DATAVERSE, LA VIGILANCIA DE LA INFORMACIÓN Y SU LEGITIMACIÓN POR MEDIO DEL DERECHO A LA PRIVACIDAD. UN ESTUDIO DE CASO: COLOMBIA A PARTIR DEL 2010 Y EL ESTADO DEL ARTE DEL DERECHO A LA PRIVACIDAD EN EL MUNDO

MARY LUZ AGUDELO OSPINA

GERMÁN ANDRÉS OSORIO RAMÍREZ

Universidad de Manizales

Facultad de Ciencias Jurídicas

Programa de Derecho

Manizales

2014

DATAVERSE, LA VIGILANCIA DE LA INFORMACIÓN Y SU LEGITIMACIÓN POR MEDIO DEL DERECHO A LA PRIVACIDAD. UN ESTUDIO DE CASO: COLOMBIA A PARTIR DEL 2010 Y EL ESTADO DEL ARTE DEL DERECHO A LA PRIVACIDAD EN EL MUNDO

MARY LUZ AGUDELO OSPINA

GERMÁN ANDRÉS OSORIO RAMÍREZ

Trabajo de grado presentado para optar al título de Abogado

Director

Dr. Rodrigo Giraldo

UNIVERSIDAD DE MANIZALES

Facultad de Ciencias Jurídicas

Programa de Derecho

Manizales

2014

TABLA DE CONTENIDO

"*DATAVERSE*, LA VIGILANCIA DE LA INFORMACIÓN Y SU LEGITIMACIÓN POR MEDIO DEL DERECHO A LA PRIVACIDAD. UN ESTUDIO DE CASO: COLOMBIA A PARTIR DEL 2010 Y EL ESTADO DEL ARTE DEL DERECHO A LA PRIVACIDAD EN EL MUNDO[1]"

RESUMEN

El *Dataverse* es un universo amplio y creciente de recopilación de datos, almacenamiento y difusión, el cual ha provocado ansiedad en la sociedad civil, ya que este fenómeno tiene dos aspectos principales: el aumento de la vigilancia tanto por organismos públicos y privados, así como el aumento de la auto-proyección de una 'tecno-cultura' de Internet y de otros elementos de la esfera de la información, un proceso que implica la creación constante, deliberada e incidental, de gran cantidad de datos por parte de sus usuarios. La angustia producida en ambos casos es generalmente articulada con el lenguaje de la vida privada. Por tanto, debe aclararse y legitimarse lo que hay bajo la superficie de este término tan opaco y difuso para establecer su relación con ciertos procesos políticos, sociales y económicos. Asimismo, es necesario configurar un derecho a la privacidad que sea más participativo e incluyente, que permita eliminar la porosidad de las fronteras jurídicas del *Dataverse*.

Palabras clave: *Dataverse*, derecho a la privacidad, derechos humanos, sector público, sector privado, sociedad civil, tecnología, vigilancia.

[1] Para el desarrollo de esta investigación se tendrán en cuenta los siguientes países: Estados Unidos, Canadá, Inglaterra, Alemania.

ABSTRACT

The *Dataverse* is a large and growing universe of data collection, storage and dissemination, which has caused anxiety in civil society, since this phenomenon has two main aspects: the increased surveillance by both public and private agencies, as well as increased self-projection of one 'techno-culture' of Internet and other elements of the field of information, a process that involves the constant creation, deliberate and incidental, of large amount of data by users. The anxiety produced in both cases is generally articulated with the language of privacy. Therefore, should be clarified and legitimized what lies beneath the surface of this term so opaque and diffuse to establish its relationship with certain processes political, social and economic. Also, is necessary configuring a right to privacy; that make it more participatory and inclusive, and that will eliminate the porosity of the legal barriers of *Dataverse*.

Key words: *Dataverse*, privacy, human rights, public sector, private sector, civil society, technology, surveillance.

0. INTRODUCCIÓN

Toda una constelación de problemas conecta a la tecnología con los derechos humanos. Uno de los principales problemas es el fenómeno de la 'ubicuidad' de los datos. Ya que en los últimos años han aparecido nuevas técnicas para la recolección, almacenamiento, análisis y despliegue de datos, lo que afecta nuestras vidas de diversas e innumerables maneras, por ejemplo, en el aspecto crediticio, laboral e incluso de movilidad debido al rastreo satelital. Por ello, la vigilancia tanto por entidades públicas como privadas juega un papel importante, no obstante, todas las personas sin importar su raza, edad, género, condición socio-económica u oficio, generan habitualmente grandes cantidades de datos sobre sí mismas, a menudo descartando que puedan llegar a ser vigiladas. Hoy en día todos somos los 'interesados', en esta nueva realidad contemporánea como lo es el *Dataverse*[2].

Así las cosas, la vigilancia ―cibernética y de medios― y otras tecnologías de recopilación se están extendiendo rápidamente a través de las fronteras. Algunas tecnologías, como las satelitales, son fundamentalmente de naturaleza global y de gran alcance. Sin embargo, todos los datos transmitidos electrónicamente, ya sea por medio de Internet (correo electrónico, redes sociales u otros) o a través de la tierra y la telefonía móvil, son propensos a ser recolectados en cualquier lugar incluso distinto a la jurisdicción de la ubicación del titular de ellos. Así pues, la interferencia en las comunicaciones es más fácil de realizar, que evitar que nuestros datos almacenados y reproducidos dejen rastro alguno.

En este orden de ideas, tanto los organismos públicos como privados se han convertido en recolectores. Aunque la vigilancia estatal o el haking de email y cuentas pueden implicar la recopilación de datos sobre las personas en todo el mundo, las grandes empresas

[2] El 'dataverse' es una aplicación Web que permite publicar, citar, almacenar, distribuir y analizar bases de datos cuantitativos.

informáticas, tales como Apple, Facebook o Google, también capturan la información de los individuos a nivel mundial y la almacenan en grandes servidores centralizados, por lo general, localizados en los Estados Unidos. Como resultado, los derechos de la protección de datos, así como los derechos humanos pertinentes incluso si son adecuados a nivel nacional, rara vez son tenidos en cuenta en el contexto transnacional, en el que el almacenamiento se lleva a cabo. Por tanto, las fronteras del *Dataverse* son inherentemente porosas.

Por tal motivo, grandes cantidades de información se llevan a cabo en diversos centros, de nuevo, tanto públicos como privados, los cuales la recogen, almacenan y procesan para una variedad de fines. En general, el realmente interesado no tiene ni idea del grado de información que existe sobre él y los fines a los que está siendo sometida. Así pues, el aumento de la asimetría informática como una condición general para la comunicación e interacción en el mundo de hoy es, sin duda, una causa de ansiedad para todas las personas. Más allá de esto, sin embargo, también es un motivo de posible injusticia. No obstante, aparece como un elemento potencialmente constitutivo e imborrable de los acuerdos sociales actuales dentro de la sociedad civil.

El derecho humano rector de este conjunto de fenómenos es, sin duda, el derecho a la privacidad, pero es igualmente claro que este ‘derecho’, al menos en su formulación actual, no encierra dentro de sí toda la gama de las preocupaciones generadas por dicha situación. Por ello, es necesario darle un doble enfoque al tema: (i) re-evaluar la posibilidad de tener una vida privada y su relación con la ley de manera más amplia, por una parte, y (ii) la exploración de la relevancia de otros derechos humanos para este tema, por el otro.

