ANALISIS DEL DECRETO 1377 DE 2013

Comentarios en protección de datos en Colombia
Por: Ivan Dario Marrugo Jimenez[1]

Con la expedición del Decreto 1377 el pasado 27 de Junio de 2013 el Ministerio de Comercio, Industria y Turismo en asocio con el Ministerio de Tecnologías de la Información han puesto un nuevo peldaño en la escalera del sistema de protección de datos personales colombiano. Al reglamentar parcialmente (Aunque de manera general) la Ley 1581 de 2012, Colombia cuenta ahora con un nuevo bloque reglamentario que viene a complementar el escenario que venía construyéndose a partir de acciones de tutela. Este nuevo instrumento suma en riqueza los detalles construidos alrededor de un nuevo sistema que ahora debe construirse con el rigor de la práctica. Nuestro sistema, como joven, adolece de los trajines de la experiencia y hasta hoy se ha construido como un entorno teórico del cual se esperan demasiadas cosas. Solo la actuación de la Superintendencia de Industria y Comercio (Autoridad de Protección de Datos de Colombia) y el tiempo permitirán madurar el sector de la protección de datos, pero los vientos permiten augurar escenarios favorables en materia de prevención corporativa y por ende un sistema basado en el protagonismo empresarial.

Enmarcado bajo recientes protestas sociales e información global que involucra a estados con violaciones en materia de privacidad, de manera agónica se requieren nuevas reglas que hagan frente a los retos de protección de la privacidad en la era de la información; por ello contar con un sistema regulatorio actual y moderno no solo es una necesidad sino un imperativo para las naciones.

Las empresas colombianas no pueden permanecer ajenas a la nueva realidad corporativa global, por ello aspectos como la protección de datos, el gobierno corporativo y los principios de accountability (Como responsabilidad demostrada) dejaran de aparecer en horizontes lejanos y descontextualizados y se convertirán cada día más en parte de su realidad de negocio.

De forma analítica presentamos los principales aspectos contenidos en el decreto 1377 de 2013 con el fin de generar escenarios participativos y de discusión alrededor de este tema cardinal para la Sociedad de la información. A continuación resaltamos los principales aspectos:

1 Abogado 2.0. Especialista en Derecho de las tecnologías y Seguridad de la Información. Socio de Marrugo Rivera & Asociados, Estudio Jurídico.

El Art. 2 del decreto en comento llama la atención sobre un tipo de tratamiento excluido de la aplicación del régimen general de protección de datos. Se trata de los datos mantenidos en ámbitos meramente personales o domésticos. Señala el decreto, desarrollando el literal a del art. 2 de la ley 1581 de 2012, que se entiende por ámbito personal o domestico aquellas actividades inscritas en el marco de la vida privada o familiar de las personas naturales. Como ejemplo podemos traer el uso de un sistema de Videovigilancia privado en su domicilio personal que haga un ciudadano y cuyo efecto se mantenga en ese ámbito personal.

Un punto importante con relación al Art. 3 del decreto se refiere a que subsisten las inquietudes frente a lo que se entiende por Transferencia y transmisión de datos ya que estas nociones permanecen de manera imprecisa y aun no terminan por aclarar lo que aparece de manera indeterminada en la Ley 1581 de 2012. Al respecto puede inferirse del articulado (en contexto con el art. 26 de la ley) que ambas nociones guardan una estrecha consonancia pero debe advertirse que la transferencia hace alusión al procedimiento relacional (En el sentido consensual -mediando o no contrato-) entre el responsable y un receptor (Que adquiere el papel de responsable) ubicado dentro o fuera de Colombia. Por su parte la transmisión se refiere más a la operación (Proceso) de comunicar -enviar un flujo de datos-, en una relación de extremos, entre el responsable y el encargado. Debe notarse que la Ley señala que la transmisión implica per se un tratamiento sobre el dato, mientras que la transferencia no.

Bajo el capítulo 2 del decreto, se agrupan una serie de nociones frente al elemento Autorización bajo los principios que orientan el deber ser en el tratamiento de datos personales. En efecto, inicia el art. 4 por desarrollar bajo los principios de finalidad y libertad la forma en cómo debe operar la recolección de los datos de los titulares. Frente al Art. 7 del decreto se regula el modo de obtener la autorización bajo el amparo del art. 9 de la ley. Permite el tratamiento automatizado de la autorización para el tratamiento, siempre que ella se manifieste por escrito o de forma verbal o por medio de una conducta del titular que permita inferir de forma razonable su consentimiento en el tratamiento de la información. Aclara el artículo que a esta inferencia no puede arribarse por vía del silencio del titular. El art. 9 del decreto al desarrollar la facultad del titular de revocar la autorización y por esta vía suprimir sus datos introdujo como obligatorio para el responsable y/o encargado la disposición de mecanismos gratuitos y de fácil acceso para presentar su solicitud de supresión. Efectuada la reclamación por parte del titular el encargado contará con 15 días hábiles (En términos generales) para proceder a su supresión so pena de ser sancionado.

