

Los controladores de datos deben cerciorarse de que las personas que manejan datos personales estén debidamente capacitados en lo que se refiere a la finalidad de protección de los datos y los procedimientos que se emplean para protegerlos, capacitándolos con programas efectivos de gestión de la privacidad.

Onceavo Principio: Flujo Transfronterizo de Datos y Responsabilidad

"Los Estados Miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente responsables por el cumplimiento de estos Principios".

En el mundo moderno de rápidos flujos de datos y comercio transfronterizo, es cada vez más probable que las transferencias de datos personales crucen fronteras nacionales, dándose el caso que la reglamentación que existe actualmente en diversas jurisdicciones nacionales varíe en cuanto al fondo y al procedimiento, dando como consecuencia la posibilidad de confusión, conflictos y contradicciones.

En ese sentido, el reto fundamental para una política y una práctica eficaz en materia de protección de datos consiste en conciliar:

1) Las diferencias en los enfoques nacionales de la protección de la privacidad con la realidad moderna del flujo mundial de datos; 2) los derechos de las personas a tener acceso a datos en un contexto transnacional; y 3) el hecho fundamental de que los datos y el procesamiento de los mismos impulsen el desarrollo y la innovación.

Todos los instrumentos internacionales para la protección de datos deben procurar alcanzar un equilibrio apropiado entre esas metas.

Estas transferencias deben permitirse en los casos en que los controladores de datos tomen las medidas apropiadas para asegurar que los datos transferidos estén protegidos de manera efectiva y en consonancia con todos estos Principios, debiendo los Estados Miembros tomar las medidas necesarias para que los controladores de datos se responsabilicen de esa protección.

En ese sentido, los Estados Miembros deben procurar el reconocimiento mutuo de las reglas y prácticas en materia de responsabilidad, a fin de evitar conflictos y poder resolverlos cuando estos surjan. En ese sentido, deben promover la transferencia fronteriza de datos, con las debidas salvaguardias, y no deben imponer cargas que limiten el libre flujo de información o actividad económica entre jurisdicciones.

Los controladores de datos deben tomar las medidas razonables para que los datos personales estén protegidos eficazmente de acuerdo a estos Principios, sea que los datos se transfieran a terceros dentro del país o a través de fronteras internacionales.

Doceavo Principio: Publicidad de las Excepciones

"Cuando las autoridades nacionales establezcan excepciones a estos Principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberán ponerlas en conocimiento del público dichas excepciones".

Si bien es cierto la privacidad es cada vez más importante, siendo necesario conferir a las personas los derechos básicos que necesitan para salvaguardar sus intereses, respetando todos los Principios a que se ha hecho referencia, es posible que las autoridades de los Estados Miembros en algunas ocasiones tengan que establecer excepciones por razones relacionadas con preocupaciones imperiosas de la seguridad nacional y la protección del público, la administración de justicia, el cumplimiento de normativas, entre otros, debiendo convertirse en excepciones y no en la regla general.

III. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

El Comité Jurídico Interamericano y el Departamento de Derecho Internacional de la OEA han participado en algunas de las reuniones de la Red Iberoamericana de Protección de Datos RIPD (la que surgió en el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala en junio de 2003), como las de Cartagena de Indias -Colombia, de La Antigua; Guatemala, siendo de las más importantes el Seminario llevado a cabo en Montevideo, Uruguay en noviembre de 2016 donde se presentó a la Red

Iberoamericana de Protección de Datos el Anteproyecto de Estándares Iberoamericanos para comentarios y observaciones, (los cuales se acordó su elaboración en la reunión de Junio de 2016 en Santa Marta, Colombia), los cuales fueron revisados y concluidos desde el punto de vista técnico en el Taller de la Red Iberoamericana de Protección de Datos que se llevó a cabo en mayo de 2017 en Cartagena de Indias, siendo aprobados por unanimidad en el Encuentro Iberoamericano de Protección de Datos llevado a cabo en Santiago de Chile en junio de 2017, donde fueron proclamados formalmente en la Sesión Abierta.

Con estos estándares la región dispondrá de una herramienta esencial con la cual poder establecer un conjunto de principios y derechos comunes de protección de Datos Personales y que los Estados puedan adoptar y desarrollar en su legislación nacional, con el objeto de poder contar con reglas homogéneas, garantizando de esta manera el ejercicio efectivo y la tutela del derecho a la protección de datos personales, así como facilitar el flujo de los datos personales en la región y más allá de sus fronteras fortaleciendo de esta manera el crecimiento económico y social y favoreciendo la cooperación internacional entre las autoridades de control de la región, fuera de la región y entre autoridades y organismos internacionales en la materia.

