

PROTECCIÓN DE DATOS PERSONALES EN INTERNET Y SU REGULACIÓN
EN EL ORDENAMIENTO JURÍDICO COLOMBIANO

JULIANA VÉLEZ OBANDO

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS
FACULTAD DE DERECHO
MEDELLÍN

2020

PROTECCIÓN DE DATOS PERSONALES EN INTERNET Y SU REGULACIÓN
EN EL ORDENAMIENTO JURÍDICO COLOMBIANO

JULIANA VÉLEZ OBANDO

Trabajo de grado para optar al título de Abogada

Asesora:

KATHERINE GÓMEZ GARCÍA

Abogada

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS

FACULTAD DE DERECHO

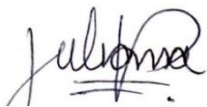
MEDELLÍN

2020

Medellín, 27 de noviembre de 2020

Juliana Vélez Obando,

“Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en ésta o en cualquiera otra universidad”. Art. 92, parágrafo, Régimen Estudiantil de Formación Avanzada.

A handwritten signature in black ink, appearing to read 'Juliana', with a horizontal line underneath the name.

Firma del autor

CONTENIDO

INTRODUCCIÓN	7
1. LOS DATOS PERSONALES.....	12
2. RIESGOS DE LOS DATOS PERSONALES EN LA WEB.....	14
3. MARCO LEGAL QUE REGULA LOS DATOS PERSONALES EN COLOMBIA	17
4. REGULACIÓN DE LOS DATOS PERSONALES EN INTERNET	19
CONCLUSIONES	22
BIBLIOGRAFÍA.....	23

RESUMEN

La evolución de las Tecnologías de Información y Comunicación, la Internet y la Inteligencia Artificial, ha favorecido el procesamiento de millones de datos personales producidos en todo el mundo, generando múltiples efectos colaterales. Con todo, hoy es claro que la información de las personas tiene un valor incalculable en el sector público y el privado.

De ahí que surja el interés por examinar en este texto, si el ordenamiento jurídico colombiano actualmente responde a los desafíos cada vez más complejos que implica el tratamiento de los datos personales en la web.

Para ello se proponen como objetivos, primero, establecer la incidencia que tiene el tratamiento de los datos personales en relación con los derechos fundamentales de *Habeas Data*, intimidad y libertad; segundo, analizar si la Ley 1581 de 2012 y el Decreto 1377 de 2013, regulan de manera adecuada el tratamiento de datos personales que se obtiene en la web; tercero, determinar si la regulación colombiana vigente en materia de protección de datos personales es adecuada para afrontar los desafíos que plantea la era digital.

Finalmente, se utilizó el método hermenéutico, y se llegó a la conclusión de que es urgente que los Estados, y más concretamente, el colombiano, fije estrategias para crear una regulación idónea frente a los fenómenos que se presentan en la virtualidad, así mismo, que le dé mayor efectividad a la Ley 1581 de 2012 y al Decreto 1377 de 2013.

Palabras clave: datos personales en internet, rastreo web, protección de datos, *Habeas Data*, privacidad.

ABSTRACT

The evolution of Information and Communication Technologies, the Internet and the Artificial Intelligence, has favored the processing of millions of personal data produced around the world, generating multiple collateral effects. That way, today it is clear that people's information is invaluable in the public and private sectors.

Hence, the interest arises to examine in this text, if the Colombian legal system currently responds to the increasingly complex challenges involved in the processing of personal data on the web.

For this, the proposed objectives are, first, to establish the impact of the processing of personal data in relation to the fundamental rights of *Habeas Data*, privacy and freedom; second, analyze if Law 1581 of 2012 and Decree 1377 of 2013 regulate the processing of personal data obtained on the web in an appropriate way; third, to determine if the current Colombian regulation on the protection of personal data is adequate to face the challenges posed by the digital age.

Finally, the hermeneutical method was used, and it was concluded that it is urgent that the States, and more specifically, the Colombian, establish strategies to create an ideal regulation against the phenomena that occur in virtuality, likewise, to give greater effectiveness to Law 1581 of 2012 and Decree 1377 of 2013.

Keywords: personal data on the internet, web tracking, data protection, *Habeas Data*, privacy.

INTRODUCCIÓN

Desde finales del Siglo XX, el mundo ha venido enfrentando una gran transformación en las estructuras económicas, políticas y sociales, animada principalmente, por los desarrollos tecnológicos.

