84.º PERÍODO ORDINARIO DE SESIONES
10 al 14 de marzo de 2014
Rio de Janeiro, Brasil

OEA/Ser.Q
CJI/doc.450 /14
25 de febrero de 2014
Original: inglés
*Distribución limitada

PRIVACIDAD Y PROTECCIÓN DE DATOS

(presentado por el doctor David P. Stewart)

La Asamblea General de la OEA, en su cuadragésimo tercer período ordinario de sesiones (La Antigua, Guatemala, junio de 2013), adoptó la resolución AG/RES. 2811 (XLIII-O/13), en la cual encomendó al Comité Jurídico Interamericano que "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".

En el 83.º período ordinario de sesiones del Comité Jurídico Interamericano (Rio de Janeiro, Brasil, agosto de 2013), el Presidente solicitó al doctor David P. Stewart que actuara en calidad de relator del tema. La doctora Hyacinth Lindsay se ofreció a colaborar con el relator en este tema.

El punto de partida de este proyecto es la "Propuesta de declaración de principios de privacidad y protección de datos personales en las Américas", aprobada por el Comité en su 80.º período ordinario de sesiones en México, D.F., mediante la resolución CJI/RES. 186 (LXXX-O/12) (marzo de 2012) (véase también el análisis que consta en el informe acompañante en el documento CJI/doc.402/12 rev. 2). La finalidad de estos principios era instar a los Estados Miembros de la Organización a que adoptaran medidas para que se respete la privacidad, la reputación y la dignidad de las personas. Su propósito era servir de base para que los Estados Miembros consideraran la posibilidad de formular y adoptar leyes con objeto de proteger la información personal y los intereses en materia de privacidad de las personas en las Américas.

En vista de las instrucciones subsiguientes dadas por la Asamblea General en la resolución AG/RES. 2811, lo más apropiado como paso siguiente parece ser una explicación detallada de esos principios con miras a su aceptación y aplicación por los Estados Miembros, incluida la posibilidad de elaborar "una ley modelo sobre protección de datos personales", teniendo en cuenta los sucesos y las normas internacionales pertinentes.

Con ese fin, en los últimos meses el relator llevó a cabo intensas consultas con expertos y otros que intervienen en la formulación de principios y prácticas pertinentes, incluso en el ámbito de la Unión Europea y otros grupos regionales, así como con representantes de instituciones gubernamentales, académicas, empresariales y no gubernamentales. A fines de febrero, el relator participó, junto con Dante Negro, Director del Departamento de Derecho Internacional, y Magaly McLean, Oficial Jurídico Principal, en una reunión muy útil organizada en La Antigua, Guatemala, por la Red Iberoamericana de Protección de Datos Personales. También se ha pedido a los Estados Miembros de la Organización que informen sobre sus prácticas y leyes vigentes en la materia.

En opinión del relator, los principios propuestos por el Comité han tenido una acogida favorable en general. En ningún caso se ha respondido que los principios contengan errores fundamentales o incluso defectos graves. La mayoría de los comentarios han sido en el sentido de que 1) es necesario ahondar en la explicación y el contexto o 2) los principios no son exactamente iguales a las directrices o fórmulas particulares adoptadas en otros contextos.

Como resultado de estas consultas, el relator cree que la orientación más apropiada para este proyecto, por lo menos para la próxima fase, consiste en la preparación de una propuesta de guía legislativa para los Estados Miembros. Esta guía legislativa debería basarse principalmente en los 12 principios adoptados anteriormente por el Comité, tomando debido conocimiento y cuenta de los diversos conjuntos de directrices preparados en la Unión Europea, la OCDE, APEC, etc. En lo esencial, habría que explayarse en los principios, proporcionando un contexto más amplio y orientación a los Estados Miembros a fin de facilitar la elaboración de leyes nacionales. De esta forma, el tema central seguirá siendo los principios y las prácticas, teniendo en cuenta aquellos que ya existen en la materia, en vez de tratar de llegar a un acuerdo sobre los detalles exactos de un texto legislativo preciso.

