Protección de Datos Personales Ley 1581 Octubre de 2012

Garzón García, Janier Rolando.
janierrol@gmail.com
Universidad Piloto de Colombia

Resumen- Constitucionalmente las personas Colombianas tienen derecho a conocer, actualizar, rectificar su información Personal, así mismo exigir a entidades de cualquier naturaleza o razón social que hayan almacenado sus datos a tener un control de almacenamiento y uso de los datos personales, por ello es de vital importancia poner en contexto la Ley Estatutaria 1581 de 2012 mediante la cual se regula el control de la información personal tanto en entes públicos como privados, con el fin de proteger los deberes y derechos fundamentales y el manejo que los mismos le dan a la información a nivel nacional; también se analiza la forma en la que la información es manejada a nivel mundial con el fin de conocer las alternativas que otros gobiernos han implementado al respecto.

Abstract - Constitutionally the Colombian people have to know, update , rectify their Personal Information , also require entities of any nature or social reason to store their data to take control of storage and use of personal data , so it is vitally important to contextualize the Constitutional law 1581 Act , 2012 by which it control personal information in both public and private entities in order to protect the fundamental rights and duties and the handling that people give to the information and is regulated on national level; also the way in which information is handled globally in order to determine the alternatives that the Colombian government based on success stories in other countries can implement.

Índice de Términos— Almacenamiento, Confidencialidad, Datos personales, Derecho, Procedimientos, aviso de privacidad, dato público, dato privado, transferencia, transmisión, deberes, derechos.

I. INTRODUCCIÓN

Este documento muestra la preocupación del gobierno de aplicar la constitución nacional y hacer prevalecer los derechos consagrados allí, uno de estos es el derecho que tienen los colombianos sobre sus datos personales y la autorización que se debe otorgar sobre el tratamiento, almacenamiento por terceras personas o razones sociales. Es necesario conocer definiciones Claves en el contexto de la Ley 1581 y el decreto que la reglamenta, como Trasferencia, Trasmisión, Datos Sensibles, Dato Publico y Privacidad.

Sin embargo, antes de poner en contexto la ley se reconoce a la información como el activo más importante con el que cuentan las empresas, ello implica un alto grado de responsabilidad con el uso de la misma y más cuando se trata de datos personales, por ello se establece en el país esta ley para que tanto empresas como los ciudadanos conozcan cuáles son sus derechos y deberes en cuanto al manejo de datos, archivos e información suministrada, ya que casi desde el nacimiento de cada individuo consiente e inconsientemente siempre está dejando información registrada, empezando por sus registros de nacimiento, cuando se abren cuentas bancarias, al realizar transacciones tanto presenciales como virtuales y en la actualidad en situaciones tan comunes como el uso de herramientas tecnológicas como el internet y uso de redes sociales.

La falta de conocimiento que se tiene al respecto nos hace estar vulnerables y al mismo tiempo hacemos vulnerables a las personas que nos rodean cuando con actividades tan comunes como subir fotos y etiquetarlas permitimos que muchas personas puedan tener acceso a nuestros datos, un claro ejemplo de ello es colocar en un buscador de internet nuestros nombres, es sorprendente la cantidad de información que se registra, de la cual muy probablemente no hemos autorizado ninguna publicación.

En Colombia se considera la protección de los datos como un derecho fundamental, por esta razón es necesario que el estado garantice la vigilancia tanto en el sector público como privado con el fin de establecer políticas que cumplan con esas decisiones.

El titular de la información siempre debe autorizar inequívocamente para que un tercero pueda tener almacenamiento de la información. Donde el tercero deberá proveer los mecanismos necesarios para garantizar los procedimientos usados en la recolección uso y almacenamiento de información personal, también debe proveer una explicación exacta sobre porque la necesidad de realizar esta recolección de Datos.