Desde esa perspectiva, la noción de riqueza que antes se medía por los factores productivos tradicionales: tierra, capital y trabajo, hoy se mide, en gran medida, por la cantidad de información que se tiene sobre las personas, lo que la convierte en un activo fundamental en el desarrollo económico de la sociedad; de ahí que se afirme que “Es un hecho irresistible que la información se genera, se trata y circula, por las venas de la sociedad, a ritmos vertiginosos, al impulso de las TIC.” (Sánchez, 2014, p. 55)

El desarrollo acelerado y conjunto de las Tecnologías de Información y Comunicación (TIC), la Internet y la Inteligencia Artificial (IA), ha posibilitado el procesamiento de millones de datos personales generados en todo el mundo a una velocidad inimaginable. Como consecuencia, estos desarrollos han venido acompañados de riesgos, problemas y críticas, que cada vez tocan más el ámbito de los Derechos Humanos y cuestionan la ética y la moral de la sociedad actual; en palabras de Bauman, Z. & Lyon, D. (2013) “Las nuevas tecnologías abren una brecha entre los seres humanos y sus responsabilidades morales en relación con los demás (...)” (p. 102)

Bajo el argumento de posibilitar la interacción entre personas de cualquier parte del mundo o hacerles la vida más fácil, esa evolución informática y tecnológica permitió la creación de redes sociales, plataformas de interacción, y del concepto de *internet de las cosas*¹, utilizado para referirse a todos aquellos dispositivos que gozan de conectividad a internet y que facilitan la vida diaria al permitir personalizar sus

¹ Concepto utilizado por primera vez por Kevin Ashton en 1999. Para una ampliación del concepto, véase Medina (2017).

características según las necesidades de su dueño, pero para ello, es necesario que la persona introduzca la mayor cantidad de datos sobre ella los cuales van a la red inmediatamente.

Entonces, lo que comenzó siendo la solución a muchas necesidades, también fue la oportunidad para otros sectores de la sociedad, que aprovecharon la ocasión para recoger, analizar y procesar toda la información que se iba dejando en la red, y ello con múltiples finalidades: comerciales, laborales, delincuenciales, de seguridad, pero todas resumidas en una palabra, *vigilancia*.

En ese orden de ideas, con la autorización de los titulares de los datos personales o sin ella, y la mayoría de las veces, sin que ellos tengan conocimiento o sean conscientes del proceso que se sigue, Téllez-Aguilera (2001) explica que:

(...) a través de las «cookies remotas» o programas rastreadores o *sniffers*, por ejemplo, se posibilita el funcionamiento de las denominadas «redes de seguimiento» a través de las cuales es posible seguir al usuario a medida que navega por determinados «sitios», “vigilando sus acciones, acumulando información personal, controlando cuales bienes o servicios adquiere, etc.”
(citado en Sánchez, 2014)

A partir de lo anterior, es preciso reconocer que la recolección de información personal en la web es una realidad a nivel mundial, que incide en el derecho de protección de datos personales, de intimidad, de libertad, de olvido y de seguridad, solo por mencionar algunos.

En ese sentido, el presente trabajo surge con el interés de analizar la forma en que el Estado colombiano está enfrentando este fenómeno que llegó con la era digital, para lo cual se plantea como enunciado problematizador, si el ordenamiento jurídico colombiano actualmente responde a los desafíos cada vez más complejos que implica el tratamiento de los datos personales en la web.

De ahí, surgen como objetivos, primero, establecer la incidencia que tiene el tratamiento de los datos personales en relación con los derechos fundamentales de

Habeas Data, intimidad y libertad; segundo, analizar si la Ley 1581 de 2012 y el Decreto 1377 de 2013, regulan de manera adecuada el tratamiento de datos personales que se obtiene en la web; tercero, determinar si la regulación colombiana vigente en materia de protección de datos personales es adecuada para afrontar los desafíos que plantea la era digital.

Para lograr esos objetivos, en las próximas páginas se propone desarrollar el concepto de datos personales, su importancia en la era digital y los riesgos e implicaciones que se generan respecto de los derechos de *Habeas Data*, intimidad, y libertad. Con esto claro, se analizará, de manera general, el marco legal que regula el tratamiento de datos personales en Colombia; se hará una reflexión sobre los desafíos que debe enfrentar el ordenamiento jurídico colombiano en materia de información personal en internet, y se finalizará con unas conclusiones.

El método que se utilizará para este estudio es el hermenéutico, respecto del cual se generará un proceso de indagación e interpretación de los textos revisados; se seleccionarán y clasificarán las categorías centrales relativas al problema objeto de análisis; por último, se realizará un ejercicio de contrastación y análisis científico para proceder a tomar posición fundamentada.

Así mismo, se realizará una revisión en las bases de datos especializadas Dialnet, Scielo y Ebsco, las cuales permitirán identificar y seleccionar artículos en revistas de alto impacto con el fin de detectar el estado de la investigación en relación con las categorías centrales que se abordarán en este trabajo.