En opinión del relator, el campo de la privacidad personal y de la protección de datos sigue caracterizándose por rápidos adelantos tecnológicos, así como una evolución constante de las amenazas a la privacidad personal. Asimismo, las respuestas a estos sucesos y amenazas han sido diferentes en distintas regiones del mundo. En las Américas no parece haber surgido un enfoque “regional” coherente. Para explayarse en los principios, el Comité podrá recurrir a los logros de otras regiones, teniendo en cuenta al mismo tiempo los sucesos de nuestro propio continente, a fin de formular una propuesta de marco que los Estados de las Américas puedan usar para abordar este campo crucial. Sencillamente, parece prematuro a esta altura dedicar tiempo a la redacción de leyes o disposiciones de códigos. Lo que se necesita es más interacción con los Estados Miembros.

Un resultado que podría ser útil sería un volumen para distribuir a los Estados Miembros (gobiernos, legislaturas, expertos, etc.) que contuviera 1) los Principios de la OEA sobre la privacidad y la protección de datos, 2) una explicación detallada de los asuntos abordados en dichos principios y las consideraciones que deberían tenerse en cuenta al plasmarlos en la legislación interna, y 3) una compilación de instrumentos pertinentes de todo el mundo (entre ellos, por ejemplo, la directiva general de la Unión Europea sobre la protección de datos, los Principios de Madrid, las directrices de la OCDE sobre la protección de la privacidad, el Marco de Privacidad de la APEC, diversas leyes nacionales y “códigos de conducta”). Si de hecho se puede redactar una posible ley modelo, también podría incluirse.

Para ejemplificar en qué podría consistir una “elaboración de los principios”, en el adjunto al presente informe se incluye un anteproyecto de análisis de ese tipo en relación con los cuatro primeros principios. Se agradecerán comentarios sobre el enfoque reflejado en dicho adjunto.

Adjunto A
Borrador interno - 24 de febrero de 2014
Comité Jurídico Interamericano

PRINCIPIOS DE LA OEA SOBRE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS

La finalidad de la explicación siguiente de los Principios de la OEA sobre la privacidad y la protección de datos es proporcionar una guía para la preparación e implementación de leyes nacionales y prácticas conexas en los Estados Miembros de la OEA. El propósito fundamental de los principios es establecer un marco para garantizar los derechos fundamentales de la persona a la protección de datos personales y a la autodeterminación en lo que respecta a la información. Con estos principios se procura en particular proteger a las personas de la recopilación, el uso o la retención ilícitos o innecesarios de datos personales e información personal.

Los principios se basan en principios internacionalmente reconocidos. Están relacionados entre sí y deben interpretarse en conjunto. Además, cada Estado Miembro de la OEA debería adoptar una política clara y eficaz de apertura y transparencia para todos los sucesos, prácticas y políticas con respecto a datos personales e información personal.

En la legislación nacional se deben establecer reglas efectivas para la protección de datos personales que den efecto al derecho de la persona a la privacidad y que respeten su información personal. La información personal puede recopilarse solo con fines legítimos y debe procesarse de una manera justa, legítima y no discriminatoria. En particular, la finalidad de estas reglas debe ser que las personas reciban la información necesaria sobre las personas o entidades que recopilan la información, el propósito para el cual se la recopila, los mecanismos de protección conferidos a las personas y las formas en que las personas pueden ejercer esos derechos.

Al mismo tiempo, la legislación nacional debe proteger el derecho de las personas a beneficiarse de la economía digital y de los flujos de información que la sustentan. 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 los intereses de las organizaciones en el uso de datos personales con fines comerciales legítimos y razonables. Las leyes sobre privacidad deben permitir que los consumidores y las empresas se beneficien del uso de datos personales de una manera segura y protegida. Deben ser equilibradas y tecnológicamente neutrales y permitir el libre flujo de información dentro de cada país y entre fronteras nacionales de una forma que fomente la innovación y el crecimiento del comercio.

