Doctrina

Título: El principio de accountability y el anteproyecto de protección de datos de Argentina: ¿Nuevo paradigma global de protección de datos personales?
Autor: Bermúdez Durana, José Alejandro
País: Argentina
Publicación: Revista Latinoamericana de Protección de Datos Personales - Número 4 - Noviembre 2017
Fecha: 15-12-2017 Cita: IJ-DXLIII-867

El principio de accountability y el anteproyecto de protección de datos de Argentina:

¿Nuevo paradigma global de protección de datos personales?

Por José Alejandro Bermúdez Durana

1. Introducción [arriba] -

Desde que en 1980 la OCDE publicó la primera versión de las Guías de Privacidad y Flujos Transfronterizos de Información, el principio de Accountability se ha venido convirtiendo en uno de los principios rectores en materia de protección de datos personales con más potencial para asegurar una efectiva protección de los datos personales de los titulares de la información.

Exigirles a las organizaciones que tratan datos que implementen programas efectivos e integrales de protección de datos personales (esto es, que materialicen el principio de accountability mediante la implementación de medidas efectivas y demostrables), es uno de los mecanismos más efectivos para alejarse de los modelos de simple compliance (donde el cumplimiento de la norma tiende a convertirse en un ejercicio formalista) y llegar a un modelo donde la protección de los datos personales se introduce en el ADN de las organizaciones. Esto último, mediante la adopción de verdaderas prácticas de gobernanza de la información con asignaciones claras de responsabilidad de manera transversal en toda la organización.

2. El principio de responsabilidad demostrada en las Guías de Privacidad de la OCDE del año 1980 [arriba] -

Desde 1978 se empezó a gestar el que quizá sea uno de los documentos seminales en materia de protección de datos: las Guías de Privacidad y Flujos Transfronterizos de Información cuya primera versión se aprobó por unanimidad en la OCDE en París en 1980. Concebido como un instrumento para intentar acercar principios comunes de los distintos países miembros de dicha organización multilateral, las guías recogieron ocho principios fundamentales de protección de datos que, aun hoy, más de 30 años después de su publicación, siguen plenamente vigentes y son reconocidos a nivel internacional como un estándar de buenas prácticas en gestión de información personal.

Dentro de los ocho principios recogidos en la versión de 1980 de las Guías se encuentra el Principio de Accountability, que de forma general hace un llamado a adoptar las medidas necesarias, en una organización, para instrumentar dentro de un programa los otros siete principios allí recogidos: (i) limitación en la recolección de datos, (ii) calidad, (iii) finalidad, (iv) limitación de uso o proporcionalidad, (v) seguridad, (vi) transparencia y (vii) participación individual.

De forma concreta, el principio de accountability como se incorporó en dicha versión, establece que "un responsable (del tratamiento de datos) es responsable por el cumplimiento de las medidas que dan efectos a los principios citados (…)".

En otras palabras, el principio de accountability (o principio de responsabilidad o responsabilidad demostrada o proactiva, como ha sido traducido), hace un llamado a los responsables del tratamiento para que implementen medidas dentro de su organización que les permitan cumplir con los deberes establecidos en las guías.

Como se describe en Thirty Years After the OECD Privacy Guidelines, un documento editado por la OCDE para conmemorar el aniversario de las Guías, hoy existe un interés renovado en "como el principio puede ser usado para promover y definir la responsabilidad corporativa en la protección de la privacidad. El desarrollo de mejores prácticas de seguridad de la información y la mejora de las prácticas básicas de privacidad en las organizaciones en respuesta a la legislación sobre incidentes de seguridad en protección de datos indican una evolución en el accountability"[1].

3. El Proyecto Galway y los Elementos Esenciales del Accountability [arriba] -

Resulta oportuno referenciar el trabajo que sobre el particular se realizó en el denominado Galway Project, liderado por el Centre for Information Policy Leadership (CIPL), que en 2009 publicó el reporte denominado Data Protection Acountability: The Essential Elements. A document for Discussión. En ese documento, resultado de las discusiones de un grupo de expertos de los sectores de gobierno, industria y academia, se definieron los denominados elementos esenciales del accountability.

Esta aproximación ha sido recogida por muchas guías posteriores publicadas por autoridades de protección de datos, tal y como se describe en la sección siguiente de este escrito que describe las guías sobre responsabilidad demostrada publicadas en 2015 por la Superintendencia de Industria y Comercio de Colombia. En términos generales, el referido documento describe cinco elementos fundacionales que recogen la manera en que una organización puede implementar un enfoque basado en responsabilidad demostrada dentro de un programa integral de protección de datos personales.