Conforme a lo anterior, como primer referente, se tiene a González-Guerrero (2019), para tener una noción acerca del monitoreo de las actividades de las personas en la web. En la primera parte de su texto, explica el rastreo y la recolección de información proveniente de millones de fuentes con la que se pretende perfilar a las personas, y los riesgos que implican esas prácticas. En un segundo momento, hace una revisión de las regulaciones que buscan establecer un control de esas

tecnologías de rastreo, a partir de la evaluación de las políticas de privacidad de las diez páginas de noticias más visitadas desde Colombia.

Dentro de su análisis pudo establecer “un bajo cumplimiento de los estándares mínimos de información y de libertad necesarios para que las personas controlen el uso de los datos recolectados por medio de tecnologías de rastreo.” (González-Guerrero, 2019, p. 209). Además, entre sus conclusiones señala que la regulación colombiana no plantea soluciones efectivas que enfrenten el riesgo que implica la recolección automatizada de datos personales.

En segundo lugar, se revisó el trabajo de Martínez (2019), para estudiar la participación que tiene la Inteligencia Artificial en el tratamiento de datos personales y las consecuencias que ello genera. Con fundamento en esto, la autora hace un análisis de las regulaciones sobre datos personales que existen en el mundo incluida Colombia. Luego, a partir de algunos casos particulares, explica los riesgos que resultan del mal uso de la información personal en las nuevas tecnologías.

En su trabajo llega a la conclusión sobre la importancia de que los titulares de la información personal reconozcan los derechos que tienen sobre la misma. Habla de la necesidad de que los gobiernos adapten sus regulaciones sobre la materia, a los avances de la era digital, debido a que “(...) uno de los problemas actuales es que las normas de protección de estos datos no avanzan al mismo ritmo de las nuevas tecnologías, provocando que las regulaciones sean precarias en cuanto a la realidad actual.” (Martínez, 2019, p. 20). Finalmente, hace énfasis en la responsabilidad que tienen los encargados del tratamiento de datos personales, pues son ellos quienes ejercen un uso masivo de los mismos.

Ahora bien, para profundizar en la legislación colombiana, se tuvo en cuenta el trabajo de investigación de Remolina-Angarita (2010), en el que hace un estudio de la regulación nacional en materia de protección de datos personales a la luz de los parámetros de la Unión Europea, para determinar si Colombia puede considerarse como un país que garantiza una adecuada protección de los mismos. Entre sus

conclusiones se resalta que Colombia no cuenta con un marco legal que garantice esa protección. Además, indica que la Ley 1266 de 2008 se cataloga como una norma sectorial, que no permite una regulación general sobre datos personales por no tener en cuenta algunos principios básicos sobre la materia.

En relación con las consecuencias que han generado los avances acelerados de la tecnología y la incidencia cada vez mayor en el ámbito de los derechos humanos, se consultó el trabajo de Garriga-Domínguez (2016), quien hace una reflexión alrededor de la información personal en la era del *big data*, y los nuevos riesgos que han surgido para los derechos de las personas, todo a la luz del marco legal europeo.

Como complemento de todo lo anterior, se tuvieron en cuenta algunos planteamientos que hacen Bauman & Lyon (2013), en la conversación que tienen en su libro *Vigilancia Líquida*. El tema central radica en la fuerza que ha tomado la vigilancia en el mundo moderno y, con ello, el acelerado aumento de la cantidad de datos procesados. La expansión de la vigilancia en todo el mundo, los lleva a cuestionarse sobre las implicaciones éticas y políticas que resultan de dicha práctica.

Finalmente, los anteriores fundamentos teóricos llevaron a la siguiente pregunta problematizadora que orientó este estudio: ¿El ordenamiento jurídico colombiano actualmente responde a los desafíos cada vez más complejos que implica el tratamiento de los datos personales en la web?

1. LOS DATOS PERSONALES

En la era digital, el desarrollo de las tecnologías de la información y la comunicación ha sido de increíble rapidez; con ello, las posibilidades de comunicación han aumentado y generado formas de acceder a información en línea que antes eran inconcebibles. Partiendo de esos avances, los datos se han convertido en un activo básico para las entidades privadas y los Estados, especialmente, aquellos relativos a las personas.

Para abordar los planteamientos que siguen, es fundamental entender el concepto de datos personales. Así, para efectos de este trabajo, se acogerá la definición que trae el literal b) del artículo 3° de la Ley 1581 de 2012, que define dicho concepto como “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”. En otras palabras, se trata de información relativa a una persona que permite su identificación, esa persona se conoce como titular y, cabe resaltar que, este nunca pierde la propiedad sobre esa información independientemente de quien la posea. Es importante agregar que los datos personales son tutelados por el derecho de *Habeas Data*.