También es necesario conocer dónde y en que ámbitos la Ley no es aplicable, como bases de datos personales almacenados con finalidad de defensa y seguridad nacional, inteligencia y contra inteligencia, información periodística y contenidos editoriales, así también archivos relacionados en las leyes 1266 de 2008, 79 de 2003.[1]
Con el desarrollo de esta ley se comienzan a cumplir objetivos de Seguridad de la información como Confidencialidad, integridad, disponibilidad, autorización.

La finalidad de lo expreso en la ley 1586 es protegernos como individuos, y garantizar el derecho a conocer y autorizar que información personal está en determinada base de datos y derecho a autorizar o no autorizar el tratamiento de dichos datos personales.

A continuación se describen algunos aspectos del estudio y revisión de la ley 1581 de 2012 y su decreto 1377 de 2013

II. DESARROLLO DE LA LEY 1581 DE 2012

A. Categorías Especiales de Datos

Es necesario comprender la sensibilidad de los datos y la forma en que están relacionados con datos de uso íntimo del propietario de la información, estos datos pueden ser orientaciones, Políticas, sociales, sexuales, datos biométricos o de salud.

Los datos anteriormente mencionados tienen y validan su importancia en evitar cualquier tipo de discriminación hacia el individuo, ya que estas características pueden ser usadas por bases de datos de terceros y generar limitantes en el libre desarrollo del individuo.

Hacia la comunidad es necesario llevar una información clara de la importancia que tienen sus datos, conocer que sus historias clínicas solo deben ser tratadas por el medico titular y el paciente, también al realizar concursos públicos, evitar situaciones de racismo, tratamiento discriminatorio en cuanto a su orientación sexual.

Se debe conocer en que entidades y bases de datos están alojados los datos personales, ya que se debe garantizar que nuestros datos no sean modificados por terceros y estén custodiados de posibles fugas de información que puedan llevar a suplantación de identidad y fraudes usando los datos almacenados. También existen excepciones en determinados casos como, que la ley no requiera autorización del titular para el tratamiento de dichos datos, situaciones jurídicas y judiciales y de defensa nacional.

La ley hace predominar los derechos de Niños, niñas y adolescentes, en cuanto a sus datos personales, esto aplica para las instituciones educativas, y hace crear conciencia de la importancia que tiene para los menores el uso de sus datos por entidades de terceros, aunque esta parte de la ley quedara establecida y reglamentada por el gobierno nacional dentro de los 6 meses siguientes a la publicación de la ley 1581 de 2012.

B. Deberes de los Responsables y encargados del tratamiento de los Datos personales

Para que se cumplan los deberes y derechos en el tratamiento de la información, se hace necesario que las entidades tengan una inversión en tecnología,

encaminados a una custodia adecuada de los datos autorizados para su manejo, las responsabilidades se basan en condiciones de seguridad y veracidad. El responsable también debe proveer mecanismos de autorización, garantizando en todo momento al usuario el ejercicio de modificación y restricción de sus datos almacenados.

Fig. 1 Derechos constitucionales [2]

El ministerio de comercio industria y turismo realizo unas disposiciones de carácter general acerca del tema en mención, las cuales están contempladas en el decreto 1377 de 2013, en el cual se establecen algunas definiciones que esclarecen la forma en la que se debe dar tratamiento a la información, el primer tema que aclara es acerca del aviso de privacidad que tiene por obligación quien solicite la información al titular de la misma, en vista de que la finalidad de la información debe quedar clara para ambas partes.