Estos elementos esenciales, según se describen en el reporte de CIPL son los siguientes:

1. El compromiso de la organización frente a la responsabilidad demostrada y la adopción de políticas internas consistentes con criterios externos;

2. Mecanismos para implementar dichas políticas, incluyendo herramientas, entrenamientos y educación;

3. Sistemas internos de supervisión permanente, auditorías y verificación externa;

4. Transparencia y mecanismos de participación para los titulares, y

5. Medios de solución de controversias y mecanismos de cumplimiento externos[2].

Dentro de esta aproximación, resulta clave entender que en un modelo basado en la responsabilidad demostrada se espera de los responsables del tratamiento un compromiso con la protección de la información personal que va más allá del simple cumplimiento normativo. Así, a diferencia de aquellos modelos donde los responsables, para cumplir con la ley, se limitan a llevar a cabo un ejercicio de "lista de chequeo" frente a sus obligaciones

de cumplimiento derivados de las normas puntuales con obligaciones de compliance, un enfoque de responsabilidad demostrada tiene un alcance más amplio que se traduce en una menor exposición al riesgo y una protección reforzada de los derechos de los titulares. Por supuesto, un primer resultado será en todo caso el cumplimiento de la ley, pues el despliegue de medidas efectivas en la organización deberá tener como primer objetivo el cumplimiento legal.

Ello no obstante, como se describe acertadamente en el informe, "(u)na aproximación a la gobernanza de datos basada en el accountability se caracteriza por su foco en establecer metas de protección de datos para las organizaciones con base en los criterios que ya se encuentran establecidos en la legislación vigente y en permitirles a las organizaciones discreción en la determinación de cuáles son las medidas apropiadas para alcanzar dichos logros. Una aproximación basada en Accountability le permite a las organizaciones adoptar métodos y prácticas para alcanzar dichos objetivos en una manera que sea consecuente con sus modelos de negocios, tecnologías y los requerimientos de sus clientes".

Estos elementos esenciales sirvieron de base para orientar gran parte del debate sobre implementación práctica del principio de responsabilidad demostrada y a la fecha continúan siendo un referente válido frente a los criterios que deben orientar los cimientos de un programa integral de protección de datos personales.

4. La actualización de las Guías de la OCDE del año 2013 [arriba] -

En 2013, la OCDE publicó la versión revisada de las Guías de Privacidad donde quizá su desarrollo más notable fue el papel protagónico otorgado al principio de accountability, así como el desarrollo adicional que hizo frente a la definición de qué debe entenderse por un programa integral de protección de datos personales.

Esta versión revisada de las guías pone un énfasis en dos elementos de la gobernanza de datos: (i) la implementación práctica de la protección de datos en las organizaciones mediante una aproximación basada en la gestión de riesgos y (ii) un llamado a abordar la globalización de los flujos transfronterizos de información a través de mecanismos de interoperabilidad.

El primero de estos dos aspectos encuentra eco en el principio de responsabilidad demostrada, que no cambió frente a la versión original de las guías de 1980, pero sobre todo en la sección III de las Guías, titulada: "Parte Tres. Implementación del Accountability".

En esta sección, el llamado de ese organismo multilateral es muy claro en el sentido de instruir a los responsables para que (i) establezcan dentro de su organización un programa integral de protección de datos, (ii) estén preparadas para demostrar dicho programa, a solicitud y (iii) establezcan mecanismos para notificar a las autoridades y/o a los titulares, cuando se produzcan incidentes con la potencialidad de afectar la información personal de los individuos.

El literal a) del numeral 15 de las guías establece que dicho programa de protección de datos debe:

(i) Dar efecto a las guías de la OCDE para toda la información personal sobre la cual haga tratamiento;

(ii) Estar confeccionado a la medida para la estructura, escala, volumen y sensibilidad de los datos tratados;

(iii) Proveer mecanismo adecuados de protección basados en evaluaciones de riesgo;

(iv) Estar integrado en su estructura de gobernanza y establecer mecanismos internos de supervisión;

(v) Incluir planes para responder a consultas e incidentes, y

(vi) Estar actualizado con base en un monitoreo permanente y evaluaciones periódicas[3].

5. El principio de Accountability en el nuevo Reglamento Europeo de Protección de Datos Personales [arriba] -

De forma no exhaustiva, conviene hacer referencia a cómo el principio de accountability ha venido ganando tracción como una aproximación cada vez más relevante para la protección de la información personal de los titulares. La interacción de los ciudadanos con empresas y organizaciones que recogen información de manera global, a través de múltiples dispositivos y en formas que retan el entendimiento tradicional de cómo proteger nuestra información, se ha convertido en un escenario para la innovación legislativa.