En cuanto a lo primero, la discusión se embarca en una reevaluación más amplia del principio de la privacidad, un principio que es fundamental para las ideas modernas acerca

del gobierno, los derechos humanos y, además, la relación entre el Estado y la sociedad, entre lo público y los sectores privados. La intimidad es fundamental para nuestras concepciones de autonomía individual que son, a su vez, fundamentales para la adecuada formación del 'público en general' ―como se entiende generalmente― como una fuente de 'interés público'. En los Estados modernos, lo privado, en este sentido, es fundamental para que la sociedad civil ―como una perspectiva de la democracia y los derechos humanos― pueda llevar a cabo sus expectativas de vida. Esto, asimismo, depende de la retención de una esfera de la vida privada. Por esta razón, la privacidad está protegida constitucionalmente[3] y garantizada a través de los derechos y acuerdos institucionales internacionales, como es el caso del *Pacto de San José*. El ideal de un espacio protegido, de intimidad, plasma nuestro comportamiento y nuestras expectativas de acción e interacción con el Estado.

Sin embargo, la ubicuidad de los datos personales y el contexto que lo produce están poniendo hoy en día una enorme presión sobre la noción de vida privada y su transformación, tal vez más allá de su reconocimiento. Así, la privacidad requiere ―entre otras cosas― el control personal sobre la información.

Empero, debido al *Dataverse* es casi imposible ejercer el control sobre nuestros propios datos. Paradójicamente, aunque seamos los generadores principales de datos sobre nosotros mismos, podemos renunciar, sin nuestro consentimiento, al control sobre ellos con facilidad y rapidez. Por otra parte, en un grado cada vez mayor, todo tipo de entidades tanto públicas

[3] En reiteradas ocasiones la Corte Constitucional se ha pronunciado al respecto, por ejemplo, en la sentencia T-491 de 2012: "*Así, el alcance del derecho a la intimidad depende de las restricciones que se impongan a los demás y aunque en principio es considerado inalienable e imprescriptible, la posibilidad de limitarlo obedece a razones de "interés general", "legítimas", y "debidamente justificadas constitucionalmente", que no afecten su núcleo esencial representado por el espacio inviolable e inaccesible en el que el individuo actúa libremente, sin injerencias, sin ser observado o escuchado*".

como privadas almacenen la información sobre nosotros y, en algunos casos —como los registros de crédito— no los podemos controlar o en determinadas situaciones —como las listas negras de terroristas— sin saber siquiera, el tipo o la cantidad de datos que poseen de nosotros por medio de la vigilancia de otros.

En términos más generales, el fenómeno de la ubicuidad de datos coloca al sector público y al privado bajo una tensión. La empresa tecnológica, la reproducción y la aceleración se llevan a cabo en una zona de indistinción público-privada. A menudo son iniciadas por las entidades públicas muchas aplicaciones de las TIC que posteriormente se cultivan por los operadores privados tanto por razones estratégicas como comerciales. Al igual que los operadores privados a menudo se basan en la información de 'reuniones' públicas —como las imágenes de satélite de Google—, asimismo, lo hacen las agencias públicas que se basan en los datos de recolección privada, por ejemplo, los datos personales de los proveedores de correo electrónico. A pesar de esto el público en general también se basa, paradójicamente, en que el Estado lo protegerá contra el abuso privado de sus datos y, al mismo tiempo, también depende de proveedores privados (vigilantes) para protegerse de la intrusión estatal. Esta fusión y confusión entre las categorías públicas y privadas plantea un serio problema para los derechos humanos, los cuales prefieren una clara distinción entre lo privado (individual) y lo público (estatal).

En cuanto a los derechos humanos, cabe preguntarnos cuál será el impacto de la transformación contemporánea de la vida privada en general, a saber: si los temores de que las tecnologías de recolección de datos generan, justifican (o deberían despertar) una posición seria y radical en cuestiones de derechos humanos y si el derecho a la privacidad (o intimidad) puede ayudarnos de manera adecuada a entender y manejar dichas preocupaciones.

En cuanto al derecho a la privacidad, autores como Ruth Gavison (2012) hacen un examen detallado de la legislación a nivel internacional poniendo de manifiesto dos tendencias. Primero, la aplicación del derecho a la privacidad parece bastante robusto en el caso de dos tipos reconocibles de intimidad: privacidad de decisión ―que es la libertad en las decisiones relativas al mismo― como la orientación sexual o la elección de credo, por un lado, y una espacial de privacidad ―que es el grado en que el individuo ejerce control sobre un espacio físico o propiedad― una casa o un automóvil, por el otro. Sin embargo, la protección es menos robusta, cuando se trata de la tercera fase de la vida privada, la cual es la que nos interesa aquí: la privacidad de la información. Ya que la protección de una expectativa razonable de la vida privada no parece decisiva en el contexto de los datos en el *Dataverse*.

Con base en lo anterior, este trabajo de grado pretende analizar las implicaciones sobre la vigilancia de las comunicaciones, almacenamiento de la información y los datos, por parte de los Estados y el sector privado para el ejercicio del derecho humano a la privacidad o intimidad. Al examinar el impacto de los avances tecnológicos significativos en las comunicaciones, se pone de relieve la urgente necesidad de estudiar más a fondo las nuevas modalidades de vigilancia y de revisar las leyes nacionales e internacionales que regulan estas prácticas de acuerdo con la normativa de los derechos humanos, como son la *Carta de los Derechos Fundamentales* y la *Directiva de Protección de Datos* de la Unión Europea, en Canadá la *British Columbia Privacy Act* de 1979, y en Latinoamérica el *Pacto de San José*.

Asimismo, las innovaciones tecnológicas han aumentado las posibilidades para la comunicación, lo que permite el anonimato, los diálogos rápidos de intercambio de información e interculturales. No obstante, los cambios tecnológicos han aumentado, al mismo tiempo, las oportunidades para la vigilancia del Estado y las intervenciones en las comunicaciones privadas de los individuos.

Así las cosas, las preocupaciones acerca de la seguridad nacional y la actividad criminal pueden justificar el uso excepcional de las tecnologías de vigilancia de las comunicaciones. Sin embargo, las leyes nacionales e internacionales que regulan lo que constituiría la implicación necesaria, legítima y proporcional del Estado en la vigilancia son a menudo insuficientes o inexistentes. Ya que los marcos jurídicos nacionales son inadecuados y crean un terreno fértil para las infracciones arbitrarias e ilegales del derecho a la privacidad y, en consecuencia, también ponen en peligro la protección del derecho a la libertad de opinión y de expresión.

Por tanto, es necesario configurar un derecho a la privacidad que sea más participativo e incluyente y que apunte a eliminar la porosidad de las fronteras jurídicas del *Dataverse*. Para ello, hemos considerado pertinente trazar la siguiente ruta: (i) describir la realidad que hoy circunda el *Dataverse*; (ii) comprobar las posibilidades con las que cuenta el derecho internacional sobre el derecho a la privacidad; (iii) analizar la relación entre derecho e información en un mundo globalizado. Finalmente, el presente trabajo de grado pretende presentar como ha sido utilizada de manera arbitraria e injusta la información almacenada en el *Dataverse*, ya que en los últimos años el derecho a la privacidad se ha visto vulnerado en determinadas ocasiones por los Estados ―a nivel nacional, el caso de las interceptaciones del DAS y a nivel internacional el caso Snowden― e incluso por sectores privados ―caso *News Corporation*―, en aras de proteger el *statu quo*. Por tanto, nuestra propuesta consiste en establecer la legitimidad de las razones esgrimidas jurídicamente para vulnerar el derecho a la privacidad de las personas, estableciendo cuáles son los límites y alcances de esta.

1. ESTADO DEL ARTE Y ANTECEDENTES

Pida a las primeras 10 personas que caminan cerca a usted en el centro comercial y pregúntele por los derechos constitucionales que conoce y es una apuesta casi segura, que incluso aquellos cuya lista solo tienen a uno de estos derechos nombrará al derecho a la privacidad, como mínimo ligado a la libertad. Este derecho es quizás el más discutido en los medios de comunicación e inclusive en una conversación casual con cualquiera de nuestros amigos.