Además de 1) la protección efectiva de la privacidad y 2) la promoción del libre flujo de información y del progreso económico, los Estados deben aplicar también 3) una política general de transparencia con respecto a sus políticas y procedimientos. Los Estados podrían ofrecer mecanismos de protección adicionales para la privacidad de los datos personales.

Ámbito de aplicación

Estos principios se aplican a los sectores público y privado por igual, es decir, tanto a los datos personales generados, recopilados o administrados por entidades públicas como a la información recopilada y procesada por entidades privadas. Se aplican tanto a los datos personales

impresos como a los archivos electrónicos. No se aplican a los datos personales utilizados por una persona exclusivamente en el contexto de su vida privada.

Definiciones

Datos personales. La frase “datos personales” abarca toda información sobre una “persona identificada”. Una persona identificada es una persona física que ha sido identificada o que puede serlo, de manera directa o indirecta, en particular por referencia a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social. Esta definición reconoce que, en muchas circunstancias, se puede recopilar o procesar información de forma tal que no se identifique a una persona en particular.

En los principios se usan intencionalmente las palabras “datos” e “información” a fin de conferir la mayor protección posible a los derechos de las personas afectadas.

A efectos de estos principios, solo la gente (personas físicas) tiene intereses en materia de privacidad, a diferencia de los dispositivos, las computadoras o los sistemas mediante los cuales interaccionan. Tampoco tienen intereses en materia de privacidad las organizaciones u otras personas jurídicas con las que tratan. Los menores (personas que no han llegado a la edad adulta) también tienen intereses legítimos en materia de privacidad que deben reconocerse y protegerse efectivamente en la legislación nacional.

Datos personales sensibles. La frase “datos personales sensibles” abarca los datos que afectan a los aspectos más íntimos de las personas físicas, entre ellos, por ejemplo, la información relacionada con su salud personal, preferencias sexuales, creencias religiosas o filosóficas, opiniones políticas u origen racial o étnico. Estos datos se consideran “sensibles” y merecedores de protección especial porque, si se manejan o se divulgan de manera indebida, es muy probable que conduzcan a graves perjuicios para la persona o a discriminación ilegítima o arbitraria.

Titular de los datos. Es la persona cuyos datos personales se recopilan, almacenan, utilizan o difunden.

Personas o entidades encargadas de la información. [Por determinar]

Autoridades. [Por determinar]

PRINCIPIOS DE LA OEA SOBRE PRIVACIDAD CON ANOTACIONES

PRINCIPIO UNO: PROPÓSITOS LEGÍTIMOS Y JUSTOS

Los datos personales y la información personal deben ser recopilados solamente para fines legítimos y por medios justos y legales.

Este principio abarca dos elementos: 1) los "fines legítimos" para los cuales se recopilan inicialmente los datos personales y la información personal y 2) los "medios justos y legales" con los cuales se efectúa la recopilación inicial.

La premisa es que muchas o incluso la mayoría de las intrusiones en los derechos de las personas pueden evitarse si se respetan los principios conexos de legitimidad y justicia desde el comienzo, cuando se recopilan inicialmente los datos. Desde luego, estos principios se aplican y deben respetarse en todo el proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales, no solo en el momento de su recopilación. Sin embargo, es más probable que se cumplan y se respeten si se recalcan desde el comienzo.

Fines legítimos

El requisito de legitimidad del fin para el cual se recopilan datos personales es una norma fundamental, profundamente arraigada en valores democráticos básicos y en el estado de derecho. Por ejemplo, el artículo 11 de la Convención Americana sobre Derechos Humanos dispone que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". Véase también el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. En el artículo 5 del Convenio N.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 1981, se enuncia la siguiente obligación para todas las Partes: "Los datos de carácter personal que sean objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente". Las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales y los Principios de privacidad de la información de APEC también contienen un "principio de limitación de recogida" o disponen, entre otras cosas, que los datos "deberán obtenerse con medios legales y justos".

