Recibido: 12/04/2015 **Aprobado**: 16/11/2015

ENSAYO

LOS DATOS PERSONALES Y EL AVANCE TECNOLÓGICO
Un campo para el desarrollo del derecho

Personal data and technological progress. A field for the development of law

Rosales Muñoz, E. y Bohórquez-Rodríguez, F.*

RESUMEN

El artículo aborda el tema de la viabilidad de utilizar el derecho fundamental del *Habeas Data*, cuando una persona jurídica que administra datos personales, específicamente cuando administradores de redes sociales realizan un trato indebido a los datos personales de los usuarios registrados en sus bases de datos; lo que genera inconvenientes de carácter personal como lo son las discriminaciones por razones de género, religiosas, ideas políticas, médicas, raza, entre otras, que generan el acceso a terceros malintencionados a esta información de carácter íntimo y personal. Se abordan los contextos del dato personal económico, social e internacional, donde el dato personal adquiere una fuerza e importancia económica que evidencia sus necesarios protección y tratamiento, como elemento fundamental para una integración por parte del individuo en las nuevas dinámicas sociales, y por la importancia de tener altos estándares y niveles de protección en el tratamiento de datos personales en las transferencias nacionales e internacionales, para garantizar la confianza por parte de los usuarios. Así mismo, se despliegan las herramientas de las que se dispone desde la legislación colombiana referente al trato para proteger los datos personales, para determinar si son suficientemente garantistas para el titular de datos personales cuando éste se encuentre en situaciones problemáticas que se generen por un trato, o una administración, indebido de los mismos. También se realiza una mirada a las legislaciones de otros países sobre las protecciones de los datos personales y el derecho de *Habeas Data*.

Palabras clave: dato personal, redes sociales, Internet, transferencias de datos personales, legislación colombiana.

ABSTRACT

The current paper talks about the viability of using the fundamental right of the "Habeas Data". When a legal entity that handles personal information, especially when the administrators of social networks, manage wrongly the data of the users in their data base. It creates several personal problems like: genre, religious, politics, medical, ethnic discrimination and many more reasons that allow the access of malicious third parties to intimate information that has been trusted since the first time and user sign in. It takes on multiple contexts about the personal information like the economic, social and the international. This information gets economic importance and that demonstrate its urge for protection and treatment, not only as a fundamental element for the integration of the individual in the new social contexts, but also because the importance of having high standards and levels of protection in the handle of personal data in the national and international transfers to guarantee the trust given by the users and to be a country considered to invest and to transfer that information for the economic growth. It also portraits the tools that the Colombian law has and the constitutional declarations about the correct treatment to protect the personal information and determine if it guarantee the people when they are in trouble generated by a mistreatment of it. Finally, it takes a look to other countries law about the protection of the personal information and the right of the "Habeas Data" to compare the levels of protection with the national levels.

***Key words**: Personal Data, Social Networks, Internet, Transfers of Personal Data, Liability, Colombian Legislation.*

* Estudiantes participantes de la clase Seminario de Investigación II a cargo de la investigadora Luisa Fernanda García Lozano en la Universidad Nacional de Colombia, durante el periodo 2015-II.

1. INTRODUCCIÓN

La internet, que desde sus principios en la década de 1970 ha sido una herramienta ha facilitado la transmisión de la información, a causa de su constante y acelerado desarrollo en la última década, ha llegado a generar una constante transferencia de datos. Datos que consisten no solamente en información general, sino en información de carácter personal la cual es trasferida de forma inmediata, globalizada e interactiva.

Al ser testigos y partícipes directos de esta globalización de datos de toda clase, por medio de la cual cada vez que se comparte información personal de forma indiscriminada a cualquier usuario que tenga acceso a las plataforma que tienen la información disponible, los mismos usuarios llegan a ser vulnerables debido a la cantidad de información que voluntariamente suben a dichas plataformas. Estos fenómenos constantemente pueden darse por la falta de educación acerca del adecuado manejo de los datos personales en la red, con la que participa toda clase de usuarios en páginas y portales que no proporcionan un aviso de privacidad ni cuentan con políticas de seguridad idóneas.

La falta de educación empieza por el desconocimiento de un derecho tan importante como lo es el derecho fundamental del *Habeas Data*. El cual se compone por una serie de acciones en cabeza del titular del dato personal, y que la Corte Constitucional de Colombia ha identificado, y de las cuales se distinguen: el derecho de las personas a conocer la información que sobre ellas está recogida en bases de datos, el derecho a incluir nuevos datos, el derecho a actualizar la información, el derecho a que la información contenida en bases de datos sea rectificada o corregida y el derecho a excluir información de una base de datos (Pretelt, 2011).