Especial mención hacemos del Art. 10 del decreto ya que introduce un procedimiento para la refrendación o validación de los datos personales

recogidos con anterioridad a la vigencia del Decreto. La disposición en mención impone a los responsables y encargados un procedimiento que deberá cumplirse a fin de continuar con el tratamiento de datos personales sobre Bases de datos anteriores al decreto. De la redacción del artículo 10 tenemos que podrán validarse los datos recogidos en bancos de datos hasta el día 26 de Junio de 2013 así:

El responsable solicitará la autorización a los titulares para continuar con el tratamiento; esto lo podrá hacer por un medio automático (esto es un mail, acceder a una web, un landing page, navegar en el sitio? etc) permitiendo que el titular autorice por cualquier medio su tratamientoi. En esta misma comunicación el responsable deberá hacer conocer al titular su política de tratamiento de la información así como el modo de ejercer sus derechos a Conocer, Actualizar, Rectificar y Suprimir sus datos. Si transcurridos 30 días hábiles a partir de dicha comunicación, el titular no expresa su intención de supresión del dato, la norma supone que ha operado la autorización y por ende el responsable o encargado podrá continuar con el tratamiento en las condiciones y finalidades señaladas en la política. En todo caso, subsistirán para el responsable el cumplimiento de todas las reglas y principios en el tratamiento de los datos. Crea el parágrafo del artículo 10 del decreto un periodo de gracia de 30 días para quien requiera implementar medios alternativos de comunicación con los titulares.

El capítulo 3 del Decreto aborda la cuestión de las Políticas de tratamiento como documento cardinal para el establecimiento de un macrosistema de aseguramiento de la información en las organizaciones. Este documento será la carta de navegación para las empresas para el manejo adecuado en protección de datos. Así mismo se advierte de la necesidad de confeccionar el Aviso de privacidad como otra herramienta para la difusión de las políticas a los titulares de los datos. El Art. 16 señala la obligación de conservar el modelo de aviso de privacidad utilizado en momentos específicos, por lo que deberán las empresas adoptar mecanismos para su conservación. El art. 19 a su vez señala que por medio de instrucciones en materia de seguridad de la información, la Superintendencia de Industria y Comercio impartirá directrices las cuales constaran en circulares y/o resoluciones. El art. 23 del decreto hace obligatorio la adopción a nivel organizacional de la función de responsable de los datos personales. Al señalar que esta designación puede ecaer sobre una persona o un área configura de manera amplia la forma en que las empresas podrán cumplir con dicho requisito.

Por otra parte, tratándose del capítulo 4 del Decreto que regula la transmisión y transferencia internacional de datos, persisten como arriba señalamos, serias dudas sobre el alcance de ambas figuras. Parece existir un yerro en el Art. 24, ya que en el numeral 2 se habla expresamente de la transmisión internacional de

datos sin que sea necesario informar al titular de tal circunstancia (la transmisión) ni contar con su autorización si entre el responsable y el encargado media un contrato. Mediante una interpretación rigurosa del Articulo en su contexto entendemos que esta exclusión también debe amparar la transmisión de datos que se hace dentro del territorio nacional; Sin embargo la redacción de la norma está desarrollada para otorgar dicho beneficio solo en la transmisión internacional y no para la nacional. Bajo el Art. 25 se señala que el contrato entre responsable y encargado deberá especificar las circunstancias especiales y las principales características del instrumento regulador de la relación entre el dueño de la base de datos y quien la gestiona. (Encargado).

El último capítulo del decreto se encarga de desarrollar el postulado de responsabilidad demostrada, como deber empresarial en el tratamiento de datos personales. Esta demostración se analizará a petición de la Delegatura de protección de datos, teniendo en cuenta entre otros factores: El tamaño de la empresa, su naturaleza jurídica, la naturaleza de los datos, el tipo de tratamiento y los riesgos potenciales. Establece el artículo 26 del decreto que la Superintendencia podrá requerir a las empresas para que suministren una descripción de sus procedimientos asi como evidencia de las medidas adoptadas en materia de aseguramiento de la información. Esto último no parece apropiado en esta etapa, ya que es deber de la Superintendencia impartir directrices en esta materia, lo que se hará a medida que se desarrolle nuestro sistema de protección de datos. Por lo anterior este último escenario se dificulta en su condición temporal por lo anteriormente señalado. Finaliza el Articulo 27 señalando que la Superintendencia impartirá las directrices tomando como parámetros de revisión en las organizaciones:

1. El que exista una estructura en la organización que propenda por la implementación de reglas sobre protección de datos.
2. Se adopten mecanismos internos para llevar a la práctica las políticas.
3. Procesos que garanticen la atención de las prerrogativas de los titulares en ejercicio de los derechos a Conocer, Actualizar, Rectificar y Suprimir (CARS) la información que sobre ellos se ha recogido.

Por expresa disposición normativa, la adopción de estos parámetros contaran para las organizaciones como atenuantes en los procesos sancionatorios.

Conclusión

El uso continuo y profuso de sistemas de información en las empresas han significado verdaderos e importantes beneficios. Así mismo debe reconocerse que estos beneficios conllevan al aumento en la complejidad de las operaciones. La cada vez mayor dependencia de los sistemas obligan a las empresas a

adoptar medidas direccionadas al control de sus activos y por ende de los datos. Colombia consciente de esta realidad ha iniciado los pasos para ponerse a tono a nivel internacional en esta materia. Sobre la actuación de la Delegatura de protección de datos, descansará gran parte del grado de maduración de nuestro sistema así como en la capacidad empresarial de asumir el importante reto que representa la protección de datos personales.

i Podemos inferir que el reglamento permite la autorización mediante navegación en un sitio web - Browse Wrap (Como forma de expresión mediante una conducta inequívoca y permitiendo el acceso suficiente a la política de privacidad y tratamiento de la información) anotando que en presencia de una visión preventiva y de ultima ratio tal circunstancia debe evitarse.