

La ley de Habeas Data y sus implicaciones de seguridad informática

Por:

Jeimy J. Cano

Profesor Investigador

GECTI

Uniandes.

A pesar de que existen importantes reparos y análisis críticos al proyecto de ley relacionado con el habeas data, recientemente conciliado por la Cámara y Senado de la República de Colombia, efectuados por destacados juristas especializados, esta reflexión busca adelantar una revisión de las posibles implicaciones de seguridad de la información que establece la mencionada iniciativa legislativa que, luego de su tránsito por la Corte Constitucional para su revisión y concepto por esta corporación, podrá ser ley de la República.

Iniciemos por la revisión de algunas de las definiciones efectuadas en el artículo 3 de la norma:

c) Operador de información. Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente;

Esta definición establece que cualquier persona, entidad u organización que maneje datos personales estará sujeta a esta iniciativa legislativa. Si esto es así, los supermercados de cadena, los grandes y medianos almacenes de ventas y restaurantes, entre otros, se obligan a cumplir con los deberes y responsabilidades para proveer protección de dicha información, es decir salvaguardar los derechos de los titulares de los datos. ¿Será que dichas empresas tienen claro que de salir bien librada la revisión de este proyecto de ley por la Corte Constitucional, ellos deberán elevar sus niveles de protección de la información?

Ahora revisemos las definiciones de dato, previstas en este proyecto de ley:

e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;

f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) *Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.*

h) *Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.*

Considerando estos enunciados de datos, surgen varias preguntas para analizar: ¿Una dirección IP es un dato personal y semiprivado?. Si es así, ¿debe tener una protección especial?. En este sentido, ¿es viable utilizar software de protección u ocultamiento de dicha dirección?. Como bien sabemos la dirección IP (única durante la sesión de trabajo y diferente cada vez que nos conectamos) que el ISP nos asigna, establece una relación directa con un equipo y las personas que lo utilizan. Esta dirección lógica (IP) es parte del contrato de servicio de conexión a internet, la cual está asociada en el sistema del proveedor con el número telefónico desde el cual se marca. Si contamos con estos dos datos, tenemos la identificación de una familia u hogar, para un equipo particular.

Siguiendo con esta exploración, los correos electrónicos, los mensajes instantáneos, los mensajes de texto, los mensajes de voz, las imágenes, entre otros tipos de comunicaciones enviados o recibidos por las organizaciones podrían ser catalogados como datos personales, por lo cual deben contar con la protección propuesta con esta iniciativa de ley. Al estar definido un dato personal como “*cualquier pieza de información vinculada a una o varias personas*”, las categorías de mensajes enumeradas previamente serían otro elemento de análisis para considerar dentro de las medidas tecnológicas requeridas para dar cumplimiento a lo establecido en este proyecto.

Los principios sobre administración de datos referidos en el artículo 4 no consideran orientaciones internacionales como el “*Sedona Guidelines*”, donde se establecen de manera exhaustiva las características y requerimientos que son necesarios para una adecuada administración de información y registros. Así mismo, en este punto los comentarios y orientaciones del Archivo General de la Nación podrían ser interesantes. Sin embargo y pese a esta situación, revisaremos dos de los principios detallados por este proyecto de ley.

f) *Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;*

g) *Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.*

En el principio de seguridad se habla de “medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado”. Con esta enumeración se establece automáticamente un sistema de gestión de

seguridad de la información, apalancado en políticas, estándares y procedimientos que inician con una adecuada clasificación de la información y concluyen con un ciclo permanente de monitoreo y actualización de las medidas tecnológicas diseñadas para tal fin.

De manera disyunta al anterior, se presenta el principio de confidencialidad, que desde el punto de vista de la administración de la seguridad debería ser parte del anterior. En este punto el legislador quiso enfatizar en el tema de la reserva y buen uso de la información. Esta directriz no se puede lograr nuevamente sin una adecuada clasificación de la información y las medidas tecnológicas que de la clasificación se deriven.