Haciendo un resumen del documento de los Estándares tenemos:

En la parte considerativa se hace alusión que ya en varios de los Estados de la región se considera el derecho de protección de datos personales como un derecho fundamental reconocido en las constituciones políticas de los Estados, bajo la forma del derecho a la protección de datos personales o *habeas data*, contando incluso con jurisprudencia por parte de los Estados; Que la falta de armonización en esta materia (ya que no todos los Estados cuentan con legislación) dificulta hacer frente a los nuevos retos y desafíos en la protección de este derecho a causa de la constante y vertiginosa evolución tecnológica, así como la globalización en sus diversos ámbitos, haciendo necesario la adopción de instrumentos regulatorios que garanticen la protección incluso para el libre flujo de datos personales entre los Estados de la región; lo que hace necesario contar con un marco regulatorio armonizado que ofrezca un nivel adecuado de protección, con reglas homogéneas que ofrezcan a los titulares las mismas garantías de protección.

En relación a las Disposiciones Generales, los estándares buscan establecer un conjunto de principios y derechos de protección de datos personales, que los Estados puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento, así como facilitar el flujo de los datos personales entre los Estados y más allá de sus fronteras con la finalidad de coadyuvar al crecimiento social y económico de la región e impulsar la cooperación internacional

entre las autoridades de control de la región y fuera de la región así como con las autoridades y entidades internacionales en la materia.

También los estándares hacen uso de una serie de definiciones para facilitar su comprensión, así mismo señalan el ámbito de aplicación subjetivo referente a que los mismos serán aplicables a las personas físicas o jurídica de carácter privado, así como a autoridades y organismo públicos que tengan a su cargo el tratamiento de datos; en cuanto al ámbito de aplicación objetivo éstos serán aplicables a los datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización; y en relación al ámbito de aplicación territorial éstos se aplicarán al tratamiento de datos personales efectuados por un responsable o encargado establecido en el territorio de los Estados de la región principalmente, así como cuando no se encuentre establecido en dicho territorio tal como lo establecen los estándares.

También los estándares regulan las excepciones generales al derecho de protección de datos personales, siendo estas limitaciones las referidas a la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

Una regulación muy importante es la referida al tratamiento de datos personales de carácter sensibles, los cuales no podrán ser tratados por el responsable salvo que los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación; cuando se dé cumplimiento a un mandato legal; cuando se cuente con el consentimiento expreso y por escrito del titular y cuando sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

Los estándares también se refieren a los Principios de Protección de Datos Personales siendo estos los siguientes: Legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad, desarrollando cada uno de éstos en los referidos estándares.

Así mismo los estándares hacen referencia a los derechos del titular siendo estos los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad. De tal manera, que el Titular tendrá el derecho de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento, siendo este el derecho de acceso. Así mismo, el titular tendrá el derecho a obtener del responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados, esto es el derecho de rectificación.

También el titular tendrá el derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último. El titular también podrá oponerse al tratamiento de sus datos personales cuando tenga una razón legítima derivada de su situación particular o cuando el tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad, esto se conoce como derecho de oposición y por último, el derecho a la portabilidad de los datos personales por el cual, cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable en caso que lo requiera.

El Derecho de Acceso, es aquel que tiene toda persona a solicitar y a obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento de datos, el origen de los mismos (como se obtuvieron), así como las comunicaciones realizadas con ellos.

El Derecho de Rectificación, es el derecho que tiene la persona a que se modifiquen sus datos que resulten ser inexactos o incompletos, razón por la cual, las autoridades correspondientes tienen la obligación de llevar sus ficheros actualizados.

El Derecho de Cancelación es el derecho que tiene la persona a que se supriman sus datos que resulten ser inadecuados o excesivos, dando lugar a que los datos sean bloqueados, pudiendo únicamente ponerse a disposición de las autoridades, quienes únicamente no procederán a su cancelación por causas justificadas.

El Derecho de Oposición, es el derecho de la persona a que no se lleve a cabo el tratamiento de sus datos de carácter personal mediante causa justificada, esto es, que exista un motivo legítimo y fundado. Solamente podrá denegarse la solicitud por causa justificada.

El Derecho de Portabilidad, es aquel por el cual el titular puede solicitar una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento.