En Colombia se atiende a la clasificación del dato personal en público, semiprivado, privado y sensible. El primero hace referencia a información que puede estar en registros y documentos públicos que no tienen reserva, es determinada por la Constitución Política y la Ley y, de manera general, es aquella que no se clasifica en las otras categorías. El segundo obedece a información que no tiene naturaleza íntima, reservada o pública, pero su contenido puede ser de interés para su titular o un sector específico. El tercero es un dato íntimo o reservado que solo es relevante para su titular. Finalmente, el dato sensible es el que afecta la intimidad de su titular y puede generar discriminación. (Superintendencia de Industria y Comercio, s.f.)

Como se mencionó anteriormente, la importancia de los datos personales y la magnitud de su procesamiento se ha venido transformado en la modernidad. Solo por mencionar algunos cambios: la variedad de información personal que se

recopila ha aumentado; las interacciones entre las personas que involucran ese tipo de información, cada vez son más complejas; las amenazas a la privacidad tienen un mayor alcance; además, los datos ahora están en constante flujo y disponibilidad global gracias a las plataformas digitales, lo que ha llevado a reevaluar los conceptos de tiempo y espacio.

Lo último encuentra relación con el término *big data*, que alude a la cantidad de datos disponibles que pueden ser utilizados con diversos fines. Dicha información es procesada por tecnologías con inteligencia artificial que emplean algoritmos que permiten hacer predicciones, perfilar personas, extraer información oculta, tomar decisiones, etc. En definitiva, los datos son la materia prima básica para realizar esos procesos que cada vez son más comunes e imprescindibles en la planeación de marketing y publicidad de las empresas, en la selección de sus empleados, en las diferentes labores que cumplen las entidades estatales, en el monitoreo de personas que padecen una afección, en la clasificación social, entre otros.

Ahora bien, entre los recursos que se utilizan para recopilar información personal en la web, se destaca (I) la navegación en internet, la cual deja un rastro que genera constantemente datos que revelan toda la actividad o el recorrido que hacen las personas allí; (II) el uso del internet de las cosas, esto es, dispositivos revestidos de inteligencia artificial; (III) la información disponible en la red, proveniente de datos públicos y/o proporcionada voluntariamente por el usuario. “El 70% del universo digital es generado por nosotros mismos a través de nuestra interacción con los diferentes servicios de la red (e-mail, redes sociales, buscadores, Smartphone, etc.)” (Craig & Ludloff, 2011, citado en Garriga-Domínguez, 2016).

Cabe agregar que esas operaciones se llevan a cabo bajo el velo de beneficios que se muestran muy atractivos para los usuarios; piénsese, por ejemplo, en un dispositivo de geolocalización que le ayuda al usuario a llegar a su destino; en un refrigerador que crea la lista de compras y la envía al supermercado; una plataforma que conecta personas de cualquier parte del mundo; o una aplicación móvil que le permita al usuario determinar su estado de salud.

Para tener una comprensión más amplia de esto, con el propósito de aprovechar todos los beneficios de esas tecnologías, las personas inconscientemente revelan datos que, al combinarse, permiten identificar su ubicación, el sector en el que laboran, su composición familiar, capacidad financiera, preferencias políticas, religión y los más íntimos detalles de su vida personal. Pero ahí no termina, porque la información que se comparte sobre terceros, también pasa a colaborar con la identificación y creación de perfiles sobre ellos.

2. RIESGOS DE LOS DATOS PERSONALES EN LA WEB

“Sin un objetivo fijo, pero presionada por las exigencias de la «seguridad» y pasada por el prisma de la insistente publicidad de las empresas de tecnología, la vigilancia se esparce por doquier.” (Bauman y Lyon, 2013, p. 11)

La vigilancia sobre los movimientos de una persona genera una cantidad de datos que, combinados con los que ella previamente ha entregado de manera voluntaria, permiten la creación de un perfil que es utilizado con diversos propósitos: de seguridad, comerciales y de publicidad, para infundir desinformación, fomentar ideologías extremistas, manipular elecciones políticas, robar la identidad de las personas, complementar la hoja de vida de los aspirantes a un puesto de trabajo, atacar la integridad física y moral, hacer una clasificación social basada en la exclusión, la desigualdad y la segregación.

Entre otros factores que agravan la situación hay que mencionar que, primero, la disponibilidad de los datos personales en la red facilita su acceso desde cualquier parte del mundo, lo que afecta la jurisdicción de los Estados, ya que el ámbito de aplicación de sus ordenamientos jurídicos queda corto para enfrentar los flujos transfronterizos constantes de información.