Más adelante revisando el artículo 7, sobre los deberes de los operadores de los bancos de datos, se enumeran una lista importante de acciones que deben ser ejecutadas por los operadores. Si miramos en detalle la lista, vemos la necesidad de acogernos a las buenas prácticas internacionales del manejo de la información asociadas con el ISO27001, de tal forma que cumpliendo con lo que esta norma propone, se exceden las expectativas establecidas por la futura ley.

En el artículo 8, sobre los deberes de las fuentes de información, es decir cada uno de los ciudadanos, se establece en el numeral 2:

2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

La periodicidad no está definida y según se ve inicialmente, estará en manos del operador. Considerando que esta información cambia con frecuencia, el operador deberá establecer mecanismos expeditos que permitan una ágil y oportuna actualización de datos. Por lo tanto, los mecanismos vía web o a través de servicios en Internet serán una opción natural para ello. En consecuencia, los operadores deberán ofrecer elementos de comunicación confiables (no seguros) para que las fuentes de información efectúen sus actualizaciones. Esto podría dar un impulso importante al desarrollo de aplicaciones vía Internet.

Continuando con la lectura llama la atención en artículo 11, requisitos especiales para los operadores, el numeral 3:

Deberán contar con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.

Donde se reitera lo ya dicho en el artículo 4. Parece una repetición pero si miramos con cuidado, mientras en los principios se habla de medidas técnicas, en este se habla de un sistema de seguridad y demás condiciones técnicas suficientes. La pregunta que cabe aquí es ¿qué son condiciones técnicas suficientes?. Esta pregunta, nuevamente nos lleva a revisar el tema de gestión de seguridad de la información. Lamentablemente no está previsto en la ley el ente independiente que revise cómo se están cumpliendo las medidas previstas en este acto legislativo.

No obstante lo anterior, la ley establece en el artículo 17 (función de vigilancia) dos elementos de verificación al respecto, que deben ser ejecutados tanto por la Superintendencia de Industria y Comercio como por la Superintendencia Financiera según el caso:

3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.

4. Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.

Si vemos estas dos medidas, son realmente poco exigentes de lo que se requiere para proteger adecuadamente los datos personales. Las verificaciones deberían ser externas y validadas por un ente independiente que emita un concepto sobre el estado de las medidas de seguridad y control sobre los datos y que al mismo tiempo, diera orientaciones sobre los niveles de protección requeridas ajustados a los estándares internacionales. Bajo esta perspectiva, los ejercicios que se adelanten sobre el nivel de protección de los datos serán una rutina propia de los operadores y no un requisito exigible para continuar administrando los datos de sus fuentes de información.

Cuando se llega al artículo 18, sobre el tema de sanciones, es preciso ver algunos de ellos. Revisamos a continuación el siguiente:

Cierre o clausura de operaciones del banco de datos cuando, una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión.

Según se lee en este enunciado, las medidas correctivas deberán tomarse de manera global en la organización en su sistema de administración de los datos. Esto significa buena práctica en administración de seguridad de la información y un alto nivel de concientización y operación de la seguridad informática, no como un requisito técnico, sino como una cultura organizacional que afecta directamente los objetivos de negocio.

Si bien no hemos analizado artículo por artículo de esta iniciativa legislativa, si tratamos de ver algunas de las implicaciones que esta ley tiene para todas las organizaciones en el tema de seguridad de la información. Dichas implicaciones tienen un matiz eminentemente preventivo y propositivo, pues busca que tanto operadores, fuentes como usuarios reconozcan en la información un activo fundamental para las personas naturales y jurídicas, así como un bien jurídicamente protegido por el estado que es transversal a todas las actividades de los ciudadanos y la dinámica social, económica, política y tecnológica de un país. Sin embargo, al no detallarse las medidas de seguridad requeridas nuestros datos personales tendrían diferentes niveles de protección o seguridad de acuerdo con las implementaciones propias de cada entidad.

Esperemos pues que, este proyecto ley, pueda ser mejorado y ajustado en la sabia revisión de la Corte Constitucional y promueva un espíritu renovado para proteger y reconocer en

nuestros datos ese activo esencial que nos representa en un mundo interconectado y en una sociedad digital.