Otro concepto importante es que los ciudadanos deben saber que información es considerada dato público y cual no, en este caso se denomina dato público al estado civil de la persona, profesión, calidad de comerciante, funcionario privado o público, entre otros, los cuales no están sometidos a reserva y no afectan en nada la integridad de las personas. [1]

De la misma forma que se aclara cuales son aquellos datos sensibles que pueden en determinado momento vulnerar a la persona como lo son: orientaciones, raciales, étnicas, convicciones religiosas o cualquier tipo de información que promueva e influencie la participación en partidos políticos y temas relacionados especialmente con la sexualidad y datos médicos, por tratarse de datos sensibles el ciudadano no está obligado a autorizar su Tratamiento. [1]

Finalmente el decreto contempla la responsabilidad de la transferencia y transmisión de la información ya que la misma en ocasiones no es manejada únicamente a nivel Colombia sino que es trasladada a centrales establecidas fuera del país, lo que implica una transmisión de datos y un impacto más significativo a quienes son responsables de realizar dicho proceso.

En los últimos meses el país está siendo inundado de Correos y comunicados que por obligación y dando cumplimiento a la ley en mención envían múltiples empresas con el fin de dar conocimiento a los usuarios acerca de la existencia en la base de datos de la empresa, en los cuales existe un alto grado de probabilidad que muchos de los ciudadanos no sabían que tenían sus datos, estos correos hacen referencia a información relacionada a cumplir con el mandato de ley, mediantes los cuales informan al usuario que sus datos están almacenados, y que si no se responde el mail en un determinado plazo se entenderá como aceptado por el usuario el tratamiento y uso de los datos.

El concepto de la ley puede ser interpretado de varias maneras; en la forma de autorización que debe ser recibida de parte del usuario, ya que los mecanismos anteriores no cumplen con la premisa de la autorización por parte del usuario de forma expresa e informada para la recolección de datos [3] esto induce al usuario a aceptar algo que posiblemente no conoce olvidando sus derechos y respaldo legal contra el uso indebido de la información intima de cada ciudadano.

Las empresas que recolectan la información están autorizadas a recibir la aprobación por parte de los ciudadanos de diversas formas, entre ellas: por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una

conducta inequívoca. [1]

La superintendencia de Industria y comercio tiene el derecho de exigir a los responsables de captar la información la descripción del proceso utilizado, de la misma forma que indagar para que fin se utilizaran los datos recolectados, se castigara a quien utilice métodos fraudulentos para obtener información. También se debe contar con la prueba de autorización que concedió el titular de acuerdo a cada una de las formas de autorización mencionadas anteriormente; en los casos en los que el usuario se retracte de que su información sea manejada por alguna entidad debe presentar un reclamo formal y las entidades deben manejar una forma clara y visible por los usuarios para que pueda realizarse este procedimiento y de esta manera eliminar los datos del solicitante, las entidades encargadas contaran con un plazo máximo para realizarlo, de no ser así el usuario podrá presentar directamente ante la Superintendencia de Industria y Comercio la revocatoria de su autorización.

C. Proceso de los Datos recolectados antes de la aplicación de la ley

Las empresas no pueden dar por entendido que la información de los usuarios que manejan la pueden seguir utilizando; aunque se sigan manejando procesos se debe contar con un soporte de la autorización del titular de la información en el que se manifieste su deseo de dar continuidad, esto se puede realizar a través de los mecanismos de comunicación que eventualmente se tengan entre empresas y usuarios; de no lograrse dicha comunicación por razones como registros o bases de datos desactualizados, incorrectos, incompletos o inexactos; las organizaciones están en la obligación de utilizar medios masivos de comunicación como: periódicos, revistas, internet, entre otros e informar a la superintendencia de industria y comercio máximo a los cinco días siguientes a la publicación de la información con el fin de que la situación tenga un precedente. Una vez pasados 30 días desde los comunicados sin recibir autorización por parte de los usuarios se entiende que la empresa puede seguir manejando la información para las finalidades indicadas en la cámara de Industria y comercio.