Por consiguiente, aunque es la jurisprudencia la que caracterizó de forma sistemática la acciones que componen el derecho de *habeas data*, lo cierto es que éste es un derecho que está recogido en diferentes textos legales, dentro de los cuales se identifican: la Constitución Política de Colombia en su artículo 15, la Ley Estatutaria 1581 de 2012, su Decreto Reglamentaria 1074 de 2015, y el Régimen especial de Protección de Datos (Ley 1266 de 2008) y sus Decretos Reglamentarios 2952 de 2010 y el 1727 de 2009.

A pesar de la vigente legislación y su intento por estar a la vanguardia de las nuevas tendencias, lo cierto es que en Colombia la administración de datos personales, en la actualidad, sigue teniendo un riesgo inminente de vulneración, para aquellas personas que hacen uso de medios electrónicos (transacciones bancarias, compras *online,* etcétera), haciendo evidente que la legislación y la normatividad que protege a los usuarios titulares de datos personales, no cumple de forma cabal con sus fines. Esta situación se manifiesta en el informe de la Superintendencia de Industria y Comercio, en el que se evidencia, sólo en el primer semestre del año 2014, que la Delegatura encargada de la protección de datos personales impuso en primera instancia 19 sanciones por la suma de $686.224.000 millones de pesos (Superintendencia de Industria y Comercio, 2014). Y es por tal razón que esta situación debe ser objeto de investigación, porque de forma preliminar las medidas tomadas por el Estado colombiano parecen ser insuficientes para solventar la necesidad de seguridad de las personas que proporcionan datos personales para acceder a innumerables portales en internet administradores de datos personales.

Incluso yendo más allá en la identificación de las causas de los problemas, puede no ser sólo la falta de regulación en materia de datos personales el inconveniente principal, sino el desconocimiento de las mismas normas existentes por parte de los intervinientes en el tráfico de datos personales otra causa. Existen empresas entre las que están la sociedad *American System Service S.A.S.* y la Cooperativa Multiactiva Universitaria Nacional y Redcord de Colombia S.A., que han sido sancionadas por la Superintendencia de Industria y Comercio por el indebido manejo de datos personales y obligadas a

pagar multas correspondientes al permitir que terceros accedieran a su red sin alguna restricción. Al estar frente a esa realidad, es posible argumentar que aún cuando el mecanismo adecuado para garantizar la protección de datos personales es el derecho fundamental del *Habeas Data*, el mismo no se aplica.

En definitiva, aún cuando se tiene en la legislación nacional normas que establecen principios mínimos por parte de los responsables de los datos que deben implementar en sus políticas de privacidad y protección, éstos siguen siendo vulnerados, razón por la cual, se debe considerar que el acceso masivo a información en pórtales de internet genera las interrogantes: ¿cómo lograr una protección real de datos personales a personas que suministran información de manera deliberada?, y ¿cómo lograr que el estado garantice, no solo la privacidad y confidencialidad de la información dada, sino también ejercer un control sobre aquellos que intenten vulnerar este derecho?

Este ensayo se desarrollará analizando en primer lugar la importancia del dato personal en el ámbito privado, en el ámbito económico y en el ámbito público con el Estado como ente regulador, para posteriormente pasar a hacer una exposición de la regulación nacional sobre los datos personales y su circulación. En un segundo lugar se realiza un análisis del manejo de los datos personales en el contexto digital de las redes sociales así como en el contexto internacional, para finalmente realizar una exposición y análisis comparativo de Colombia en cuanto a la protección y el manejo de datos personales con otros países, que permite caracterizar y delimitar de forma clara el papel del Estado frente al manejo de los datos personales y su protección por medio del *habeas data*.

2. DESARROLLO

2.1. La importancia del dato personal

El dato personal, junto con su noción de protección históricamente, data desde hace más de cien años cuando, en el año de 1859, John Stuart Mill afirmó que los aspectos concernientes al individuo consistían en el derecho a una absoluta independencia, puesto que sobre sí mismo, sobre su cuerpo y mente, el individuo era soberano (Mill, 2004, pág. 126 y ss).

El dato personal es aquel dato íntimo, es esa información que refleja la personalidad de un individuo y por tanto está ligado estrechamente a la intimidad de cada sujeto. Así cuando se habla del dato personal, se está entonces frente a una información de carácter muy íntima, que en las interacciones sociales comunes, solamente es puesto a disposición del prójimo, cuando por propia voluntad esta información por parte del titular se comparte y no trasciende más allá de un simple intercambio de datos propios de una adecuada relación social. Esto ha venido variando gracias a los avances tecnológicos, los cuales han empezado a trasgredir aquellos ámbitos que forman parte de la intimidad del ser humano.