Segundo, las autorizaciones de tratamiento de datos personales que normalmente utilizan las entidades privadas y públicas, no permiten realmente que el titular de la información emita una manifestación de voluntad inequívoca, libre, específica e

informada², ya que hoy gran cantidad de servicios están condicionados a dicha autorización, dejando sin muchas opciones a las personas. Otras veces el lenguaje de esas autorizaciones se torna complejo de entender para muchos; contienen cláusulas donde se autoriza compartir esos datos personales que se están recogiendo con terceros diferentes al responsable o encargado³ del tratamiento de esa información; y, de manera general, son documentos que intrínsecamente llevan a la aceptación del titular de la información, porque no dan opciones para negarse, a veces con el simple uso del servicio, suponen dicha aceptación.

Todo lo anterior ha llevado a que diversos sectores de la sociedad empiecen a reflexionar sobre las implicaciones que tiene el tratamiento de datos personales en la web respecto de los derechos fundamentales de *Habeas Data*, de intimidad y de libertad, que se explicaran a continuación.

El *Habeas Data* está consagrado en el artículo 15 de la Constitución Política de Colombia, y dice que es la facultad que tienen las personas de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas.

Ese mismo artículo explica que “todas las personas tienen derecho a su intimidad personal y familiar (...); lo que se puede complementar con el artículo 12 de la Declaración Universal de Derechos Humanos, cuando dice que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia (...)”

² Estas son características del consentimiento en la autorización del tratamiento de los datos personales, elaboradas por el Article 29 Working Party (2018).

³ La Ley 1581 de 2012 en su artículo 3° literal d) explica que encargado es la “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”. Por su parte, el mismo artículo en su literal e) indica que responsable es la “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”.

Por otro lado, el inciso primero del artículo 13 de la Constitución Política de Colombia, señala que

Todas las personas nacen libres e iguales ante la ley, recibirán la misma protección y trato de las autoridades y gozarán de los mismos derechos, libertades y oportunidades sin ninguna discriminación por razones de sexo, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica.

Con esto claro, a simple vista se puede afirmar que esa continua vigilancia, ya no solo de los entes gubernamentales sino de otros interesados, a través de plataformas digitales, del internet de las cosas, del reconocimiento biométrico, etc., irrumpe en la privacidad y la intimidad de las personas; dificulta y, muchas veces, imposibilita el ejercicio del derecho de *Habeas Data*, ya que con cada actividad que se registra en la web o con cada autorización consciente que dan los usuarios, pierden poco a poco el control sobre sus datos personales; y coarta la libertad de las personas, porque una vez procesada la información y creado un perfil, pueden influenciar sus decisiones, ideologías, generar discriminación, monitorear los comportamientos cuando son diferentes a los prototipos creados para una sociedad de consumo. La vigilancia que hoy se practica con el propósito de brindar seguridad, ha tomado un enfoque "(...) no contra peligros concretos, sino contra unos riesgos amorfos y misteriosos." (Bauman & Lyon, 2013, p. 107)

Todas esas operaciones contribuyen a que la vida de las personas cada vez sea más transparente y menos privada frente a los entes que las vigilan, pero además, que las actividades de estos sean más difíciles de descifrar, lo mismo cuando se trata de conocer con precisión, quién conserva y utiliza dicha información. Con todo, progresivamente y sin que sea perceptible para la mayoría, las personas van siendo despojadas de sus derechos.

3. MARCO LEGAL QUE REGULA LOS DATOS PERSONALES EN COLOMBIA

El ordenamiento jurídico colombiano ha desarrollado el régimen de protección de datos personales a partir del artículo 15 de la Constitución Política. Con ese fundamento se crearon (I) la Ley 1266 de 2008 que regula el derecho de *Habeas Data* en el escenario financiero, crediticio, comercial, de servicios y de terceros países; (II) la Ley 1581 de 2012 que establece disposiciones generales sobre el derecho a la protección de los datos personales; (III) el Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012 en aspectos relativos a las políticas para el tratamiento de datos personales; la autorización del titular para realizar dicho tratamiento; el ejercicio de los derechos que tiene el titular; la transferencia de datos personales; y el principio de responsabilidad demostrada.

Respecto de la Ley 1266 de 2008, la Corte Constitucional expresó en sentencia C-1011 de 2008, que aquella aplica únicamente al procesamiento de datos personales de contenido crediticio y financiero, por lo que se trata de una disposición de carácter sectorial, esto es, una regulación que procede solo frente a quienes cumplan unas características especiales en materia financiera y comercial.

En ese orden de ideas, es claro que hasta la entrada en vigencia de la Ley 1581 de 2012 y el Decreto 1377 de 2013, el ordenamiento jurídico colombiano carecía de una regulación que abordara situaciones diferentes a las financieras relativas al tratamiento de datos personales, razón por la cual, hasta ese momento, Colombia no había sido considerada por la Comisión Europea como un Estado con un nivel adecuado de protección; reconocimiento que es de gran importancia para los países por tres motivos: primero, aumenta la protección de la información ciudadana mediante normas jurídicas; segundo, genera confianza en la realización de negocios que requieren transferencia de información personal desde Europa; tercero, la adecuada protección de datos personales es elemental dentro de las sociedades democráticas (Rodotà, 2003, citado en Remolina-Angarita, 2010).