El requisito de legitimidad también excluye la recopilación arbitraria y caprichosa de datos personales. Implica transparencia y una estructura jurídica a la cual pueda tener acceso la persona cuyos datos estén recopilándose.

En muchos contextos se podría hacer cumplir el requisito de legitimidad exigiendo que la persona o entidad encargada de la información informe al titular de los datos sobre las bases jurídicas de la solicitud de los datos en el momento de su recopilación (por ejemplo, "se solicita su número de identificación personal de conformidad con la Ley de Registro Nacional de 2004" o "la Directiva 33-25 del Ministerio de Economía"). En otros casos podría necesitarse una explicación diferente, como "se requiere esta información para garantizar que el reembolso se envíe a la dirección correcta del reclamante".

Medios justos y legales

El principio uno también requiere que los medios que se empleen para recopilar datos personales sean "justos y legales". La información personal se recopila por medios justos y legales cuando la recopilación es compatible *tanto* con los requisitos jurídicos pertinentes *como* con las expectativas razonables de los titulares de los datos basadas en su relación con la persona o entidad encargada de recopilar la información y en el aviso o los avisos dados a los titulares de los datos en el momento en que se recopile su información.

Este principio excluye la obtención de información personal por medio de fraude, engaño o con pretextos falsos. Se infringiría, por ejemplo, si una organización se hiciera pasar por otra en llamadas de telemarketing, avisos publicitarios impresos o mensajes por correo electrónico a fin de engañar a los consumidores e inducirles a divulgar el número de su tarjeta de crédito, información sobre cuentas bancarias u otros tipos de información personal delicada.

Naturalmente, la "justicia" es contextual y depende de las circunstancias. Requiere, entre otras cosas, que se ofrezcan opciones apropiadas a los titulares de los datos con respecto a la forma y el momento en que proporcionen información personal a personas o entidades encargadas de la información en los casos en que no sea razonable prever que pueda recopilarse la información en vista de la relación de los titulares de los datos con la persona o entidad encargada de la información y del aviso o los avisos que hayan recibido en el momento en que se recopiló su información. Las opciones que se ofrezcan a los titulares de los datos no deberían interferir en las actividades y en la obligación de las personas o entidades encargadas de la información de promover la seguridad externa e interna y el cumplimiento de la normativa ni impedir que tales personas o entidades empleen prácticas comúnmente aceptadas para la recopilación y utilización de información personal.

Al aplicar estos principios, los Estados Miembros podrían establecer, si así lo deciden, un requisito de "justicia" separado del tema del engaño.

PRINCIPIO DOS: CLARIDAD Y CONSENTIMIENTO

Se deben especificar los fines para los cuales se recopilan los datos personales y la información personal en el momento en que se recopilen. Como regla general, los datos personales y la información personal solamente deben ser recopiladas con el conocimiento o el consentimiento de la persona a que se refieran.

Este principio también se centra en la recopilación de datos e información. Abarca dos conceptos que gozan de amplio reconocimiento a nivel internacional: el principio de "transparencia" y el principio de "consentimiento". Combinados, estos principios requieren que 1) se especifiquen los fines para los cuales se recopilen datos personales; 2) tal especificación se efectúe a más tardar en el momento en el cual se inicie la recopilación; y 3) se recopilen datos personales e información personal solo con el conocimiento o el consentimiento de la persona a la que se refieran.

Además de los tipos o categorías de información personal que se recopilará, se debe informar a las personas sobre la forma en que podría usarse esa información, si podría darse a conocer a terceros y con qué fines, y qué medidas se han tomado para garantizar su exactitud.