Esto es lo que se llama Derechos ARCO y de Portabilidad, que han quedado muy bien definidos en los estándares.

Los estándares también se refieren al Encargado y a las actividades de este. Así mismo, regulan todo lo relativo a las transferencias internacionales de datos personales, siendo la legislación nacional de los Estados de la región aplicable en la materia la que podrá establecer expresamente límites a las transferencias

internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

Los estándares también se refieren a las autoridades de control, estableciendo que en cada Estado deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad a su ordenamiento jurídico y que podrán ser órganos unipersonales o pluripersonales, que actuarán con carácter imparcial e independiente en sus potestades, y que serán ajenas a toda influencia externa, ya sea directa o indirecta, y que no solicitarán orden ni instrucción alguna.

Dichos estándares también regulan las reclamaciones y sanciones, así como el correspondiente derecho a indemnización para el titular que hubiere sufrido daños y perjuicios, a consecuencia de una violación a su derecho a la protección de datos personales.

Así mismo los estándares alientan a los Estados a dotarse de Mecanismos de Cooperación Internacional que permiten reforzar la asistencia judicial internacional entre los Estados, así como la adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

IV. LEGISLACIÓN INTERNACIONAL SOBRE LA MATERIA

En el "Sistema Interamericano de Derechos Humanos", está regulado el "Derecho a la Privacidad", en el artículo V de la "Declaración Americana de los Derechos y Deberes del Hombre" adoptada el 30 de abril de 1948, que dice: "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

El artículo IX de dicha Declaración que establece: "Que toda persona tiene derecho a la inviolabilidad de su domicilio ",

Y el artículo X de la misma que regula: "Que toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia".

En el artículo 11 de la Convención Americana sobre Derechos Humanos o "Pacto de San José" de 22 de noviembre de 1969, que establece:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En el Marco Universal el “Derecho a la Privacidad” está regulado en el artículo 12 de la Declaración Universal de Derechos Humanos, adoptada el 10 de diciembre de 1948, que expresa:

”Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

El artículo 18 de la misma, establece: “Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia”.

El artículo 19 de dicha Declaración que estipula: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

Y el artículo 20 de la Declaración, que reza:

1. Toda persona tiene derecho a la libertad de reunión y de asociación pacíficas.

2. Nadie podrá ser obligado a pertenecer a una asociación.

Dicho derecho también está garantizado en el “Pacto Internacional de los Derechos Civiles y Políticos” de 1966, que en su artículo 17 expresa:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El artículo 18 de dicho Pacto establece:

1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de tener o de adoptar la religión o las creencias de su elección, así como la libertad de manifestar su religión o sus creencias, individual o colectivamente, tanto en público como en privado, mediante el culto, la celebración de los ritos, las prácticas y la enseñanza.
2. Nadie será objeto de medidas coercitivas que puedan menoscabar su libertad de tener o de adoptar la religión o las creencias de su elección.

3. La libertad de manifestar la propia religión o las propias creencias estará sujeta únicamente a las limitaciones prescritas por la ley que sean necesarias para proteger la seguridad, el orden, la salud o la moral públicos, o los derechos y libertades fundamentales de los demás.

4. Los Estados Partes en el presente Pacto se comprometen a respetar la libertad de los padres y, en su caso, de los tutores legales, para garantizar que los hijos reciban la educación religiosa y moral que esté de acuerdo con sus propias convicciones.

Y el artículo 19 del mismo Pacto reza:

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

   a) Asegurar el respeto a los derechos o a la reputación de los demás;

   b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas."

La "Carta de los Derechos Fundamentales de la Unión Europea" de 2000, regula el Derecho a la Privacidad en sus artículos 1, 7,8, 10, 11 y 12 que respectivamente expresan:

Artículo 1:"La dignidad humana es inviolable. Será respetada y protegida."

Artículo 7: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."

Artículo 8:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan".

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Artículo 10:

1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión. Este derecho implica la libertad de cambiar de religión o de convicciones, así como la libertad de manifestar su religión o sus convicciones individual o colectivamente, en público o en privado, a través del culto, la enseñanza, las prácticas y la observancia de los ritos.
2. Se reconoce el derecho a la objeción de conciencia de acuerdo con las leyes nacionales que regulen su ejercicio.

Artículo 11:

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.
2. Se respetan la libertad de los medios de comunicación y su pluralismo.