Hay que agregar que el Grupo de Trabajo del Artículo 29, estableció que un nivel adecuado de protección depende de la interrelación que existe entre los derechos que tiene el titular de los datos y las obligaciones en cabeza de quien procesa o controla dicha información; de la existencia de mecanismos judiciales y no judiciales que garanticen la efectividad de las normas, sancionen su incumplimiento y contemplen un derecho de reparación para quien se haya visto afectado con el indebido tratamiento de su información; y de la existencia de una autoridad garante de la protección de datos que se encargue de dar aplicación a lo anterior y de recibir las quejas de los ciudadanos (Remolina-Angarita, 2010).

Con ese propósito surge la Ley 1581 de 2012 y el Decreto 1377 de 2013 que contienen una regulación más amplia, aplicable a todos los sectores que por su actividad deban manejar información personal de los ciudadanos.

Por otra parte, atendiendo a la regulación internacional, la Organización para la Cooperación y el Desarrollo Económicos (2013), propuso una serie de principios básicos en materia de tratamiento de datos personales, ellos son:

- Limitación de la recolección.
- Calidad de datos.
- Especificación de propósito.
- Limitación de uso.
- Salvaguardias de seguridad.
- Apertura.
- Participación individual.
- Responsabilidad.

Así pues, al analizar dichos principios en relación con la normatividad interna, se encuentra que esta los acoge en su regulación; un ejemplo de ello, es el desarrollo que se le ha dado en Colombia al principio de responsabilidad.

Es así como la Superintendencia de Industria y Comercio como autoridad de protección de datos según el artículo 19 de la Ley 1581 de 2012, respondiendo a la

solicitud de la industria de generar claridad sobre la construcción de un Programa Integral de Gestión de Datos Personales, desarrolló la Guía para la Implementación del Principio de Responsabilidad Demostrada (*Accountability*), principio “(...) según el cual una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos.” (Superintendencia de Industria y Comercio, 2015, p. 5)

4. REGULACIÓN DE LOS DATOS PERSONALES EN INTERNET

Habiendo desarrollado el concepto de datos personales, su presencia en internet y los riesgos que ello conlleva, cabe hacer una última reflexión acerca de la protección que ofrece el ordenamiento jurídico colombiano a la información personal que diariamente circula en la web, situación que hoy es una realidad y requiere con urgencia reglamentación especial.

Como se explicó antes, el mundo digital ha evolucionado para permitir a las personas realizar una gran cantidad de actividades sin tener que desplazarse a diferentes lugares, sin embargo, para que la experiencia sea cada vez más satisfactoria, es necesario que el usuario deposite sus datos personales en la web, lo cual tiene múltiples consecuencias. Por este motivo, los Estados y organismos internacionales se han visto obligados a incluir en sus agendas esta nueva realidad.

Siguiendo las directrices sobre protección de datos personales desarrolladas por el Grupo de Trabajo del Artículo 29 (2018), en materia de consentimiento como requisito fundamental en el procesamiento de datos personales, se destacan situaciones como el hecho de que las personas, al navegar en internet, están recibiendo todo el tiempo solicitudes de consentimiento para hacer uso del servicio; esto evidentemente se ha convertido en una labor agotadora generando como resultado que los mecanismos dispuestos para obtener ese consentimiento pierdan efectividad y con ello disminuya el nivel de protección.

Otra situación preocupante es la relativa a las formas que utilizan los encargados y responsables de los datos personales para obtener el consentimiento del usuario. Al ingresar a un sitio web, es común encontrar una autorización que advierte que un solo clic o deslizamiento se entiende como aceptación del tratamiento de los datos personales; otras veces lo que sucede es que, con un clic en el botón *acepto*, se generaliza la autorización para manejar todo tipo de información personal que provenga de esa persona.

Frente a situaciones como las antes mencionadas, el Grupo de Trabajo del Artículo 29 (2018), ha indicado que es necesario que el usuario tenga la posibilidad de manifestar su voluntad sobre todas y cada una de las operaciones que realiza el responsable o encargado del tratamiento de datos personales, a través de actos inequívocos que reflejen su verdadero deseo.

Igualmente, se debe permitir al titular de la información el retiro de su consentimiento con la misma facilidad con que lo dio. Ello implica, entre otras cosas, que el responsable o encargado del tratamiento debe hacer posible ese retiro de forma gratuita, sin dificultar el proceso y sin reducir la calidad del servicio.