Así, es importante para entender la importancia del Dato personal saber qué son y cuáles son. Como primera medida se debe tener claro que la categoría de dato personal no se refiere únicamente a datos íntimos, sino a cualquier tipo de dato que identifique o permita la identificación de una persona, y que esté en conocimiento o tratamiento de terceros. Entonces, dato personal es el nombre, DNI, una fotografía o una grabación de voz, la IP, un pin de teléfono, un avatar, la dirección de correo electrónico (*e-mail*), el CV, la orientación sexual, la condición de consumidor de un producto o de cliente de una empresa, la situación crediticia, un diagnóstico, el historial médico, los hábitos de consumo, la cuenta de banco, la afiliación a un club o red social, etcétera (Dozo, 2015). Los datos personales se clasifican en varias categorías, las cuales son: (Dozo, 2015)

- *Datos de identificación:* son aquellos entre los que están el nombre, el apellido, el teléfono, El PIN, el correo electrónico personal, la firma, la fecha de nacimiento, la edad, nacionalidad, el estado civil, el sexo, la imagen, la dirección de IP, etcétera.

- *Datos Laborales*: cargo, empleador, domicilio, correo electrónico institucional, teléfono del trabajo, nómina, sanciones, licencias, información de seguridad social, aportes, historial en la empresa
- *Datos Patrimoniales*: información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, información de consumos, situación de solvencia, etcétera.
- *Datos Académicos*: hoja de vida (c*urriculum vitae*), trayectoria educativa, títulos académicos, matrículas habilitantes, certificados, condición de alumno, calificaciones, etcétera.
- *Datos Ideológicos*: creencias religiosas, afiliación política, sindical, pertenencia a organizaciones de la sociedad civil, asociaciones religiosas, etcétera.
- *Datos de Salud*: estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, régimen de licencias, etcétera.
- *Características Personales y Físicas*: tipo de sangre, ADN, huella digital, altura, peso, discapacidades, color de piel, iris y cabellos, señales particulares, etcétera.
- *Vida y Hábitos sexuales*: origen étnico y racial, orientación sexual, análisis de perfiles, etcétera.

Esta clasificación de dato personal, que parece tan sencilla de definir y categorizar, comprende por lo tanto toda la información de la vida que cada persona tiene y que va paulatinamente entregando. Se entrega información cada vez que una persona se registra a una nueva red social o cuando envía un correo electrónico, con una acción tan sencilla como un mensaje de texto o un *me gusta* a cualquier publicación de alguna nueva promoción de la marca favorita. Las anteriores acciones son del diario vivir, por lo que se hace necesario que los titulares de datos personales tengan el debido cuidado de saber a quién se le entrega tanta información, saber para qué fines será utilizada y qué tipo de personas y entidades harán uso de ella.

2.2. El Dato personal en sus diferentes entornos

2.2.1. El Dato Personal en el ámbito económico

Hasta el momento se ha puesto en evidencia que reuniendo toda la información que una persona deposita en el registro de una página se tiene un panorama altamente definitorio de la misma a nivel comercial; es decir, se logra tener conocimiento de una persona acerca de todo lo que le gusta, lo que no le interesa, los sitios que frecuenta, su género, edad, etcétera, convirtiéndose, la persona, en un objetivo comercial claro. Sus datos personales empiezan a generar un interés a nivel industrial, con lo cual el poseedor de esta información puede llegar a comercializar de forma más exitosa, que si no poseyera esta información.

De esta forma es claro que en el ámbito económico el dato personal es una herramienta que siempre ha tenido una relevancia importante, debido a que éste establece un patrón de comportamiento y evidencia los gustos por parte del titular de los datos. Con únicamente saber el género y la edad del individuo se puede dirigir una oferta adecuada para lograr que dicha persona acceda a lo que la empresa quiera ofrecer disminuyendo el porcentaje para que la oferta fracase; y de la misma forma el dato personal está ligado a poder brindar una atención adecuada al cliente por parte de los responsables de la administración del dato. La información personal se convierte de cierta forma en una manera nueva de moneda por la que el interesado pagará su debido precio.

Es en razón de lo expuesto que el dato personal, siendo la nueva moneda digital, como lo define Angarita (2010), es demandado por una infinidad de empresas en el plano empresarial debido al gran valor comercial que éste puede llegar a alcanzar, y de la misma forma, el dato personal se convierte en parte fundamental del correcto funcionamiento de una empresa y de su constante crecimiento en la dinámica económica actual.

Con lo anterior se debe entender que si bien es cierto que el flujo de datos es una pieza clave en la actualidad para crear distintas actividades económicas, por esta misma razón es que se ha llegado a excesos, y por lo tanto se requiere de forma inmediata una regulación que garantice el buen manejo de los datos personales que las personas por voluntad propia dan a conocer a otras personas. En esta materia es preciso alcanzar el debido balance entre la protección de datos y el flujo de información de interés comercial.