En estas situaciones, imponerle una carga mayor a las organizaciones, indicando la obligatoriedad de desarrollar programas de protección de datos, se convierte en una alternativa favorecida en distintas jurisdicciones para proteger la información.

En el caso europeo, son notorias las disposiciones que privilegian una aproximación basada en el accountability o responsabilidad demostrada. En concreto, el reglamento hace un primer reconocimiento del principio de accountability en el considerando 74 cuando establece que:

“Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas”[4].

Este texto, que recoge en gran medida los contenidos esenciales del numeral 15 de las guías revisadas de la OCDE, se complementa con el considerando 78 que establece lo siguiente:

“La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumpla en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrán consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de sus datos y al responsable del tratamiento crear y mejorar elementos de seguridad”.

Los considerandos transcritos anteriormente se desarrollan entre otros en el artículo 24 del Reglamento que es del siguiente tenor literal:

“Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertadas de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es confirme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Como se puede observar, el nuevo Reglamento Europeo, que entrará en plena vigencia en mayo de 2018, recoge los conceptos esenciales de las Guías revisadas de la OCDE y envía un mensaje importante a las organizaciones en cuanto a la manera en que debe afrontarse la conformación de un programa de protección de datos que tenga como objetivo fundamental la protección efectiva de la información personal: las organizaciones son las llamadas a establecer medidas efectivas internas que se ajusten a sus realidades operativas y deben estar en capacidad de demostrarle a las autoridades, o a cualquier tercero, cuáles son esas medidas, cómo se implementaron y en qué medida son efectivas para proteger la información personal de los ciudadanos.

6. El caso colombiano [arriba] -

Colombia ha sido uno de los países latinoamericanos que más ha abogado por el desarrollo del principio de accountability como un mecanismo para proteger efectivamente a los titulares. Este desarrollo se materializó por primera vez con su reconocimiento reglamentario, mediante su inclusión en el Decreto 1377 de 2013. De igual manera, fue acogido por la autoridad de protección de datos, la Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio, como se desprende del texto de las Guías para la Implementación del Principio de Responsabilidad Demostrada de 2015, de las decisiones tomadas en diversas investigaciones adelantadas por la entidad e inclusive en la reciente Circular Externa No. 5 sobre transferencias internacionales de datos.

La primera referencia a la responsabilidad demostrada en Colombia se incluyó en el Decreto 1377 de 2013, reglamentario de la Ley Estatutaria 1581 de 2012. Específicamente, el gobierno introdujo dentro de esa norma dos artículos de gran importancia para el desarrollo del concepto en Colombia. El capítulo VI de ese decreto, que recoge dichos artículos, estableció lo siguiente:

“Responsabilidad demostrada frente al tratamiento de datos personales

Artículo 26. Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

(…)

Artículo 27. Políticas internas efectivas. (…) Dichas políticas deberán garantizar:

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.

2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.

4. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto". (Subrayas fuera del texto original).

Como se desprende del texto citado, durante el proceso de reglamentación de la norma en Colombia, resultó de gran utilidad la discusión que en ese entonces se estaba dando frente al que sería el texto revisado de las Guías de Privacidad de la OCDE. En efecto, el Decreto 1377 de 2013 tuvo la particularidad de haberse expedido unos meses antes de dichas guías, pero recogiendo casi en su integridad los apartes más relevantes de ellas, con lo cual se logró anticiparse al instrumento normativo de dicho organismo introduciendo en el ordenamiento local una norma ajustada al nuevo debate global.

De forma novedosa, la norma incorporó un llamado a la autoridad de protección de datos, obligándola a tener en cuenta la implementación de programas integrales de protección de datos, por parte de una organización, como un criterio de atenuación frente a la imposición de una sanción de carácter administrativo por violación al régimen de protección de datos.

Con posterioridad a dicho decreto, y atendiendo entre otras cosas a los llamados de la industria que tenían interés en entender la manera práctica de volver operativo el principio de responsabilidad demostrada dentro de un programa, la Superintendencia publicó las Guías para la Implementación del Principio de Responsabilidad Demostrada que dotaron de elementos prácticos su implementación.

La SIC introdujo en dichas guías los siguientes aspectos fundamentales para la creación de un programa integral de protección de datos personales. De manera general, se previeron tres componentes fundamentales para el programa:

1. El compromiso de la organización, bajo el entendido de que solo si existe un compromiso corporativo con la protección de la información personal y la construcción de un programa integral, será posible que dicho programa sea efectivo en los términos descritos por la norma y las guías. Como subcomponentes de este punto se resaltan el involucramiento de la alta dirección como soporte del programa, la necesidad de contar con un oficial de protección de datos y la importancia de generar métricas, informes y mediciones para hacer un buen seguimiento del progreso del programa.