Para Samuel Warren y Louis Brandeis, en su artículo "El derecho a la privacidad" publicado en la *Revista de Derecho* de Harvard en 1890, el derecho a la privacidad (o intimidad) se esgrime como:

> el derecho consuetudinario ha reconocido siempre la casa de un hombre como su castillo inexpugnable, a menudo, ni siquiera para sus propios funcionarios que participan en la ejecución de sus órdenes (Warren y Louis Brandeis, 1890, p. 23).

Así las cosas, la privacidad es un derecho humano fundamental reconocido en la *Declaración de los Derechos Humanos*, el *Pacto Internacional de Derechos Civiles y Políticos* de las Naciones Unidas y en muchos otros tratados internacionales y regionales. Privacidad sustentada en la dignidad humana y otros valores fundamentales como la libertad de asociación y la libertad de expresión. Por ello, se ha convertido en uno de los temas más importantes de los derechos humanos en la era moderna. Por lo que casi todos los países del mundo reconocen el derecho a la intimidad explícitamente en su Constitución. Así como mínimo, estas disposiciones incluyen los derechos de

inviolabilidad del domicilio y el secreto de las comunicaciones. Incluso la mayoría de las Constituciones recientes tales como en Sudáfrica y Hungría incluyen derechos específicos para acceder y controlar la información personal.

Asimismo, en los países donde la privacidad no se reconoce explícitamente en la Constitución, como es el caso de los Estados Unidos, Irlanda y la India, los tribunales supremos han determinado a este derecho en otras disposiciones. A su vez, también en muchos países, como España, Inglaterra, Italia, Alemania, los acuerdos internacionales que reconocen el derecho a la privacidad, como el *Pacto Internacional de Derechos Civiles y Políticos* o el *Convenio Europeo de Derechos Humanos* han sido adoptados como ley.

A principios de la década de 1970, los países comenzaron a adoptar leyes generales destinadas a proteger la privacidad individual. En todo el mundo hubo un movimiento general hacia la adopción de leyes integrales sobre la privacidad que establecieran un marco para su protección. La mayoría de estas leyes se basan en los modelos presentados por la Organización para la Cooperación y Desarrollo Económico y el Consejo de Europa.

En 1995, consciente tanto de las deficiencias de la ley como de las muchas diferencias en el nivel de protección en cada uno de sus Estados, la Unión Europea aprobó una directiva de ámbito europeo que ofrecería a los ciudadanos un abanico más amplio de protección sobre los abusos de sus datos. La Directiva sobre la *Protección de las personas con respecto al tratamiento de datos personales y a la libre circulación de estos datos*, establece un punto de referencia para la legislación internacional. Así, cada Estado de la Unión debe aprobar la legislación complementaria de octubre de 1998 sobre protección de datos.

La Directiva también impone a los Estados miembros garantizar que los datos personales relativos a sus ciudadanos están cubiertos por la ley cuando se exporta o procesa en países por fuera de Europa. Este requisito se ha traducido en una creciente presión a nivel internacional para la aprobación de leyes sobre la protección a la intimidad. En este orden de ideas, más de cuarenta países cuentan con la protección de datos o leyes de privacidad de la información y todavía hay más en el proceso de ser promulgadas, aunque en Colombia no hay noticias de ello, a pesar de los últimos escándalos al respecto.

Por tanto, son varias las razones que sustentan el movimiento hacia una completa privacidad y las leyes de protección de datos del *Dataverse*. Así, muchos países están adoptando estas leyes por una o más razones, entre ellas, para poner remedio a las injusticias del pasado. La mayoría de los países, especialmente en Europa, América del Sur y Sudáfrica, están adoptando leyes para remediar las violaciones a la privacidad que se produjeron por los regímenes autoritarios anteriores a sus democracias.

1.1. Marco de antecedentes

En este orden de ideas, la privacidad puede ser definida como un elemento fundamental de los derechos humanos. Las leyes sobre ella se remontan tan atrás como lo es 1361, cuando los jueces de paz en Inglaterra proporcionaron la detención de mirones y espías. En 1765, lord Camden escribió sobre aquellos que entraron en una casa y confiscaron documentos privados: “podemos decir con seguridad que no hay ley en este país para justificar los acusados en lo que han hecho, si la hubiera, se destruiría todas las comodidades de la sociedad, porque los papeles suelen ser la propiedad más querida que un hombre puede tener” (James, 1994, p. 15). Asimismo, el parlamentario William Pitt afirmó: “el hombre más pobre puede en su casa desafiar a toda la fuerza de la Corona; puede ser frágil, el techo puede temblar, el viento puede soplar y las tormentas pueden entrar, la lluvia puede entrar,

pero el rey de Inglaterra no puede entrar; todas sus fuerzas no se atreven a cruzar el umbral de la casa de un vecino así esté en ruinas" (Hixson, 1984).

A su vez, diversos países desarrollaron protecciones específicas para la privacidad en los siglos que siguieron. En 1776, el parlamento sueco aprobó la "Ley de Acceso a Registros Públicos", la cual requería que toda la información en poder del gobierno debía ser utilizada tan solo para fines legítimos. En 1789, la *Declaración de los Derechos del Hombre y del Ciudadano* afirmó que la propiedad privada era inviolable y sagrada. Francia prohibió la publicación de datos privados y estableció multas en 1858. En 1890, los abogados Samuel Warren y Louis Brandeis definieron el derecho a la privacidad como una acción de responsabilidad civil, describiéndolo como "el derecho a ser dejado solo".

El concepto moderno de privacidad a nivel internacional se puede encontrar en la *Declaración Universal de Derechos Humanos*, la cual protege específicamente la privacidad territorial y las comunicaciones. El artículo 12 establece: "*nadie debe ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques*".

También numerosos pactos internacionales de derechos humanos dan una referencia específica a la privacidad como un derecho. El *Pacto Internacional de Derechos Civiles y Políticos* (PIDCP), la *Convención de la ONU sobre Trabajadores Migrantes* y la *Convención sobre la Protección del Niño* adoptan el mismo idioma.

Así pues, para muchos autores anglosajones y franceses[4], el derecho al respeto de la 'vida privada' es el derecho a la privacidad, el derecho a vivir por lo que uno desea, a estar protegidos de la publicidad, y demás. Sin embargo, el derecho al respeto de la vida privada no termina ahí. Comprende también, en cierta medida, el derecho a establecer y desarrollar relaciones con otros seres humanos especialmente en el campo emocional para el desarrollo y cumplimiento de nuestra propia personalidad y planes de vida.

Por su parte, a nivel regional, el artículo 11 de la *Convención Americana sobre Derechos Humanos* establece el derecho a la privacidad en términos similares a la *Declaración Universal*. En 1965, la Organización de los Estados Americanos proclamó la *Declaración Americana de los Derechos y Deberes del Hombre*, la cual aboga por la protección de numerosos derechos humanos, entre ellos la privacidad. Asimismo, la Corte Interamericana de Derechos Humanos también ha comenzado a direccionarse sobre los problemas a la privacidad en sus casos.

Por tal motivo, el interés por el derecho a la privacidad ha aumentado desde los años 1960 y 1970 hasta hoy, con el advenimiento de la tecnología de la información (IT) y el *Dataverse*. El potencial de la vigilancia de los sistemas informáticos de gran alcance impulsó la demanda de normas específicas[5] que regulan la recolección, el almacenamiento y el tratamiento de la información personal. En muchos países, las nuevas constituciones reflejan este derecho, por ejemplo, desde el 2002 la India, Suráfrica, Bélgica y Australia

[4] Entre los autores anglosajones encontramos: Ruth Gavison, Lothar Determann, David H. Holtzman, Charles Glasser, Adam Moore; mientras que del lado francés tenemos: Sébastien Crosnier, Simon Grunwald, Guido Bonolis, Ivana Roagna; entre otros.