Artículo 12:

1. Toda persona tiene derecho a la libertad de reunión pacífica y a la libertad de asociación en todos los niveles, especialmente en los ámbitos político, sindical y cívico, lo que implica el derecho de toda persona a fundar con otros sindicatos y a afiliarse a los mismos para la defensa de sus intereses.
2. Los partidos políticos a escala de la Unión contribuyen a expresar la voluntad política de los ciudadanos de la Unión."

La Carta de los Derechos Fundamentales de la Unión Europea hace por lo tanto, una distinción en todos estos derechos.

En cuanto al Derecho al Libre Flujo de Información, tenemos que en el Sistema Interamericano está regulado en el Artículo IV de la "Declaración Americana de los Derechos y Deberes del Hombre" de 30 de abril de 1948, que establece lo siguiente:

Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio.

De igual manera la "Convención Americana sobre Derechos Humanos" de 22 de noviembre de 1969, regula este derecho en su artículo 13 que establece:

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

En el ámbito Universal, tenemos que la "Declaración Universal de Derechos Humanos" de 10 de diciembre de 1948 en su artículo 19, dispone:

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

En cuanto al "Convenio para la protección de los Derechos Humanos y de las Libertades Fundamentales" de 1950, en su artículo 10 establece:

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la

protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial.

La "Convención Americana sobre Derechos Humanos o Pacto de San José", de 22 de noviembre de 1969, regula el Derecho de Rectificación o Respuesta, en su artículo 14 que literalmente expresa:

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo Órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.
2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.
3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

V. CONCLUSIÓN

En relación con lo anterior, es conveniente que en el Sistema Interamericano se cuente con una Ley Modelo de Protección de Datos Personales, para que aquellos Estados de la región que no cuenten con legislación al respecto, puedan tomar de esta ley modelo los parámetros necesarios para poder incorporarlos en su legislación interna, ya que es conveniente establecer un conjunto de principios y derechos comunes que los Estados del Continente americano puedan adoptar y desarrollar en sus ordenamientos jurídicos con la finalidad de contar con reglas homogéneas en la región.

En sociedades en donde las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana, así como lo hace la globalización, lo que provocó que hace algunos años los Estados le dieran relevancia al derecho de acceso a la información pública, con el objeto de tener mayor transparencia en el manejo a la información pública y que ahora los Estados cuenten en sus ordenamientos jurídicos con Leyes de acceso a la Información pública, lo cual es indudablemente necesario para que se perfile el derecho de participación ciudadana y la obligación de las autoridades a la rendición de cuentas de la gestión pública, convirtiéndose en herramientas idóneas para prevenir, detectar, sancionar y erradicar los actos de corrupción, fortaleciendo de

esta manera la Democracia y el Estado de Derecho, así como fomentar una cultura de transparencia.

Ahora bien, este derecho de acceso a la información pública debe tener su equilibrio que es el derecho de protección a los datos personales y a la privacidad, porque si bien es cierto debe existir un derecho de acceso a la información también debe regularse un derecho a la privacidad y a la protección de datos personales.

En ese sentido, no todos los países del continente americano gozan de una Ley de Protección de Datos Personales, ni tampoco tienen regulado el derecho al *habeas data*, lo cual es necesario para la protección de los derechos fundamentales de la persona.

Por tal motivo, es conveniente que la región cuente de acuerdo con sus particularidades con una Ley Modelo sobre Protección de Datos Personales para que los países que no cuenten con legislación interna sobre la materia, puedan adoptarla.

Para ello se puede tomar como base las leyes que otros Estados de la región han regulado sobre el tema, entre ellos México, Uruguay, Argentina, Colombia, Perú, Nicaragua, o bien los Estándares que recientemente han sido aprobados por la Red Iberoamericana de Protección de Datos RIPD, en el XV Encuentro Iberoamericano de Protección de Datos, celebrado del 20 al 22 de junio de 2017 en Santiago de Chile donde fueron adoptados por unanimidad los Estándares de Protección de Datos Personales, los cuales se han basado también en las leyes de Iberoamérica sobre esta materia.

Se debe buscar un equilibrio entre el Derecho de Acceso a la Información y el Derecho e la Protección de Datos Personales. Es decir, se debe buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales y su derecho a tener acceso a los datos, así como el derecho que tienen las personas y organizaciones en el uso razonable de datos personales con fines comerciales legítimos y de una manera segura y protegida.

De tal manera, que con una Ley sobre Protección de Datos Personales tendríamos por concluido el binomio equitativo sobre lo que sería La Ley de Acceso a la Información Pública y la Ley sobre Protección de Datos Personales.

* * *