2. Los controles efectivos del programa, entendidos como aquellas medidas operativas que instrumentan el programa en la organización. De manera no exhaustiva podrían reseñarse los inventarios, las políticas internas, el sistema de administración de riesgo, los planes de capacitación internos, la gestión de terceros y los planes y protocolos de respuesta a incidentes.

3. Evaluación y revisión continua, bajo el entendido de que un programa de protección de datos de ninguna manera es un proyecto estático, que se ejecuta una sola vez sino que, por el contrario, requiere de un monitoreo y revisión continuo para asegurarse que no ha habido cambios internos (nuevos usos de los datos, adquisiciones, reorganizaciones) o externos (legislación, jurisprudencia, decisiones de la autoridad) con la potencialidad de afectar y dejar el programa desactualizado.

Finalmente, la Superintendencia de Industria y Comercio expidió en el pasado 10 de agosto, la Circular Externa No. 5 que tiene como propósito principal establecer los criterios para considerar que un tercer país es adecuado y definir las condiciones para obtener las declaraciones de conformidad. Además de la publicación de una "lista blanca" de países adecuados en dicha circular, con acertado criterio, se vinculó el principio de responsabilidad demostrada (accountability) como una condición que los responsables no pueden eludir en cualquier transferencia.

La inclusión del principio de responsabilidad demostrada dentro de dicha circular debería convertirla en un instrumento que facilitará las transacciones que involucran transferencias, pero manteniendo la efectiva protección del derecho de los titulares. Esto es especialmente claro al establecer que es deber de los responsables, en cualquier operación que involucre tratamiento, "implementar medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en el Régimen General de Protección de Datos Personales". Los responsables, además, deben poder demostrar la implementación de dichas medidas, inclusive cuando las transferencias se realicen a países "adecuados".

7. Breve comentario frente al anteproyecto de ley argentino [arriba] -

Argentina, país pionero en protección de datos en América Latina, tiene la posibilidad, con el proyecto de ley próximo a presentarse para debate legislativo, de actualizar su legislación e incorporar el principio de accountability como un principio rector de reconocida importancia.

Así parecen haberlo reconocido los redactores del proyecto al incluir dentro de su articulado el denominado principio de responsabilidad proactiva (art. 10 del proyecto actual), donde específicamente se establece el deber del responsable y/o encargado de adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente ley, y que le permitan demostrar a la autoridad de control su efectiva implementación".

El principio de accountability, o responsabilidad proactiva, como lo denomina el decreto, también se desarrolla en el artículo 19 del proyecto. Aun cuando el título del artículo se refiere de manera concreta al principio de seguridad de los datos personales, es clara la referencia al accountability que se desprende de pedirle al responsable que implemente medidas de seguridad que respondan al nivel de riesgo inherente por tipo de dato, al desarrollo tecnológico, y a la sensibilidad de los datos, entre otros aspectos.

Como conclusión, valga anotar que la protección de los titulares es mucho más efectiva cuando las normas y las autoridades de control centran sus esfuerzos en exigirles a los responsables que adopten un programa efectivo de protección de datos integral, con controles efectivos que se ajusten a su realidad operativa.

El primer gran beneficiado será el titular de la información, que en la práctica viene viendo como su autorización para el tratamiento de datos es en la inmensa mayoría de los casos un formalismo plagado de los formatos propios de los contratos de adhesión. Las autoridades de protección de datos, por su parte, reconocen cada vez más que la implementación de este enfoque reduce la carga operativa derivada de las reclamaciones mal atendidas y en cambio, les permite centrar sus recursos escasos de supervisión en las organizaciones con mayores niveles de riesgo. Finalmente, para las organizaciones responsables, adoptar estándares de responsabilidad demostrada se convierte en un mecanismo que minimiza el riesgo y eleva la concientización corporativa. Todo lo anterior, en contraste con los enfoques excesivamente formalistas (de mero cumplimiento), que en la práctica carecen de buenos elementos de gobernanza.

Notas [arriba] -

[1] OECD. Thirty Years After the OECD Privacy Guidelines. 2011.p. 53
[2] Centre for Information Policy Leadership. Data Protection Accountability. The Essential Elements. A document for discussión en https: //www.hunt on.com/files/webup load/CIPL-Gal way-Accounta bility-Paper. pdf. 2009.
[3] OECD. 2013 Revised Privacy Guidelines en http://www.oe cd.org/sti/iecon omy/privacy-gui delines. htm
[4] Reglamento Europeo de Protección de Datos en: http://eur-l ex. europa. eu/legal-con tent/ES/TXT/ ?uri=CELEX% 3A320 16R0679