2.2.2. El Dato Personal en el ámbito privado

Como se ha dejado claro, el dato personal es importante a nivel económico, debido a la posibilidad que tiene para facilitar transacciones, compras y ventas de todo tipo, además de llegar a ser una moneda de cambio en la red para generar beneficios a los oferentes de diversidad de servicios, asimismo, se debe entender que de la misma manera es importante en el ámbito de las relaciones personales por medio de la internet, como es el caso específico de las redes sociales, esto valiéndose de la enorme facilidad para compartir y generar contenido nuevo con los datos personales de los titulares de los derechos, aparecen nuevos escenarios y nuevas formas para una posible discriminación utilizando cualquiera de los datos que son considerados como personales.

El dato personal puede ser también considerado con fines sociales con igual o aún mayor transcendencia que en el ámbito económico, por parte del titular de la información para considerarse como una parte activa de una sociedad globalizada. Pues gracias a los cambios en las actividades personales por medio de interacciones constantes, dinámicas e inmediatas que en la red se ven diariamente, se permite que con la sola idea de que una persona no se pueda individualizar por la red, se entiende que socialmente está de cierta forma apartado de ella. De esta forma nace la necesidad por parte del titular de figurar en la alguna red social, ya sea para observar la dinámica, para compartir un momento representado en una foto, un video o un pensamiento o para interactuar con pensamientos, videos o fotos de otros usuarios que intervienen en ese devenir de información continuada prácticamente en tiempo real.

Cuando se encuentra que la dinámica social ha cambiado en elementos tan esenciales como lo son hablar, estudiar, comprar y vender, pagar cuentas, reservar una cita médica, un vuelo de negocios o compartir un álbum familiar con el mundo entero, y que todas estas actividades se pueden hacer bajo una misma plataforma sin tener que salir de la casa y prácticamente todo al mismo tiempo, se debe entender que las relaciones personales también han cambiado. Las personas ya no se relacionan únicamente con el vecino de toda la vida, con el mismo tendero de hace más de 10 años, y que no es sólo una persona la que oferta algún servicio, sino que son alrededor de tres mil millones de personas que pueden hacerlo, como lo revela un informe de 2014 de la Unión Internacional de Telecomunicaciones de las Naciones Unidas (UIT) (Unidas U. I., 2014). En el mismo sentido, de la misma forma como podemos tener nuestros inconvenientes con el portero del parqueadero por diferencias religiosas, lo podemos llegar a tener si expresamos una idea política por alguna plataforma mundial y generar inconvenientes de todo tipo, ya sean raciales, políticos, religiosos, etcétera.

Al estar frente a una dinámica social tan diferente y donde una simple idea o algo tan sencillo como la orientación sexual o cualquier otro tipo de información personal puede llegar a tantas personas y generar diferentes reacciones e interpretaciones por parte del receptor, estamos frente a potenciales situaciones de conflictos, ya sea porque el mismo usuario ha decidido evidenciar dicha información, ya sea por ignorancia de lo que esto puede acarrear o porque los responsables de la administración donde estos datos reposan no se han ocupado de ellos de manera adecuada para garantizar el apropiado límite de las personas que pueden acceder a ellos.

Frente a esta problemática encontramos que así mismo como la internet puede ser la plataforma que recorta distancias, que facilita el desarrollo económi-

co globalizado, que facilita enormemente algunas exigencias y responsabilidades del usuario que a ellas accede, también puede llegar a ser una fuente importante de situaciones donde, por motivos personales, se encuentre segregación, racismo, manipulación económica, amenazas, injurias, calumnias y discriminación de muchas formas como antes no era posible en las dinámicas sociales que exigían el encuentro físico de las personas para lograr una verdadera interacción.

Al tener este primer panorama de todas las problemáticas que pueden llegar a presentarse al depositar datos de carácter personal en cualquier base de datos que la recoja, ya sea con finalidades económicas o sociales, cabe introducir también que el otro factor por el cual esta información puede ser motivo de discriminación: el uso inadecuado de esta tecnología y por la calidad de los recolectores de esta información. Muchas veces los administradores no cuentan con los protocolos para el tratamiento de datos personales, haciéndolos poco confiables y llegando a amenazar los derechos de los titulares, debido a que los datos que contienen pueden ser datos erróneos, inexactos o falsos generando una fuente problemática más que debe tenerse en cuenta al momento de garantizar el adecuado tratamiento de estos datos y su calidad por parte de los ordenamientos internos de cada país (Angarita, 2005).