[5] Entre las diversas normativas específicas tenemos: en la República de Corea, la *Ley de Comunicaciones de la Información*, aprobada en 2007; en Pakistán el *Fair Trial Act* de 2012; en los Estados Unidos la *Foreign Intelligence Surveillance Amendment Act* de 2008; en Brasil la *Ley Federal 12683* de 2012; en Suráfrica la *Regulation of Interception of Communications and Provisions of Communication-Related Information Act* de 2010.

dan cuenta de ello. La génesis de la moderna legislación en esta área se remonta a la primera ley de protección de datos en el mundo promulgada en el Estado federado de Hesse en Alemania, en 1970. Esto ha sido seguido por la legislación nacional en Suecia (1973), los Estados Unidos (1974) y Francia (1978).

No obstante, dos instrumentos internacionales son fundamentales para las nuevas leyes. El Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos personales y la Organización para la Cooperación Económica y las Directrices del Desarrollo del Consejo de Protección de la Privacidad y Datos de los flujos transfronterizos de datos personales, los cuales articulan normas específicas sobre el tratamiento de los datos electrónicos en el *Dataverse*. Las reglas dentro de estos dos documentos forman el núcleo de las leyes de protección de datos de decenas de países. Estas reglas describen la información personal desde la protección en cada paso de la recolección hasta el almacenamiento y su difusión. Por tanto, el derecho de las personas a acceder y modificar sus datos es un componente principal de estas normas.

Pero esta estructura jurídica no ha sido suficiente para proteger y garantizar nuestro derecho a la privacidad. El registro de la información sobre las actividades específicas en Internet o vía telefónica se ha convertido en una de las mayores amenazas emergentes a la privacidad. Cada vez que un usuario accede a una página Web, el servidor que contiene la página registra la dirección de Internet del usuario junto con la hora y la fecha. Algunos sitios colocan ‘cookies’ para ayudar a las actividades de seguimiento de las personas en un nivel mucho más detallado. Otros preguntan por el nombre del usuario, dirección y otros datos personales antes de permitir el acceso. Compras por Internet se registran de manera similar. Tiendas en línea valoran muy positivamente estos datos, sobre todo por la posibilidad de vender los datos a los comerciantes y otras organizaciones, y ni hablemos del registro y almacenamiento de nuestras comunicaciones telefónicas.

Así, en los últimos años el derecho a la privacidad se ha visto vulnerado en determinadas ocasiones por los Estados e incluso por sectores privados, en aras de proteger el *statu quo*. Lo que ha causado una gran alarma entre los defensores de los derechos humanos, sin embargo, la discusión apenas comienza y los mecanismos jurídicos han demostrado ser ineficientes[6], lo que merece una revisión a luz de los derechos humanos.

[6] Tradicionalmente, estos controles se encontraban en manos del Estado. El Estado construyó y era dueño de una infraestructura de telecomunicaciones y seguridad, manteniendo activamente el control sobre ellas. Ahora, esas estructuras se han privatizado, renunciando a los controles públicos y dejándolos en manos privadas, como por ejemplo Google o Yahoo!. Como resultado de ello, las responsabilidades paternalistas que antes desempeñaba el Estado han pasado al sector privado, que ahora, se supone, debe gestionar nuestra privacidad de la información. Lo que ha ocasionado que los viejos mecanismos jurídicos que no tenían en cuenta a dicho sector se hayan vuelto ineficientes y obsoletos.

2. DELIMITACIÓN DEL ÁREA

El área de estudio general del presente trabajo de grado se enmarca dentro del contexto jurídico-político, con base en el análisis de una figura de origen político-legal, como lo es el derecho a la privacidad tanto a nivel nacional como internacional, y su correspondiente estudio a la luz de los postulados constitucionales y, en especial, de la *Declaración Universal de Derechos Humanos*. También, para su desarrollo es necesario recurrir al estudio de las principales fuentes del derecho, como lo son la ley (nacional e internacional), la jurisprudencia y la doctrina.

Así las cosas, y respecto a la delimitación general del área, este tema se encuentra enmarcado dentro del derecho público y el derecho privado, ya que en los últimos años, el derecho a la privacidad ha sido violado tanto por organismos estatales como empresas del sector privado[7]. Debido a que la distinción público-privado desempeña un papel indispensable en la estructura de las bases jurídicas y conceptuales del Estado y la sociedad, además de la relación entre estos. Aunque a menudo de manera implícita, se supone constantemente que un régimen jurídico moderno y estatal debe preservar y consolidar los distintos ámbitos públicos y privados, en muchas ocasiones, esta barrera se vuelve difusa, generando una tensión entre ambos sectores, lo que violenta la protección de los derechos humanos.

En conclusión, tenemos entonces que el área del presente trabajo es jurídico-política con elementos de derecho público especialmente constitucional y administrativo, además de

[7] Por ejemplo, el caso de la agencia NSA del gobierno de los Estados Unidos interceptando las comunicaciones de la canciller alemana Angela Merkel y las interferencias en las comunicaciones realizadas por el periódico *The Sun*, propiedad del multimillonario Rupert Murdoch.

derecho privado, civil y comercial y, en especial, de los derechos humanos en el derecho internacional.

2.1. Delimitación del tema

El tema central de este trabajo de grado es el derecho a la privacidad y su relación con los sectores públicos y privados, para lo cual será abordado de la siguiente manera:

En primer lugar, se desarrollará de manera detallada el derecho a la privacidad y su formulación en la *Declaración Universal de Derechos Humanos*, para conocer y comprender las implicaciones de este derecho dentro de los ordenamientos jurídicos estadounidense, de la Unión Europea y colombiano.

En segundo lugar, se realizará un estudio comparativo del derecho a la privacidad en la normativa nacional e internacional, además de un rastreo jurisprudencial sobre la forma en cómo la Corte Constitucional ha entendido su aplicación y la manera de garantizarlo.

Por último, al tener clara la normativa en torno al derecho a la privacidad y el contenido de los postulados constitucionales, se procederá a realizar el análisis, por medio de estudio de casos, de la manera en que este derecho debe evolucionar a la par en que evolucionan los desarrollos tecnológicos.

3. PLANTEAMIENTO DEL PROBLEMA

El problema que dio sustento al desarrollo de este trabajo de grado se centró en cómo se percibe la privacidad y la amenaza que se cierne sobre ella por las tecnologías de recolección y almacenamiento de datos y, en especial, la vigilancia en el *Dataverse*. Típicamente, la vigilancia y la privacidad son presentadas en oposición, pero también es el caso de que cada una presupone a la otra. Por tanto, la intimidad se ha convertido en nuestra ruta por defecto, pero no es el único punto a tratar, ya que en determinadas ocasiones la vigilancia es necesaria para conservar el *statu quo,* lo importante aquí es encontrar el justo equilibrio entre ambas a la luz de los derechos humanos y la normativa internacional.

Una parte esencial de los derechos humanos contemporáneos es el concepto de la autonomía personal. Cada persona tiene que tener autonomía para que pueda sentirse libre de tomar decisiones. Así, una persona que es libre de tomar decisiones se siente segura y feliz. El ser humano se entiende que es una entidad esencialmente independiente y su desarrollo es de forma individual. Por supuesto, no podemos subestimar el papel de la sociedad porque la vida de las personas no está aislada y siempre se encuentra influida por muchos factores externos, por lo que el individuo se encuentra a menudo frente al poder coercitivo del Estado.

Las restricciones, reglas e interferencias autorizadas en la privacidad del individuo hacen del tema de la autonomía muy importante. Así, para sobrevivir como individuo, la persona se compromete a aceptar ciertas limitaciones a su libertad de acción. Por lo que cada Estado tiene la obligación internacional de garantizar los derechos humanos básicos por todos los medios legítimos (legislación, aplicación de la ley, entre otros).

Bajo el anterior entendido, el derecho a la privacidad es una de las áreas fundamentales de los derechos humanos. Asimismo, el derecho a la privacidad o el derecho a tener un área autónoma para nuestra vida puede ser descrito usando términos diferentes, por ejemplo, el 'derecho a elegir' o 'el derecho a la libertad de desplazamiento'. No existe una lista particular de las actividades que definen los límites de la vida privada (es decir, la intimidad), la cual viene siendo un espectro de la libertad. Por ende, el contenido del derecho a la privacidad (el derecho a la autonomía personal) es difícil de definir e identificar en la mayoría de los casos para los Estados, en especial, cuando hablamos del manejo de la información que cada uno de nosotros producimos.