III. LEYES DE PROTECCIÓN DE DATOS EN EL MUNDO

En Colombia el tema de protección de datos es algo relativamente nuevo, ya que a nivel mundial existen normas y leyes que tienen más de 10 años, lo que demuestra preocupación de los gobiernos por respaldar y resguardar la intimidad de los ciudadanos. En Europa, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 que garantiza una alta protección de los datos personales en todo el territorio de la Unión Europea [4]es pionero en la gestión de estos temas y han dado al mundo herramientas para el establecimiento de políticas de protección de datos.
Uno de los principales representantes de esta región es España en donde se establece el derecho Europeo denominado Ley Orgánica de protección de datos LOPD de cuyo cumplimiento se encarga la agencia Española de protección de datos desde el año 2007 que permite a los usuarios mantener el control de los datos personales, y mantener las políticas establecidas en la región con el fin de velar por la protección de cada uno de sus ciudadanos, de la misma forma que establecer mecanismos de control a las empresas; esta entidad tiene herramientas tecnológicas que permiten a las empresas a registrar todos los procesos que se hagan con el uso de la información con el fin de mantener un control exigente de los datos. [5]

Alemania tiene una de las leyes de protección de datos más estrictas en todo el mundo, en donde cada persona facilita y decide que datos estará dispuesto a suministrar y a quien; en este país contrario a los otros países Europeos las empresas no están obligadas a proporcionar sus bases de datos a ningún ente estatal.

En EEUU existe una ley denominada ley patriota de espionaje, la cual autoriza el espionaje de ciudadanos dentro y fuera del país, todas las compañías Americanas están obligadas a entregar la información de sus bases de datos para garantizar la protección de los datos y reducir cualquier riesgo.

En la Región Asia-Pacífico se realizó la reunión celebrado la versión 39 del "Asia Pacific Privacy Authorities Forum (APPA)" y contó con la participación de Colombia, como segundo país latinoamericano aceptado como miembro de APPA (Asia Pacific Privacy Authorities) [5], con esto Colombia puede adquirir y apropiar experiencias de muchos años de estos países y puede aplicar a la visión y leyes colombianas.

En el caso de América Latina, aun no es una realidad que se protejan los datos personales en su totalidad, aproximadamente desde el año 2013 se evidencio que no nos encontramos seguros, ya que se han dado a conocer muchos escándalos de espionaje uno de los más conocidos casualmente en el gobierno Colombiano.

Entre los países de la región se evidencia la presencia de leyes que protegen y velan por la información, a nivel general podemos catalogar dentro de las más importantes nombradas a continuación, las cuales desde el año 2000 en adelante han tomado fuerza y han hecho a los países a los que pertenecen más conscientes de la importancia de cuidar la información:

En Paraguay la Ley 1.682 del 16 de enero de 2001 se empieza a aplicar con la finalidad de proteger y delimitar específicamente los datos considerados sensibles, siempre y cuando los ciudadanos den autorización expresa y por escrito. [6]

En Panamá existen dos Normas: la Ley 6 de 22 de enero de 2002 que dicta normas para la trasparencia de la gestión pública, establece la acción de habeas data y otras disposiciones y la Ley 24 de 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito de los consumidores o clientes. [6]

En Brasil la ley 9.507 del 12 de noviembre de 1997 regula o el acceso a la información y disciplina o rito procesal de habeas data. [6]

En Ecuador, los artículos 30 a 45 de la Ley de Control Constitucional (18 de junio de 1997) regulan el habeas data, la cual cuenta con una ley (ley orgánica de transparencia y acceso a la información de mayo de 2004) la cual vela por la protección de la información pública personal [6]

Argentina es el único país de la región que cuenta con una agencia de protección de datos similar al modelo Europeo y certificado directamente por la Unión Europea quien les otorgo la calificación de un nivel adecuado de protección [6]

En Chile cuentan con la ley que protege la vida privada ley 19,628 del 30 de Agosto de 1999 quien destaca la protección de la información relacionada con los datos financieros y bancarios [6]