2.3. Regulación de la circulación de Datos Personales

2.3.1. Regulación nacional

Al considerar que el dato personal es indispensable para las personas, para las empresas sin importar su naturaleza, de la misma manera será primordial para el Estado, y es precisamente la facilidad de transferencia de estos datos, tanto en el ámbito público como en el privado y en el nacional como en el internacional ya sea entre personas naturales o jurídicas, la que establece un punto de partida para evidenciar la necesidad de contar con una adecuada regulación por parte del Estado.

Para empezar, en Colombia la primera vez que se legisló sobre la protección de datos personales fue en la Constitución del año de 1991, en su artículo 15:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución...

No sólo se debe entender que fue un avance importante, debido a que fue esta Constitución la que introdujo el derecho del *habeas data* y la protección del mismo como un derecho fundamental en el país, sino que además abrió la puerta a una serie de leyes que más adelante regularían con más especificidad y claridad todo lo correspondiente a este derecho.

Lo primero que se debe analizar es la ley por la cual se regula el *habeas data* en el país: Ley 1266 de 2008. El problema que trae es que se encarga sólo de regular información de tipo financiera, crediticia, comercial, de servicios y la proveniente de terceros países, dicho por la Corte Constitucional de Colombian por el concepto 2009029082- 002 del 4 de junio de 2009; con ello se denota la falta de protección en datos de tipo personales (sensibles) que revelan el origen étnico o racial, las convicciones religiosas o filosóficas, las opiniones políticas, la pertenencia a sindicatos y el tratamiento de los datos relativos a la salud o a la sexualidad.

En efecto una de las más graves situaciones que se observan en la Ley 1266/2008 (Congreso de la República, 2008) es en su artículo 5, literal F:

> A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la

> entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular...

... el cual al operador y no a la autoridad de control (que para el caso colombiano serían: la ley, la superintendencia de industria y comercio y la superintendencia financiera) le da la facultad de establecer si un país diferente a Colombia garantiza un nivel adecuado de protección; sin embargo, dejar a voluntad la protección de datos del usuario al operador (empresarios interesados en exportar datos personales) y no a las autoridades nacionales evidencia un problema en el trato de los datos personales de los colombianos en el exterior. Como consecuencia, la comunidad internacional no ve a América Latina como un territorio confiable en regulación y trato de datos personales (sensibles), países entre los que está España, en su artículo 35 del Real Decreto 1720/2007 (Real Decreto 1720 de 2007, 2007) establece:

> Artículo 35. Ejercicio del derecho de oposición. 1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento. Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho. 2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición 3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Como se puede observar, España trata un tema relacionado con el derecho de oposición. El derecho de oposición permite al titular del dato evitar el tratamiento de su información o solicitar el cese del mismo, algo que aún no se contempla en la legislación colombiana, y que sin lugar a dudas deja un vacío a la hora de ejercer una protección amplia y suficiente. Por tal razón, se debe entender que los vacíos legislativos acarrean problemas para quienes dan uso a las plataformas de datos.

Además, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, considera que Colombia no cumple los parámetros trazados por esta regulación que, aunque no es realmente universal (obligatorio cumplimiento para países no europeos), se ve con buenos ojos a quienes la cumplen y siguen dichos mandatos.

A causa de esto Colombia busca estar a la vanguardia en el tema de protección de datos, para ello se ha tramitado una serie de leyes que buscan regular todo lo correspondiente al *habeas data* tal y como lo mencionan la Ley 1581/2012 y el Decreto 1377/2013, donde se tratan principios y deberes aún más específicos en materia de *habeas data.* La sentencia C-748/2011 (Pretelt, 2011) proporciona las características que se deben tener para catalogar qué son datos personales en Colombia:

> i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.

Además, la sentencia C-1011/2008 (Sentencia de Constitucionalidad, 2008) ya había tratado la idea de unos principios básicos para el uso de datos personales por parte de operadores:

- Libertad
- Necesidad
- Veracidad
- Integridad
- Incorporación
- Finalidad
- Utilidad

- Circulación restringida
- Caducidad
- Individualidad
- Principio de diligencia y seguridad

Dichos principios son dados por la Sentencia para complementar lo consagrado en la Constitución en su artículo 15

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas…

Fue necesario que la Corte complementara esto, debido a que con el paso del tiempo el uso de plataformas de información masiva se ha vuelto algo cotidiano, por tal razón la regulación debe ser más específica, estos principios buscan eso, que el trato y cuidado de los datos personales se haga de manera responsable.

Además, los últimos años se han caracterizado por la acumulación de información, sea para abrir un correo electrónico, o una cuenta en una red social, se exige siempre cierta información personal para poder acceder a ello, el problema está en el uso desviado de la tecnología de tratamiento de datos personales que supone claros peligros para la libertad, para el derecho a no ser discriminado y así mismo para la misma dignidad humana (Domínguez, 2004). El indebido uso de las redes sociales y los portales masivos de internet es uno de los principales problemas a la hora de hablar de manejo indebido de los mismos.