Por tanto, el problema jurídico en torno al cual giró el presente trabajo de grado fue el siguiente: *¿Por qué el Dataverse y la vigilancia de la información se pueden legitimar por medio del derecho a la privacidad, a través de un estudio de caso: Colombia a partir del 2010 y el estado del arte del derecho a la privacidad en el mundo?*

3.1. Preguntas orientadoras

¿Cuáles son los elementos característicos del derecho a la privacidad?

¿Qué tipo de relación existe entre el derecho a la privacidad y la vigilancia?

¿Qué es el *Dataverse* y es posible su control por parte de las entidades estatales?

¿Cuál es la relación del derecho a la privacidad con el sector público y privado?

¿Cuáles son las consideraciones de la Corte Constitucional, respecto al derecho a la privacidad?

¿Cómo es regulado el derecho a la privacidad a nivel internacional y nacional?

4. JUSTIFICACIÓN

Interés:

Las preocupaciones sobre la seguridad nacional y la actividad criminal pueden justificar el uso excepcional de las tecnologías de vigilancia sobre las comunicaciones. Sin embargo, las leyes nacionales que regulan lo que constituiría la implicación necesaria, legítima y proporcional del Estado en este tipo de vigilancia son a menudo insuficientes o inexistentes. Los marcos jurídicos nacionales son inadecuados[8] y crean un terreno fértil para las infracciones arbitrarias e ilegales del derecho a la privacidad en las comunicaciones, como lo vimos en Colombia por el caso de las interceptaciones del DAS. Por tanto, el interés de este trabajo de grado radica en el impacto que puede tener la implementación de la vigilancia y el uso de la información por parte del Estado y del sector privado sobre el derecho a la privacidad.

Además, el desarrollo de la normativa internacional y nacional sobre el derecho a la privacidad se hace cada vez más importante debido al gran impacto que puede causar el uso de la información del *Dataverse* sobre la sociedad civil, lo que conlleva a generar injusticias, debido al uso inadecuado de la información recolectada y almacenada.

[8] Las nuevas tecnologías avanzan a pasos agigantados, mientras que los marcos jurídicos son de lenta evolución, por lo que quedan rezagados frente a nuevas situaciones, por ejemplo, en muchos Estados, las leyes no regulan los cibercafés, lo anterior es particularmente problemático para los países donde la propiedad de computadoras personales es baja y las personas confían en gran medida en las computadoras de acceso público. Así las cosas, "las nuevas tecnologías de información han dado un giro a las relaciones humanas dentro de la sociedad. El mundo contemporáneo se caracteriza por una producción, una circulación y un consumo de informaciones sin precedente. Efectivamente, el consumo de las informaciones de toda índole se ha vuelto esencial para nuestra vida diaria" (Celis, 2006, p. 79-80).

Novedad:

La novedad que presenta este trabajo de grado reside en que hoy en día en Colombia, no hay una ley que regule el uso de la información, tan solo se han llevado a cabo una serie de sentencias por parte de la Corte Constitucional sobre este tema, entre ellas encontramos las siguientes: T-414 de 1992, T-1202 de 2000, T-437 de 2004; por lo que el enfoque del derecho a la privacidad y su relación con la vigilancia a la luz de los derechos humanos y de la normativa internacional es novedoso, ya que siempre han sido vistos como contradictorios, mientras que nosotros los presentamos como complementos el uno del otro, así este modelo podría ser implementado a nivel nacional, dando un paso hacia la praxis desde lo teórico.

Utilidad:

Este proyecto es importante para la comunidad académica del Programa de Derecho de la Universidad de Manizales, porque se enfoca en la realización de un estudio que permitirá describir y analizar las normativas internacionales de mayor relevancia sobre el derecho a la privacidad y su relación con la vigilancia y el uso de la información. Así las cosas, el presente estudio ayudará a determinar los posibles efectos y tendencias normativas al respecto.

Por tanto, este trabajo de grado le aporta a la comunidad académica al ser construido de manera teórico-práctica, por tal motivo, servirá de base para futuros estudiantes o personas interesadas en el tema permitiéndoles, a su vez, tener claro el proceso de convergencia que se está llevando a cabo a nivel mundial sobre el manejo de la información y su relación con el derecho a la privacidad.

5. OBJETIVO GENERAL

- Analizar las implicaciones sobre la vigilancia de las comunicaciones, almacenamiento de la información y los datos, por parte del Estado colombiano y el sector privado para el ejercicio del derecho humano a la privacidad.

5.1. Objetivos específicos

- Describir la realidad que hoy circunda el *Dataverse*.

- Analizar las posibilidades con las que cuenta el derecho internacional sobre el derecho a la privacidad.

- Presentar cómo ha sido utilizada de manera arbitraria la información almacenada en el *Dataverse* por parte del sector público y del sector privado en Colombia.

6. METODOLOGÍA

El presente proyecto de investigación utiliza una metodología correlacional, la cual analiza la covariación de dos o más variables. Por ejemplo, en nuestro caso se examinará la covariación de la vigilancia de la información en el *Dataverse* y su influencia en el derecho a la privacidad. Así pues, la investigación correlacional se puede lograr mediante una variedad de técnicas que incluyen la recolección de datos empíricos, así como los análisis estadísticos de correlación y regresión, incluyendo además los análisis multivariados para muestras categóricas. Muchas veces, la investigación correlacional se considera como aquella donde el observador no manipula la información. Asimismo, el investigador solo recoge los datos de las dos variables sin ser controladas o afectadas por él.

Es importante destacar que la investigación correlacional no es una investigación de tipo causal, por eso, hay dos razones principales por las que no podemos hacer declaraciones de causa y efecto, en primer lugar, no sabemos la dirección de la causa y, en segundo lugar, la participación de una tercera variable de la que no somos conscientes, pero que puede afectar el resultado final de la investigación.

6.1. Tipo de investigación

Todo trabajo de investigación debe tener en cuenta el contexto donde se va a realizar, ya que allí existen múltiples variables e influencias que debemos analizar a la hora de obtener una respuesta adecuada a la pregunta problema, entonces, si queremos determinar el impacto de la vigilancia de la información en el *Dataverse* en el derecho a la privacidad, debemos llevar a cabo un proceso de integración y síntesis del análisis de la información respecto a este tema de investigación. Por tal motivo, este proyecto es de tipo correlacional

debido a que va más allá de una simple lectura y descripción de conceptos, por eso, se analizará el contenido del derecho a la privacidad a la luz de la normativa nacional e internacional, con el fin de encontrar un control a la información obtenida en el *Dataverse*, por parte de los diferentes sectores.

6.2. Método

Con base en el tipo de investigación referenciado, el método a utilizar en el presente proyecto es de carácter hermenéutico, así podremos conocer y articular lo que generalmente pasa desapercibido a simple vista y poder encontrar una solución al problema planteado de una manera más profunda.

6.3. Fuentes de información primaria y secundaria

En un rastreo inicial del tema, se logró una primera recolección bibliográfica que llevó a una investigación más específica de las principales fuentes teóricas y normativas. A partir de esta recolección bibliográfica y su posterior lectura, se hizo un análisis correlacional e interpretativo de los conceptos básicos, entre ellos el derecho a la privacidad, así como dichos conceptos son aplicados al tema en cuestión, a saber, la vigilancia de la información localizada en Internet y el *Dataverse*.