Con base en las directrices internacionales que entienden la trascendencia del derecho de *Habeas Data* en la era digital y la necesidad de que ella sea regulada de una manera especial, se podría pensar que el Estado colombiano ya ha empezado a fijarse unos objetivos para fortalecer su ordenamiento jurídico en el tema.

Sin embargo, el Estado se ha quedado corto para regular la actividad en la internet, donde constantemente se están presentando situaciones que ponen en riesgo derechos como el de *Habeas Data*, libertad e intimidad. Se ignora una realidad que afecta a las personas, incluso desde antes de su nacimiento, y es la relativa a la gran cantidad de datos que se recolectan diariamente en la web y se procesan mediante algoritmos para formar un perfil de cada individuo.

En Colombia, la Corte Constitucional ha reconocido explícitamente los peligros de la acumulación desproporcionada de información personal por los perfiles y categorías que se pueden crear para tomar decisiones sobre las personas (C-748, 2011). Sin embargo, esta preocupación no quedó consignada en la ley ni en la regulación de protección de datos. (González-Guerrero, 2019, p. 223)

De otra parte, la Superintendencia de Industria y Comercio, ha venido generando conciencia en la comunidad sobre la importancia de proteger su información personal, pero a pesar de sus esfuerzos, su reglamentación poco habla sobre las consecuencias de albergar dicha información en la web.

De manera general y sin mayores detalles, el legislador colombiano y la autoridad en la materia, han dado a entender que la Ley 1581 de 2012, el Decreto 1377 de 2013 y las demás normas sobre protección de datos personales, también rigen para los casos en que la información ha sido recolectada a través de internet.

Lo anterior lleva a afirmar que la normatividad colombiana está pasando por alto formas en que se obtiene información personal que son mucho más invasivas y peligrosas que las que hasta el momento se han considerado. Podría anticiparse que dicha falta se debe a la dificultad para controlar la actividad de las personas en la web, un lugar que no descansa en ningún momento y que ha cruzado todas las barreras espaciotemporales.

No obstante, hoy más que nunca se requiere que el Estado tome un papel activo en la protección de datos personales, especialmente los que circulan en internet; esto a través del fortalecimiento de sus estructuras regulativas, el acompañamiento y educación de la población, la inversión en recursos que le permitan a la autoridad, en este caso, la Superintendencia de Industria y Comercio, ampliar su capacidad de vigilancia y control, así como especializarse en los fenómenos que se están presentando con el uso de las plataformas digitales y el llamado internet de las cosas.

CONCLUSIONES

Hoy la sociedad asiste un asombroso desarrollo tecnológico que cada día sorprende con sus novedades, y que en gran medida se ha enfocado en la recolección de todo tipo de datos sobre cualquier persona en el mundo, consiguiendo, por ejemplo, desplazar el comercio de productos y servicios para darle todo el valor a la información; ha posibilitado realizar clasificaciones sociales de acuerdo a la ideología, raza, color, sexo, religión y demás preferencias, a través de algoritmos implantados en todo lo que hace parte de la cotidianidad de las personas. En todo caso, aún es incierto lo que se puede lograr en un futuro con la información personal.

Así pues, los datos personales son el intangible más valioso que pueden tener las personas y el bien por el que los entes públicos y privados están dispuestos a luchar. De hecho, ya son muchos los espacios que se han propiciado para que los sujetos intercambien su información por beneficios, sin que tengan la posibilidad de evaluar las consecuencias.

De esta manera, mediante el tratamiento de datos personales, obtenidos bajo una presión indirecta ejercida sobre el titular –por ejemplo, cuando la prestación de un servicio es condicionada a la aceptación–, los responsables o encargados de los mismos, transgreden derechos fundamentales como el de *Habeas Data*, libertad e intimidad.

Es cierto que existen propósitos validos por los cuales las entidades deben tener determinada información de las personas, el problema es la seguridad con la que la conservan o las facultades que se han atribuido desde la autorización dada por el titular.

En este punto, los principios éticos y morales de quienes dirigen las empresas y los Estados, juegan un papel fundamental, pues son ellos quienes finalmente deciden cómo obtener, utilizar, conservar y negociar, los datos de las personas.

Por otro lado, en relación con el marco jurídico colombiano, se pudo evidenciar que todavía hacen falta esfuerzos para que la regulación comprenda de manera adecuada el tratamiento de datos personales en internet, y que la que ya existe se haga cumplir a través de mecanismos más efectivos; pero en todo caso, es urgente atender los desafíos que se presentan en esa esfera tan compleja de controlar.

Hay que reconocer que el flujo transfronterizo de datos a través de internet, está poniendo en crisis la soberanía de los Estados, puesto que ya no es tan fácil ejercer control sobre los responsables o encargados del tratamiento de la información personal; a veces ni si quiera se logra determinar quién tiene el manejo de dicha información, pues una vez en la web, fácilmente puede quedar a disposición de cualquier persona o entidad que se encuentre en cualquier parte del mundo.