Gracias a esto podemos encontrar que en la Ley 1581/2012 (Congreso de la República, 2012) se tiene una definición aún más específica de lo que se considera dato personal y sus conceptos derivados, en el artículo 3ro de dicha Ley se enuncia:

> a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales; b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento; c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento; e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos; f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento; g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

2.3.2. Principios

Además, no sólo se encuentran definiciones taxativas sino una serie de principios los cuales intentan suplir los vacíos legislativos y dar una interpretación más precisa a la hora de hablar de datos personales, en el artículo cuarto literales F, G y H en lo correspondiente al acceso, la circulación, la seguridad y la confidencialidad, dice:

> Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.
> Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
> Principio de confidencialidad: Todas las personas que

> intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

Igualmente, el Decreto 1377/2013 (Congreso de la República, 2013) el cual se encarga de regular parcialmente la ley mencionada con anterioridad (1581/2012), también busca llenar vacíos en materia internacional, dedica el capítulo V a tratar sobre este tema, artículos 24 y 25:

> Artículo 24: De la transferencia y transmisión internacional de datos personales. Para la transmisión y transferencia de datos personales, se aplicarán las siguientes reglas: 1. Las transferencias internacionales de datos personales deberán observar lo previsto en el artículo 26 de la Ley 1581 de 2012. (Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.)

> Artículo 25. Contrato de transmisión de datos personales. El contrato que suscriba el Responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el responsable. Mediante dicho contrato el encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables. Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado: 1. Dar Tratamiento, a nombre del Responsable, a los datos personales conforme a los principios que los tutelan. 2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales. 3. Guardar confidencialidad respecto del tratamiento de los datos personales.

Por consiguiente y entrando en materia, Colombia busca no sólo cubrir las demandas internacional con respecto a este tema, sino también cumplir con los retos que traen las nuevas plataformas de información, tales como las redes sociales, que se han convertido en los nuevos bancos de datos, donde se puede encontrar información de todo tipo (personal, sensible, familiar, religiosa, política, etcétera), lo cual lleva a pensar si realmente se está en capacidad de proteger a los usuarios de dichos portales masivos de internet.

2.4. Los datos personales y el contexto digital de las redes sociales

En el ámbito de las relaciones personales por la internet, como en el caso específico de las redes sociales, se genera una facilidad enorme para compartir y para generar contenido nuevo con los datos personales de los titulares de dicha información. Para los derechos que a las personas le asisten, se generan nuevos escenarios y nuevas formas incluso de generar discriminación.

Cuando se habla de redes sociales se debe tener en cuenta lo que son y para lo que son utilizadas. La red social es la estructura donde un grupo de personas mantienen algún vínculo, ya sean de amistad, sexuales, comerciales o de otra índole. Estas redes pueden tener múltiples usos, entre ellos los más usados son el compartir fotografías, videos, comentarios, ideas e información general, ya sea utilizando la opción de crear una comunidad con gustos específicos o a toda la colectividad virtual sin exclusividad alguna.

Las redes sociales comunican a través de, como lo define Nicholas Carr, «*micromensajes,* que son lanzados sin pausa alguna y nos ofrecen una capacidad de distracción que es casi adictiva» (Celis, 2011). Al tener una mirada como ésta, donde la necesidad de comunicación siempre ha sido de relevancia mayor, y a la que le añadimos el factor *adictivo,* tendremos una cantidad significativa de información sobre las redes sociales.

Cuando se tiene claro lo que es una red social habrá que preguntarse cuánta gente accede a ella y cuál es su crecimiento, datos que se encuentran disponibles en una investigación pertinente hecha por la *Online Business School* (OBS) (Purita, 2015) la cual arrojó que desde el año 2000 hasta el año 2014, la audiencia *online* ha crecido un 741%, y ha sido la irrupción de las redes sociales en 2009 lo que más ha contribuido a este crecimiento. Sólo en 2014 la audiencia *online* creció un 11 %, lo que implica que se tienen 300 millones de usuarios nuevos en internet hasta llegar a los 3.000 millones.

Como se preveía en el informe anterior, *Social Media 2014,* el Mundial de Futbol impulsó la venta de *Smartphones* y *Tablets* para seguir el evento desde cualquier lugar. «Lo importante es que quienes accedieron a las redes por primera vez a partir del Mundial de Futbol, se han incorporado al universo de usuarios *online* y esto ha hecho crecer la actividad en las redes sociales un 13% respecto de 2013», comenta Genoveva Purita.