6.4. Técnicas e instrumentos de recolección de información

La información se analizó a través de referencias bibliográficas, normativas y jurisprudenciales, ya que estas son las fuentes directas del marco teórico y conceptual del presente trabajo de investigación. Además, realizamos los resúmenes analíticos correspond

6.4.1. Fases de la investigación

Después de tener claridad sobre el problema a desarrollar y la metodología a utilizar se emplearon las siguientes fases:

***Fase 1*:** exploración teórica, normativa y jurisprudencial, y su respectivo análisis.

***Fase 2*:** con posterioridad, realizamos la sistematización e interpretación de la información dentro del marco del problema planteado.

***Fase 3*:** informe final, que incluye las conclusiones respectivas.

6.5. Sistematización de la información

La información recolectada y analizada en las fases anteriores fue debidamente sistematizada para llegar a las conclusiones respectivas. En la fase correlacional e interpretativa se analizó y clasificó de acuerdo con su importancia dentro del trabajo de investigación.

6.6. Resultados esperados

Los resultados del presente proyecto de investigación, ayudarán a la consolidación y orientación del derecho a la privacidad y su relación con la vigilancia de la información en Internet y el *Dataverse*, lo cual podrá ser sometido al debate académico con posterioridad.

7. CRONOGRAMA

Después de exponer el desarrollo metodológico en el que este trabajo de grado fue realizado, es necesario establecer la línea de tiempo en la cual este proyecto se llevó a cabo, a saber:

		MESES					
		1	2	3	4	5	6
FASES	Exploración teórica, normativa y jurisprudencial, y su respectivo análisis.						
	Sistematización e interpretación de la información dentro del marco del problema planteado.						
	Informe final, que incluirá las conclusiones respectivas.						
	Presentación de los resultados alcanzados.						

8. RESULTADOS ALCANZADOS

CAPÍTULO I

EN BUSCA DEL DERECHO A LA 'PRIVACIDAD DE LA INFORMACIÓN', DEBIDO A LAS NUEVAS AMENAZAS TECNOLÓGICAS

Es apenas novedoso decir que Internet plantea una grave amenaza para la privacidad de la información. Durante años, los académicos y teóricos han predicho la llegada del denominado 'Gran Hermano'[9], advirtiendo que el gran temor planteado por George Orwell, en su novela de ficción *1984*, acerca de un Estado de vigilancia se había convertido o, por lo menos, se acercaba a la realidad. Algunos, como Matthew Bunker han expuesto que la metáfora acerca del problema de la privacidad en Internet realmente debe plantearse de otra manera, es decir, la recopilación y difusión de la información por parte de las empresas privadas, refiriéndose a ello como la amenaza del 'Little Brother'[10].

De hecho, los problemas acerca de la intimidad han llevado a Margaret Ann Irving a comparar Internet con un Estado totalitarista que rivaliza con los de Hitler y Stalin. A pesar de que son simples metáforas, la amenaza es muy real. Ya que todo lo que hacemos en Internet está lejos de ser privado. Por ejemplo, el decano de la Escuela de Teología de

[9] Orwell predice un futuro en el que el 'Gran Hermano' es el gobierno omnipresente y omnisciente. El 'Gran Hermano' mantiene el control sobre la mente de la población a través de un uso asfixiante de la tecnología de vigilancia. Hay cámaras ocultas y micrófonos por todas partes, incluso una telepantalla en la casa de cada ciudadano.

[10] Bunker ha adaptado esta metáfora para describir la amenaza a la privacidad causada por las bases de datos del sector privado, a menudo refiriéndose a dichas entidades como 'Little Brother'. Esto no quiere decir que el 'Gran Hermano' no represente una amenaza para la privacidad.

Harvard se vio obligado a dimitir después de que se descubrió que había descargado pornografía en su ordenador personal. Mientras tanto, se ha demostrado cómo los proveedores de servicios de Internet podrían ser los eslabones débiles de la cadena de la vida privada.

Efectivamente, el proveedor de servicios de Internet NetZero afirmaba: "un público que conocemos íntimamente, ya que nos permiten seguir a donde quiera que vayan por Internet" (Litman, 2000, p. 1283). Al igual que el consejero delegado de Sun Microsystems (hoy Oracle Corporation, productor del famoso JavaScript), ha sido citado en reiteradas ocasiones por decir: "ustedes tienen cero privacidad. Terminemos con eso ya" (Froomkin, 2000, p. 1462).

Así las cosas, el público es muy consciente de la amenaza de Internet para la privacidad informacional. De acuerdo con una encuesta realizada por las Naciones Unidas el 92% de los estadounidenses están preocupados por las amenazas a su privacidad personal al usar Internet, mientras que el 72% de los europeos afirman estar muy preocupados[11]. El mercado ha respondido a la creciente preocupación de la opinión pública mediante el desarrollo de tecnologías potenciadoras de la privacidad (PET por sus siglas en inglés), programas que pretenden permitir a los consumidores navegar en secreto. Aunque el Internet entró en uso de forma popular hace más de diez años, no es poco común hoy en día proclamar que Internet es una seria amenaza para la privacidad informacional.

[11] Los datos presentados se basan en la encuesta realizada por el Human Rights Council de las Naciones Unidas, sobre la percepción de seguridad en Internet en Estados Unidos y la Unión Europea. Tomado de: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* de 2012.

Lo que sigue siendo una novela, sin embargo, es el argumento a favor de un derecho que proteja nuestra privacidad en Internet. Tan solo unos pocos estudiosos, como Overton y Giddings, prenden las alarmas sobre la necesidad de un derecho más específico con respecto al uso de la Web. Del mismo modo, solo un pequeño número de comentaristas, entre ellos Ken Gormley, recomiendan la protección de todo Estado constitucional al derecho a la privacidad informacional. Así pues, la mayoría de los teóricos han citado al derecho como la única posible solución a la creciente amenaza tecnológica a la privacidad de la información, ya sea calificándolo como débil —o, presumiblemente, incapaz de modificar la situación—, o sea sosteniendo que las constituciones no están preparadas para protegernos contra las tecnologías que destruyen la privacidad. No obstante, el debate sobre la privacidad de la información en Internet, en particular, oscila entre: (i) la autorregulación del sector y (ii) la legislación del gobierno; aunque en los últimos años ha aumentado el apoyo para otras soluciones, como la vinculación del derecho a la intimidad como un derecho de propiedad o la ampliación de los agravios a la privacidad.

En este capítulo discutiremos cómo el derecho a la privacidad informacional es necesario para la protección de la privacidad en Internet. Por otra parte, teniendo en cuenta los avances que ya se han hecho y su receptividad a la experimentación, las constituciones de los Estados son y deben seguir siendo la base de pruebas para un derecho constitucional de la intimidad en Internet.

Asimismo, expondremos la amenaza que representa Internet y las computadoras, la definición de los contornos y la tecnología informática para la privacidad de la información. Además, de centrarnos menos en el aspecto de la divulgación y más en la difusión y uso de la información personal.

Finalmente, señalamos que la privacidad en línea es el aspecto más importante de la preocupación por el derecho a la intimidad hoy en día. Por tal motivo, argumentamos que Internet ha creado la necesidad de un derecho más constitucional mediante la elevación de la privacidad de la información a una preocupación generalizada. Examinando el fracaso del actual régimen jurídico, no constitucional, para enfrentar la amenaza de Internet. El derecho ha sido poco utilizado para controlar Internet, por lo que la falta de un 'interés generalizado' en la intimidad es una de las razones de la debilidad actual, por ello Internet ha cambiado el interés por la privacidad de la información de tal manera que la protección constitucional es necesaria y, además, inmediata.

1. Internet, una verdadera amenaza a la privacidad

Mientras que el Internet ha tenido un uso popular desde hace más o menos unos 10 años, la noción de que los ordenadores en general podrían causar pérdidas no deseadas de privacidad de la información ha sido establecida recientemente, los grandes avances tecnológicos han dado el salto a una 'era de la comunicación', donde la información es el elemento vital que sustenta las decisiones políticas, sociales y económicas. Por ejemplo, en 2007, más de 1550 empresas tenían 'información' como su producto.