Claridad

Los fines para los cuales se recopilen datos personales e información personal deben especificarse claramente. Además, se debe informar a las personas sobre las prácticas y políticas de las entidades o personas que recopilen información personal, a fin de que los titulares de los datos puedan tomar una decisión fundamentada con respecto al suministro de la información. El requisito de claridad refuerza la regla general de que la información puede recopilarse solo con el conocimiento o consentimiento de la persona a la que se refiera. Sin claridad, el consentimiento no puede ser válido.

Por consiguiente, los encargados de recopilar datos personales deben informar a las personas a las que se refieran esos datos como mínimo sobre el uso que darán a sus datos personales. Para que los titulares de los datos cuenten con fundamentos para decidir a quiénes proporcionarán sus datos personales y por qué razón, se necesita más información que los meros fines del manejo de esos datos.

Por lo tanto, es importante que a esas personas se les informe también sobre la forma en que se almacenarán y procesarán sus datos personales, incluida la identidad de los encargados de manejar esos datos e información para contactarlos, toda transferencia de datos que pueda efectuarse y los medios de que disponen para ejercer sus derechos con respecto a su información personal.

Consentimiento

La persona debe dar su consentimiento respecto de la recopilación de datos personales de la forma y con los fines previstos. El consentimiento de la persona debe basarse en suficiente información y debe ser claro, es decir, no debe dar lugar a ninguna duda o ambigüedad con respecto a la intención de la persona. Para que el consentimiento sea válido, la persona debe ser capaz de efectuar una elección real y no debe correr ningún riesgo de engaño, intimidación, coacción o consecuencias negativas significativas si se niega a dar el consentimiento. El consentimiento debe abarcar los detalles concretos de la información que se recopilará, los fines del procesamiento y toda divulgación que pueda efectuarse.

El método para obtener el consentimiento debe ser apropiado para la edad y la capacidad de la persona afectada y para las circunstancias particulares del caso. Evidentemente, el consentimiento obtenido bajo coacción o sobre la base de información engañosa no cumple de manera adecuada la condición para el procesamiento.

Como regla general, el consentimiento debe ser explícito. Sin embargo, en los principios se reconoce que, en algunas circunstancias, el “conocimiento” podría ser la norma apropiada en los casos en que el procesamiento y la divulgación de datos satisfagan intereses legítimos. El conocimiento o consentimiento de las personas con respecto a la recopilación de su información personal puede inferirse de sus interacciones con personas o entidades encargadas de la información, los avisos dados por las personas o entidades encargadas de la información, las prácticas comúnmente aceptadas con respecto a la recopilación y el uso de información personal, y las obligaciones legales de las personas o entidades encargadas de la información. El consentimiento implícito podría ser apropiado en unos pocos casos pero *nunca* con respecto a datos personales sensibles.

En todo caso, la parte que procure recopilar y procesar la información debe demostrar que tiene una necesidad clara de hacerlo para los fines de sus intereses legítimos o los de un tercero a

quien puedan divulgarse los datos. También se debe demostrar que hay un equilibrio entre los intereses legítimos de la parte que busque la divulgación y los intereses del titular de los datos. La condición de los "intereses legítimos" no se cumplirá si el procesamiento tendrá efectos perjudiciales en los derechos y libertades o en intereses legítimos del titular de los datos.

En los casos en que haya una gran discrepancia entre intereses en pugna, los intereses legítimos del titular de los datos tienen prelación. Por último, el procesamiento de información de acuerdo con la condición de los intereses legítimos debe ser justo y legal y ceñirse a todos los principios de la protección de datos. Los datos personales sensibles pueden procesarse sin el consentimiento de su titular solo en los casos en que ello sea de gran interés público.

Momento

Se debe informar a las personas sobre los fines para los cuales se recopile la información y se debe obtener su consentimiento a más tardar en el momento en que se recopilen los datos. En la mayoría de los casos, los fines deben expresarse claramente antes de obtener datos personales, a fin de que las personas en cuestión puedan tomar una decisión fundamentada sobre el suministro de la información.

En la mayoría de los casos, el consentimiento durará todo el tiempo que lleve el procesamiento al cual se refiera.