Además la Corte Constitucional en sentencia T-260/12 (Sentencia de Tutela, 2012) hace hincapié y emite unos conceptos sobre lo que se entiende por derecho a la intimidad y datos personales en redes sociales:

> (i) el derecho de las personas a conocer –acceso- la información que sobre ellas está recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a un incluir nuevos datos con el fin de que se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos o archivo, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. Como se aprecia la protección del derecho fundamental del habeas data tiene como finalidad la protección de los datos en un mundo globalizado, en el que el acceso a la Sociedad de la Información y el conocimiento es cada vez mayor. Esta protección responde, además, a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el honor y la honra.

Entonces se puede ver cómo la corte reconoce el derecho que tienen los usuarios de manejar su información a voluntad, decidir qué incluir y qué omitir a la hora de usar una red social o ingresar sus datos en cualquier sistema masivo de información (Facebook, Twitter, correo electrónico, etcétera).

Además, la Corte aborda un tema importante: la seguridad de datos en infantes y adolescentes, los cuales pueden acceder a estas redes sociales sin ningún control, filtro o mecanismo que garantice la protección de la privacidad de menores de edad:

> En el caso en particular de los menores de edad los riesgos están íntimamente relacionados con lo siguiente: los niños y niñas tienen la posibilidad de acceder en las redes sociales a contenidos de carácter inapropiado para su edad; los menores tienen la posibilidad de iniciar contacto on-line, e incluso físicamente con usuarios malintencionados; existe proliferación de la información personal gráfica de los menores, ya sea publicada por ellos mismos o por terceros con desconocimiento de los riesgos a los cuales pueden ser expuestos. Las anteriores circunstancias pueden exponer a los niños y niñas, en caso de no acceder al mundo de las redes sociales con el debido acompañamiento de los padres a situaciones como abusos, discriminación, pornografía y otros que pueden incidir de manera negativa en su crecimiento y desarrollo armónico e integral. Tales riesgos pueden ser evitados si se tiene conocimiento acerca del funcionamiento y las políticas de privacidad de los diferentes sitios en línea, en especial de las redes sociales. De allí que en el caso específico de los menores de edad, en especial niños y niñas, el acceso a las redes sociales debe darse con el acompañamiento de los padre o personales responsables de su cuidado, a fin de que éstos sean conscientes de que si bien en mundo de la información y la tecnología implica un sinnúmero de beneficios para su desarrollo, al mismo tiempo genera una serie de riesgos que se pueden evitar con un correcto manejo de la información y con una adecuada interacción con los demás miembros de la red.

Después de analizar estos conceptos emitidos por la

corte, se puede dar por sentado que, aunque no se desconoce la importancia de la protección de los datos personales (sensibles), en usuarios de redes sociales y portales de internet y se reconoce lo fácil que es su acceso y lo vulnerable que puede llegar a ser la imprudencia y el mal manejo de datos por parte de las personas (tanto mayores de edad, como niños y adolescentes), es más un problema de culturizar y concienciar a la población que potencialmente le da uso a dichas redes para que puedan no sólo entender que proveer información de manera deliberada y sin ningún tipo de control o privacidad, acarrea riesgos que a la larga pueden llevar a robo y manejo indebido por parte de personas o empresas encargadas de obtener información para terceros.

2.5. Los datos personales a nivel internacional

Todo lo anterior deja ver por qué es importante para un país en un nivel interno tener la confianza de sus usuarios para depositar sus datos en los portales de almacenamiento. Ahora bien, se debe tener claro por qué lo es también a nivel internacional y qué consecuencias trae cuando la regulación interna no cumple con los parámetros mínimos de seguridad ante las miradas de los demás países, más específicamente la Unión Europea que desde la década de 1970 ha regulado estas actividades, tema en el que la Organización de las Naciones Unidas (ONU) ya se ha pronunciado en su Resolución 45/95 del 14 de diciembre de 1990 (Unidas A. G., 1990), en la que adoptó los «principios rectores para la reglamentación de los ficheros computadorizados de datos personales». Entre ellos, la ONU estableció el principio de *Flujo de datos a través de las fronteras*, según el cual: «cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos».

Esta resolución evidencia que no es un tema reciente a nivel internacional, que lleva ya 20 años esta resolución dictaminando que debe existir un nivel de seguridad equiparable entre el que exporta los datos con el país que los va a recibir. Bajo esta mirada y con intención de intercambiar datos personales con países europeos se analizarán los requisitos que la Unión Europea exige, y si Colombia es ante la mirada de estas regulaciones un país seguro para la transferencia de datos. De esta forma es importante tener claro por qué para un país es trascendental contar con este nivel, así como lo describe Remolina (Angarita, 2010) en tres puntos. El primer punto, el autor caracteriza al modelo europeo tradicional como un modelo garantista, riguroso y efectivo en esa materia, lo que genera un aumento en el grado de protección jurídica de la información de la ciudadanía. El segundo punto que resalta es el de un escenario nacional más competitivo a nivel económico, debido a que éste se genera cuando un país es un lugar seguro en el que pueden realizarse negocios que implican transferencia de información personal, desde estos países hacia el territorio nacional, y menciona los *call centers* internacionales. El tercer y último punto que el autor expone es el de la efectiva protección de datos personales, ya que es considerada como un elemento consustancial de las sociedades democráticas.