En una especie de debate sobre quien fue primero el huevo o la gallina, algunos comentaristas, como Anne W. Branscomb, sostienen que la tecnología ha transformado la naturaleza misma de la información y ha hecho que sea más valiosa, mientras que otros creen que la tecnología simplemente ha hecho que la información previamente valiosa sea más atractiva para el mercado. No obstante, está claro que la información personal, se encuentra ahora en una mayor demanda como nunca antes se había visto. Sin embargo, la tecnología informática y la digitalización en particular, han reducido el costo y el espacio

necesario para el aumento de la velocidad de almacenamiento y transferencia, lo que resulta en una mayor difusión de la recolección y comercialización de la información.

El Internet se encuentra en la encrucijada de la preocupación por el efecto de las computadoras en la privacidad informacional y la necesidad exponencial de información. Es al mismo tiempo el equipo más grande del mundo y el espacio comercial más eficiente[12]. El hecho de que Internet supone una amenaza debe estar por fuera de toda duda. Sin embargo, muchos buscan consuelo en la idea de que, como peones sin importancia y sin un perfil público, "[la] información personal no es de suficiente interés para ser recogida, compilada o correlacionada por cualquier persona" (Litman, 2000, p. 1285).

En este capítulo trataremos de definir la privacidad informacional y precisar la amenaza planteada por las computadoras y el Internet, es decir, el *Dataverse*, para aquellos que tienen consuelo en este anonimato percibido, lo que además constituye la base necesaria para una discusión inteligente de una solución, en derecho, potencial de la amenaza a la privacidad de la información.

1.2. La privacidad de la información

Definir la privacidad de la información es una tarea vertiginosa. Como plantea Fred Cate,

[12] Internet es una colección suelta de millones de computadoras en todos los lugares del mundo, donde se comparte información. Miles y miles de redes locales se conectan con el software de comunicación, gestionando las comunicaciones entre ellos.

> […] para toda la pasión que rodea a la discusión acerca de la privacidad, y la reciente atención que se dedica a la privacidad electrónica, existe muy poco consenso en cuanto a lo que significa 'privacidad' (1997, 68).

Ya ha pasado un buen tiempo desde que Cate escribió esto, no obstante, las definiciones han hecho todo menos converger. El problema de fondo parece ser que la 'privacidad' es un concepto demasiado amplio y que la privacidad de la información no es más que una mera parte de un conjunto más grande. Esto plantea dos cuestiones distintas. En primer lugar, no existe un consenso sobre los intereses que conforman la vida privada. Por ejemplo, Jerry Kang describe tres 'cluster'[13] sobre la confidencialidad con respecto a: (i) el espacio físico (privacidad espacial); (ii) elección; y (iii) el flujo de información personal.

Sin embargo, Allen-Castellitto divide a la privacidad en al menos cuatro tipos básicos: (i) la privacidad de la información; (ii) la intimidad física; (iii) la intimidad decisional; y (iv) la privacidad propiamente dicha. Mientras tanto, los padres del derecho a la intimidad, Samuel Warren y Louis Brandeis, describen un,

> derecho general a la privacidad de los pensamientos, emociones y sensaciones [que] deben recibir la misma protección, ya sea expresado por escrito, o en la conducta, en la conversación, en las actitudes o en la expresión facial (1890, p. 26).

[13] "Los métodos de análisis de grupos clasifican grupos de casos o elementos, en base a criterios cualitativos o cuantitativos (distancias o similaridades). A veces, en lugar de los casos, se forman grupos con las variables […] El análisis de grupos (cluster) […] se define mediante el cálculo de distancias o similaridades, a partir de los valores de algunas variables que se consideran adecuadas para ello" (Álvarez, 1994, p. 203).

En segundo lugar, la segmentación de uno de estos tipos bajo el subtítulo ‘privacidad de la información’ es difícil, ya que cada uno de ellos esta interconectado. Cualquier definición parece, en el mejor de los casos, discutible y, en el peor, arbitraria. Por ende, trataremos de encontrar ya sea un punto medio o el mínimo común denominador en la teoría que abarcará los menos disputados y, por tanto, más esenciales elementos de la privacidad informacional.

Así pues, en la búsqueda de una definición de privacidad de la información, es útil comenzar con el caso más referente en esta materia, el caso de la Corte Suprema de los Estados Unidos *Whalen vs. Roe*. En el caso *Whalen*, la Corte separó el derecho a la privacidad en al menos dos intereses: (i) el interés individual en evitar la revelación de asuntos personales y (ii) el interés por la independencia en la toma de ciertos tipos de decisiones importantes.

El control de la divulgación de asuntos personales ha sido ampliamente reconocido como la definición de la Corte Suprema de privacidad informacional. La gran mayoría de teóricos han adoptado una definición muy similar, a saber, la conceptualización de intimidad de la comunicación como un derecho a controlar el flujo de datos personales.

Sin embargo, un relativamente nuevo grupo encabezado por Paul Schwartz ha comenzado a criticar la definición de intimidad como control. Ya que en el ‘control absoluto’ sobre la información personal de cada uno parece lógico incluir la capacidad unilateral de renunciar a dicho control. Como resultado, la definición de privacidad informacional, es decir, de privacidad como control, se interpreta con frecuencia como un derecho de propiedad personal de cada uno sobre su propia información.

Los críticos, en especial Allen, argumentan que dicha visión no puede proteger a la intimidad mediante la creación de incentivos inapropiados e inadecuados. Más fundamentalmente, aquello que permite la 'administración individual' de la comunicación personal en Internet (o el *Dataverse*) no tiene en cuenta los costos de transacción, las asimetrías de la información o la racionalidad limitada frente a los consumidores.

Así pues, Paul Schwartz y Daniel Solove ofrecen teorías competidoras acerca de lo que es privacidad de la información. En lugar de, como control de la divulgación, Schwartz la concibe como un 'valor constitutivo'. Mientras que Solove también evita la concepción que lo ve estrictamente como un derecho de control individual. Más bien, él ve a la privacidad informacional como un derecho a que la propia información sea 'tratada cuidadosamente' para entender las revelaciones de los datos personales de cada uno y para participar de manera significativa en el uso de ellos.

Así que el hilo conductor aquí es que los problemas de la privacidad de la información, entendida como 'información personal', por lo general, abarquen cualquier tipo de dato que sea identificable por cualquier individuo en cualquier momento y lugar.

Esto incluye tanto datos asignados, tales como nombre, dirección y la información que se genera, por ejemplo, registros financieros o de tarjetas de crédito, registros médicos y registros telefónicos. A los efectos del presente trabajo de grado, la comunicación personal se define como cualquier información, no importa lo trivial, que pueda ser rastreada o vinculada a un individuo identificable. Además de este componente de la información personal, las concepciones anteriores de privacidad informacional centran sus preocupaciones en las consecuencias tanto reales como percibidas de la divulgación. Es decir, no solo que los datos hayan sido revelados, sino que también sean utilizados en muchos aspectos no deseados e inesperados. Por ejemplo, una parte esencial de la

definición de la vida privada como control es que las subvenciones de control absoluto nos dan la autonomía y la capacidad de determinar cuáles son los datos que queremos divulgar de sí mismos.

> El control de privacidad pretende lograr la autodeterminación informativa a través de la administración del individuo de los datos de carácter personal, manteniendo la información aislada de cualquier acceso (Schwartz, 2000, p. 820).

Mientras tanto, y en esto tiene razón Solove, ser 'tratado cuidadosamente' surge de una preocupación por los usos y prácticas asociadas a nuestra comunicación. Por último, el 'valor constitutivo' de Schwartz también se eleva desde el reconocimiento de que "el acceso a la información personal y sus límites ayudan […] a formar nuestras identidades individuales" (2000, p. 834).