Finalmente, es indispensable que los Estados desarrollen políticas públicas más efectivas, que generen conciencia en las personas sobre el valor que tiene su información, los riesgos que enfrentan y las facultades que les pertenecen; pero también, sobre el deber que todos tienen de reconocer en el otro derechos fundamentales como el de *Habeas Data*, libertad e intimidad. Nuevamente se trata de un asunto ético y moral.

BIBLIOGRAFÍA

Article 29 Working Party (2018). *Guidelines on consent under Regulation 2016/679*. European Commission.

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. Recuperado de

http://www.secretariassenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Bauman, Z. & Lyon, D. (2013). *Vigilancia líquida*. Barcelona, España: Paidós.

Congreso de La República de Colombia. (2008). *Ley Estatutaria 1266 del 31 de diciembre de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Bogotá D.C.: Congreso de La República de Colombia.

Congreso de La República de Colombia. (2012). *Ley Estatutaria 1581 del 18 de octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales*. Bogotá D.C.: Congreso de La República de Colombia.

Corte Constitucional. (16 de octubre de 2008). Bogotá. C-1011. [MP. <Jaime Córdoba Triviño>]

Craig, T. & Ludloff, M. (2011). *Privacy and big data*. Sebastopol (California): O'Reilly Media, Inc.

Garriga-Domínguez, A. (2016). *Nuevos retos para la protección de datos personales en la era del big data y de la computación ubicua*. Madrid: Dykinson.

Recuperado de
<https://books.google.com.co/books?id=qxkJDAAAQBAJ&printsec=frontcover&dq=NUEVOS+RETOS+PARA+LA+PROTECCI%C3%93N+DE+DATOS+PERSONALES.+EN+LA+ERA+DEL+BIG+DATA+Y+DE+LA+COMPUTACI%C3%93N+UBICUA&hl=es&sa=X&ved=2ahUKEwjzjvDx9e7qAhXpYN8KHV5TCfIQ6AEwAHoECAMQAg#v=onepage&q=El%2070%25%20del%20universo%20&f=false>

González-Guerrero, L. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, 21(1), 209-244. <http://dx.doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>

Martínez, A. (2019). La inteligencia artificial, el *big data* y la era digital: ¿una amenaza para los datos personales?. *Revista la propiedad inmaterial*, (27), pp. 5-23. <https://doi.org/10.18601/16571959.n27.01>

Medina, M. A. (5 de octubre de 2017). La historia detrás de la Internet de las Cosas. *El Espectador*. Recuperado de <https://www.elespectador.com/noticias/tecnologia/la-historia-detras-de-la-internet-de-las-cosas/>

Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. Recuperado de https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Presidente de La República de Colombia. (2013). *Decreto 1377 del 27 de junio de 2013 por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Bogotá D.C.: Presidente de La República de Colombia.

Remolina-Angarita, N. (2010). ¿Tiene Colombia Un Nivel Adecuado De Protección De Datos Personales a La Luz Del Estándar Europeo?. *International Law: Revista Colombiana de Derecho Internacional*, (16). 489-524. Recuperado de <http://aplicacionesbiblioteca.udea.edu.co:2277/ehost/detail/detail?vid=3&sid=8bacdc29-6fa9-46c3-8d17-47c64d7e66c1%40pdc-v-sessmgr05&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=61020726&db=fua>.

Rodotà, S. (2003). Democracia y protección de datos. *Cuadernos de Derecho Público*, (19-20). 15-26.

Sánchez, A. (Ed.). (2014). *Derechos humanos y protección de datos personales en el siglo XXI*. Sevilla, España: Punto Rojo Libros. <https://books.google.com.co/books?id=O6hcDwAAQBAJ&printsec=frontcover&dq=DERECHOS+HUMANOS+Y+PROTECCI%C3%93N+DE+DATOS+PERSONALES+EN+EL+SIGLO+XXI.#v=onepage&q=DERECHOS%20HUMANOS%20Y%20PROTECCI%C3%93N%20DE%20DATOS%20PERSONALES%20EN%20EL%20SIGLO%20XXI.&f=false>

Superintendencia de Industria y Comercio. (2015). Guía para la implementación del principio de responsabilidad demostrada (Accountability). Recuperado de <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

Superintendencia de Industria y Comercio. (s.f.). *Protección de datos personales*. Recuperado de <https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>

Organización para la Cooperación y el Desarrollo Económicos. (2013). The OECD privacy framework. Recuperado de https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Téllez-Aguilera, A. (2001). *Nuevas tecnologías: intimidad y protección de datos*. Madrid, España: Edisofer.