En Perú se encuentra la ley 27,806 de transparencia y acceso a la información pública de Julio de 2002, cuyo enfoque es muy parecido al Colombiano ya que vela por la protección de los datos personales y familiares, teniendo como prioridad cuidar la intimidad de las personas a través de mecanismos en los que los usuarios siempre autoricen el manejo de los datos que se manejaran. [6]

En Uruguay se establece la ley 17,838 de Octubre de 2004 está enfocada en la protección de datos personales basados en información estrictamente comercial, la cual también requiere para cualquier proceso la previa autorización para el titular de los datos. [6]

De esta manera se observa que las leyes de protección de datos a nivel Latinoamérica se ha constituida en los últimos 15 años, dando la importancia necesaria y constitucional que los datos personales representan en un mundo globalizado, donde la información es el activo más importante

IV. CONCLUSIONES

Con la aplicación de la ley de protección de datos personales se hace conciencia de la importancia que tienen los datos para el individuo y afirma los derechos de los colombianos consagrados en la constitución nacional, sobre el uso responsable de los datos que hacen parte de nuestra intimidad en la sociedad.

Es de vital importancia entender que la información es el activo más importante con el que

cuentan las empresas y con el avance de tecnologías de la información y un mundo más globalizado, es más común que la información no solo sea manejada localmente sino que circule rápidamente a nivel global, esto hace cada vez más indispensable que existan herramientas de control que prevalezcan los derechos y deberes de las personas. Con el boom de las tecnologías y la forma de interactuar de las personas en la redes sociales especialmente, se vulneran muchos de los aspectos contemplados en la ley de protección de datos, muchas veces sucede esto por desconocimiento, ya que en ocasiones por seguir las tendencias se comparte a diario una infinidad de información que circula en internet, de la cual no se es consciente en qué momento se autorizó; Hoy en día en las grandes redes sociales se evidencia un flujo importante de información sin control, un ejemplo claro de ello, es la compra de la empresa Facebook a WhatsApp con el fin de adquirir los datos telefónicos de cada usuario que está registrado, entre otros datos de agenda y correos electrónicos.

Gracias a la aplicabilidad de esta ley a nivel mundial , los individuos y empresas comprenderán el significado de Seguridad, confidencialidad, integridad, autenticidad, autorización, en relación al manejo e importancia que tienen los datos personales y se toma cada vez más conciencia de la responsabilidad del manejo de la información a nivel personal, las empresas también toman acciones para el manejo y control adecuado de la información, aprovechando el alto impacto que tienen en este momento nuevas herramientas y tecnologías de la información.

V. *REFERENCIAS*

[1] Ley Estatutaria 1581 de 2012, Decreto 1377 de 2013 REPÚBLICA DE COLOMBIA -GOBIERNO NACIONAL

[2] Abc para proteger los datos personales, Certicámara disponible en https://web.certicamara.com/media/47158/cartilla-abc-protecci%C3%B3n-de-datos.pdf

[3] Germán Realpe Delgado, revisado 25 Septiembre de 2013 disponible en www.enter.co/enterprise/la-privacidad-y-la-proteccion-de-datos-en-colombia/.

[4] Equipo de Redacción Mercado Dinero, revisado 25 Septiembre de 2013, disponible en: www.mercadodedinero.com.co/index.php/opinion/entrevista/5682-proteccion-de-datos-en-el-entorno-internacional

[5] Agencia Española de protección de Datos, Revisado Noviembre de 2014, disponible en: https://www.agpd.es/portalwebAGPD/jornadas/dia_proteccion_2011/responsable/index-ides-idphp.php

[6] Protección de Datos Personales en América Latina — Juan Pérez ante una disyuntiva de progreso y bienestar, Revisado 20 Noviembre de 2014, disponible en: http://www.iijlac.org/docs/juanperez.pdf

Autor

Janier Rolando Garzón García
Ingeniero Electrónico, Universidad de Cundinamarca
Estudiante candidato a Grado de Especialización en Seguridad Informática, Universidad Piloto de Colombia
2014