Una persona tiene derecho a retirar el consentimiento según la índole del consentimiento dado y los fines para los cuales se recopile la información. En general, el retiro del consentimiento no afecta la validez de lo que ya se haya hecho sobre la base del consentimiento.

PRINCIPIO TRES: PERTINENCIA Y NECESIDAD

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

La exactitud, la pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deben evaluarse en relación con el contexto específico en el cual se recopilen, usen y divulguen los datos y la información. Las consideraciones contextuales incluyen qué información particular se recopila y con qué fines.

Exactitud

Los datos recopilados de personas deben ser exactos y completos y estar actualizados con respecto a los fines para los cuales se hayan recopilado. Los datos inexactos pueden perjudicar tanto a la persona o entidad encargada de la información como al titular de los datos, pero en una medida que varía mucho según el contexto. Por lo tanto, el encargado de recopilar datos debe adoptar mecanismos para cerciorarse de que los datos personales que maneje sean correctos, exactos y completos y estén actualizados.

Podría o no ser necesario actualizar continuamente los datos y velar siempre para que estén completos a fin de que sean exactos en lo que se refiere al fin expreso para el cual se hayan recopilado los datos. En los Principios de privacidad de la información de APEC, el principio de la

integridad de la información personal requiere que los encargados de recopilar datos se cercioren de que la información personal sea "exacta, completa y debe estar actualizada *al grado necesario para los propósitos para los que será usada*". Análogamente, de acuerdo con el artículo 5, inciso *d*, del Convenio 108, los datos deben ser "exactos y *si fuera necesario* puestos al día". Las directrices de la OCDE contienen conceptos prácticamente idénticos en el principio de calidad de los datos.

Pertinencia

El requisito de que los datos sean "pertinentes" significa, básicamente, que los datos deben guardar una relación razonable con los fines para los cuales hayan sido recopilados y se tenga la intención de usarlos. Por ejemplo, los datos relativos a opiniones podrían ser fácilmente engañosos si se usan para fines con los cuales no guarden ninguna relación.

Necesidad

Los datos personales y la información personal deben recopilarse y usarse solamente para alcanzar los fines para los cuales hayan sido recopilados; por ejemplo, cuando sean necesarios para proporcionar el servicio o el producto solicitado por la persona. Deben ser acordes con los fines expresos de la recopilación y no excederlos. Deben seguir un criterio de "minimización", de acuerdo con el cual el encargado de la recopilación debe hacer un esfuerzo razonable para cerciorarse de que los datos personales que maneje correspondan al mínimo requerido para el fin expreso.

Proporcionalidad

En algunos sistemas jurídicos se usa el concepto de "proporcionalidad" para hacer referencia al equilibrio de valores en pugna. La proporcionalidad permite a las instancias decisorias determinar si una medida ha ido más allá de lo que se requiere para alcanzar una meta legítima y si los beneficios alegados excederán los costos previstos. En el contexto del procesamiento de datos del sector público, la idea de necesidad a veces se mide sobre la base de la proporcionalidad; por ejemplo, al exigir un equilibrio entre 1) el interés del público en el procesamiento de los datos personales y 2) la protección de los intereses de las personas en materia de privacidad.

En el Marco de Privacidad de la APEC (que, en cambio, trata exclusivamente de entidades comerciales encargadas de los datos), la palabra "necesaria" impone limitaciones al uso en vez de la recopilación, señalándose que "la información personal recopilada sólo debe ser usada para cumplir con los propósitos de recolección y otros propósitos compatibles o relacionados, excepto: a) con el consentimiento del individuo cuya información personal es recopilada; b) cuando sea necesaria para proporcionar un servicio solicitado por el individuo".

PRINCIPIO CUATRO: USO LIMITADO Y RETENCIÓN

Los datos personales y la información personal 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.