3. CONCLUSIONES

Al entender que los datos personales y su protección han sido temas que desde hace más de cien años se han tenido en cuenta, y que debido al gran y recurrente cambio producto de los avances en la tecnología, que da una incidencia mundial a la forma de compartir estos datos, marcando la pauta de cómo y cuándo se comunican nuevos contenidos desde hace ya más de una década, se demuestra que es una tendencia que no solamente está sólidamente establecida, sino que seguirá en una constante expansión, dando mayor acceso y mayor facilidad a los usuarios para compartir lo que desee.

De tal modo que, entendiendo dicha tendencia a nivel mundial, es necesario que la legislación aborde el tema como una prioridad, y sabiendo que la legislación nacional colombiana es precaria en comparación con los modelos, en los que están el español y en

general el europeo, en materia de protección de datos personales y datos personales sensibles, si hablamos de redes sociales y portales de información masiva en internet, aun así en la última década el Colombia se ha puesto a la vanguardia no sólo profiriendo leyes estatutarias, sino reconociendo en el ámbito jurisprudencial la importancia y el cuidado que se debe tener en el tema. Aunque aún falta mucho por hacer para darle el manejo debido que necesita, pues es una cuestión de normas y coacción por parte del estado a su vez que es una cuestión de conocimiento por parte del usuario, el cual muchas veces ignora los riesgos de un uso deliberado y de la publicación de datos sin el debido cuidado (fotos de infantes, familiares, etcétera). Como todo, en una sociedad, la cultura y el debido uso de las herramientas dadas por ella son fundamentales para el funcionamiento correcto de la misma.

REFERENCIAS

ANGARITA, N. R. (2005). *Data Protection: Riesgos Y Desarrollos (Enfasis en el caso Colombiano)*. Revista Chilena de Derecho Informático, 111-134. Obtenido de El Semanario Republicano.

ANGARITA, N. R. (2010). *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estandar europeo?* Revista Colombiana de Derecho Internacional, 489-524.

CELIS, B. (29 de Enero de 2011). *Elpais.com*. Obtenido de Elpais.com: http://elpais.com/diario/2011/01/29/babelia/1296263535_850215.html

CONGRESO DE LA REPÚBLICA (31 de Diciembre de 2008). *Ley estatutaria 1266 de 2008*. Ley Estatutaria. Bogotá, Colombia.

CONGRESO DE LA REPÚBLICA (17 de Octubre de 2012). *Ley 1581 de 2012*. Bogotá, Colombia.

CONGRESO DE LA REPÚBLICA (27 de Junio de 2013). *Decreto 1377*. Decreto. Bogotá, Colombia.

CONSTITUCIÓN POLÍTICA (1991). Bogotá, Colombia.

DOZO, P. M. (2 de Noviembre de 2015). *Habeasdat S.A*. Obtenido de HabeasdatS.A : http://www.habeasdat.com/faq.html

DOMÍNGUEZ, A. G. (2004). *Tratamiento de datos personales y derechos fundamentales*. Madrid.

MILL, J. S. (2004). *Sobre la Libertad*. Madrid: Alianza Editorial.

PRETELT, J. I. (2011). *Sentencia de la Corte Constitucional C-748/11*. Bogotá.

PURITA, G. (26 de Enero de 2015). *Online Business School*. Obtenido de Online Business School: http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/

REAL DECRETO 1720 DE 2007 (21 de Diciembre de 2007). *Real Decreto 1720 de 2007*. Madrid, España.

SENTENCIA DE CONSTITUCIONALIDAD C-1011/08 (Corte Constitucional 16 de Octubre de 2008).

SENTENCIA DE TUTELA, T-260 (Corte Constitucional 2012).

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (2014). (S. d. Comercio, Ed.) Retrieved 2015 23-10 from Superintendencia de Industria y Comercio: http://www.sic.gov.co/drupal/site/default/files/informe_consolidado_sanciones_1_20_2014_VERSION_SIC.pdf

UNIDAS, A.G. (14 de Diciembre de 1990). Resolución 45/95.

UMIDAS, U. I. (5 de Mayo de 2014). ITU. Obtenido de ITU : https://www.itu.int/net/pressoffice/press_releases/2014/23-es.aspx