En este principio se enuncian dos premisas fundamentales con respecto a la retención de información: 1) los datos personales deben mantenerse y utilizarse de una manera legítima que no sea

incompatible con el fin para el cual se hayan recopilado, lo cual se conoce en la doctrina y la normativa mexicanas como “principio de finalidad”; y 2) los datos personales no deben mantenerse más del tiempo necesario para ese propósito y de conformidad con la legislación nacional correspondiente.

Uso limitado

Con respecto a la primera premisa, los datos personales y la información personal deben manejarse con propósitos específicos y legítimos, sobre los cuales se haya avisado a la persona afectada y en relación con los cuales tal persona haya dado su consentimiento. La retención y el uso de información personal debe ser compatible con las expectativas razonables de las personas, su relación con la persona o entidad encargada de recopilar la información, el aviso o los avisos proporcionados por la persona o entidad encargada de la información y las prácticas comúnmente aceptadas.

No deben mantenerse ni utilizarse datos personales con fines que no sean aquellos para los cuales se hayan recopilado, excepto con el consentimiento del titular de los datos o por mandato de ley. El concepto de “incompatibilidad” da cierto grado de flexibilidad en este sentido, ya que permite hacer referencia al objetivo o propósito general en relación con el cual la persona haya dado inicialmente su consentimiento para que se recopilaran datos. En ese sentido, la medida apropiada podría ser a menudo el respeto del contexto en el cual la persona haya proporcionado su información personal.

Por ejemplo, si un comprador da su nombre y dirección a un vendedor en línea y dicho vendedor, a su vez, da el nombre del consumidor y su domicilio particular al expedidor para que se puedan entregar al comprador los productos comprados, esa divulgación es evidentemente un uso “compatible” de datos personales. Sin embargo, si el vendedor divulga el nombre del consumidor y su domicilio particular a otro tipo de vendedor o comerciante con fines que no sean necesarios para completar la transacción en línea del consumidor y que no estén relacionados con dicha transacción, lo más probable es que sea un uso “incompatible” de los datos del consumidor y que no esté permitido salvo que el consumidor dé su consentimiento expreso.

Retención limitada

Asimismo, los datos personales pueden mantenerse solo 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. La realidad de la tecnología moderna exige una limitación para la retención de datos. Como el costo del almacenamiento de datos ha bajado considerablemente, suele ser menos costoso para muchas personas o entidades encargadas de la información almacenar datos indefinidamente en vez de examinarlos y borrar los que no sean necesarios. No obstante, la retención innecesaria y excesiva de datos personales tiene evidentemente implicaciones para la privacidad. Como regla general, por lo tanto, los datos deben eliminarse cuando ya no se necesiten para su fin original o tal como se disponga en la legislación nacional.

Sin embargo, eso no implica que las personas o entidades encargadas de la información deban *siempre* borrar datos cuando ya no los necesiten. Las personas pueden optar por consentir, ya sea de forma expresa o por implicación, en que se use y retenga su información personal con fines

adicionales. La legislación interna pertinente impone requisitos legales explícitos para la retención de datos.

Asimismo, una persona o entidad encargada de la información podría tener razones legales legítimas para retener datos durante un período determinado aunque no se lo requiera explícitamente. Por ejemplo, los empleadores podrían conservar expedientes de ex empleados o los médicos podrían conservar expedientes de ex pacientes a fin de protegerse de ciertos tipos de acción judicial, como juicios por mal ejercicio de la profesión, despido ilegal, etc. Las personas o entidades encargadas de la información pueden retener información personal durante períodos más largos de lo razonablemente necesario en los siguientes casos:

- para proporcionar servicios a personas, a fin de cumplir otras obligaciones legales;
- para proteger los derechos, la seguridad o bienes del titular de los datos, la persona o entidad encargada de la información o un tercero; o
- si se suprime la identificación de la información personal o se la combina de manera tal que ya no sea razonablemente posible identificar personas, computadoras u otros dispositivos.

84 pos março 2014
e450DI-2014 – Stewart- data protection
DS/msg – 25/2/2014
Luis Toro U. 3 de marzo, 2014