No obstante, estas definiciones difieren principalmente en la forma en que hacen frente a las consecuencias de la divulgación. A cierto nivel, sin embargo, todos ellos parecen apuntar a la queja de Solove, que las tecnologías informáticas se parecen a lo planteado por Kafka en *El proceso,* a saber, una vez que se haya revelado la información, esta se usa y se abusa sin ningún sentido, propósito o razón. Por tanto, los defensores como control de la privacidad quieren devolver el control al individuo; Solove busca restaurar el sentido de que la propia información debe ser 'tratada cuidadosamente' y Schwartz espera acorralar a la utilización de los datos en la construcción de la norma mediante la definición clara de los denominados 'territorios informacionales'.

Así pues, el mínimo común denominador del que hablábamos es el deseo de tener a la información de cada uno tratada con un objetivo comprensible. Superficialmente, esto puede empezar a sonar muy parecido a la privacidad como control. Incluso Solove afirma: "tal vez la idea más adecuada de la privacidad de las bases de datos es la de control de la información personal" (2001, p. 1445).

Sin embargo, él también va a decir que,

> [aunque] los teóricos que ven a la privacidad como control sobre la información a menudo lo entienden en el marco de la propiedad y el concepto de los contratos […] esta no es la única manera en la que el control se puede entender (Ibíd. p. 1446).

Se trata de un control de la información personal, en la medida en que alguien define las consecuencias de la divulgación, pero ciertamente no es el 'derecho de control' que Schwartz, Solove y otros rechazan rotundamente. Se basa en un sentido de la autonomía de la decisión que es mucho menos literal que la simple capacidad de regular la válvula de cierre de los datos personales de cada uno. No es control, *per se*, más bien, no es una falta de control. Un individuo no está necesariamente relacionado con el control directo de su información personal, pero debería, por lo menos, estar enterado sobre los límites y parámetros dentro de los cuales ésta, una vez divulgada, puede ser utilizada. Por tanto, privacidad de la información es un derecho en la medida en que entendemos las consecuencias reales y percibidas de la divulgación de nuestra información personal.

1.3. Todos podríamos estar siendo vigilados

Como una situación multi-afrontada, la amenaza a la privacidad de la información que representan las armas tecnológicas disponibles en las computadoras e Internet parece tan amplia como la definición de la privacidad informacional.

Gran parte de la tecnología, sin embargo, se centra en la recopilación y como tal, es decir, en sentido estricto, una amenaza directa solo de divulgaciones injustificables. Como ya lo hemos definido, privacidad de la información no se refiere a la divulgación injustificada.

La verdadera amenaza para la privacidad de la información surge de las tecnologías que se ponen en uso una vez que la información ha sido recolectada[14]. Esto reduce la amenaza tecnológica a una fuente principal: las bases de datos informáticas. La información digitalizada es más fácil de manipular, analizar y sintetizar, transmitir y almacenar, al igual que de usar y abusar sin un sentido, propósito o razón.

Las bases de datos informáticas almacenan, ordenan y procesan las comunicaciones de una manera tal que trasciende tanto las restricciones temporales y espaciales. Almacenada en una base de datos, la información una vez valiosa solo en tiempo real se puede compilar para reconstruir el pasado, descifrar los patrones y servir como evidencia. Como lo ha dicho Froomkin, "las bases de datos multiplican los efectos de [en tiempo real] los sensores" (2000, p. 1468). Ahora, la llegada de Internet ha multiplicado los efectos de las bases de datos, ya que une a cientos y miles de estas en una base a escala mundial.

[14] Por supuesto, la recolección y recopilación de la información, especialmente la que se hace de manera furtiva y a gran escala, contribuye y agrava la amenaza a la privacidad de la información. De hecho, la mayor parte de los datos recopilados a través de Internet facilita las transferencias secundarias y diversos usos para aumentar el potencial de consecuencias de la divulgación.

Tal vez la mayor amenaza planteada por las bases de datos informáticas es la destrucción de la 'oscuridad práctica', a veces referida como el anonimato a través de la oscuridad. Anteriormente, las restricciones físicas de tiempo y espacio impedían las violaciones graves a la privacidad de la información. Por ejemplo, los registros en papel a menudo se presentan en numerosos lugares, son fáciles de extraviar o destruir de manera permanente y se requiere una gran cantidad de esfuerzo para recopilar y ordenar sus datos. Además, incluso a pesar de los mejores esfuerzos por tener una colección completa de los registros en papel, probablemente, dicha colección seguiría estando incompleta. No obstante, las bases de datos informáticas cambiaron esto con su capacidad para almacenar, buscar y ordenar grandes volúmenes en cortos períodos de tiempo. Y mientras que la dispersión de la información a lo largo de numerosas bases de datos informáticas había conservado cierta 'oscuridad práctica', Internet ha eliminado casi por completo los restos de este aislamiento.

Un corolario a la destrucción de la 'oscuridad práctica' es el uso de bases de datos para la fabricación de perfiles de identidad. Estas pueden ser fácilmente exploradas y, a su vez, cruzadas sus referencias para reunir grandes cantidades en el tiempo real de un individuo en particular. El perfil resultante es, probablemente, mucho más amplio y con información que incluso el propietario tenía la intención de no divulgar. Esto ha sido denominado como la 'Teoría Mosaic': la suma de una serie de bits de información es exponencialmente más valiosa que cada bit individual. De hecho, Patricia Mell ha señalado, "una vez que la persona se ha registrado alcanza más credibilidad que como individuo" (1996, p. 11).

El problema se agrava por el hecho de que estas bases de datos que contienen tanto los datos brutos y los perfiles de los consumidores son cada vez más sofisticados en la venta de información, por lo general, sin el conocimiento de los consumidores. Se ha demostrado que los datos personales de un individuo pueden ser transferidos a más de cinco ordenadores en un solo día. Como resultado, las bases de datos de los ordenadores e

Internet han aumentado significativamente el acceso y la facilidad de acceso a la información.

Muchas agencias gubernamentales tienen bases informatizadas, que han sido recientemente vinculadas a Internet y entre sí. Al igual que las empresas privadas, algunas agencias gubernamentales han comenzado a interrogar a otras bases de datos de referencia para crear perfiles de ciudadanos. De igual forma las bases privadas también han surgido y se publican con frecuencia en Internet. Por lo que las búsquedas en Internet ahora pueden revelar un conocimiento superficial de la información con relativamente poco tiempo y esfuerzo[15].

Las capacidades de almacenamiento de las bases de datos informáticas, así como su precisión y seguridad cuestionable, generan preocupaciones adicionales sobre la privacidad. En especial, debido a que la información digital tiene una vida verdaderamente infinita. Como resultado, puede resurgir en cualquier momento, a pesar de que nuestra vida puede haber cambiado y que la información en particular puede no ser válida. Asimismo, los datos inexactos pueden almacenarse con la misma facilidad que una información precisa, por lo que las violaciones de seguridad, ya sean accidentales o por piratas informáticos deberían ser preocupaciones muy reales para cada uno de nosotros.

[15] Overton comenta que fue capaz de obtener a través de Internet la siguiente información acerca de Giddings en menos de diez minutos: su nombre completo, su número de teléfono, la dirección de su residencia en Tallahassee, su fecha de nacimiento y su número de seguro social; la misma información, pero de su esposa; además del ingreso medio de su barrio, el valor mediano de las casas de su barrio, los nombres de diez de sus vecinos más cercanos (incluyendo sus direcciones y números de teléfono). Giddings, confirmó que toda la información era correcta. De hecho, hoy en día todo tipo de información se puede encontrar en Internet, incluyendo registros de vehículos, información de crédito, para nombrar unos pocos ejemplos (cf. Overton & Giddings, 1997).

1.3.1. Tecnologías para recolección y recopilación de la información

Aunque las tecnologías de recopilación no son una amenaza directa a la privacidad de la información, merecen una breve consideración, ya que estas proporcionan los cimientos para las bases de datos. Si no hay ninguna divulgación, no puede haber ninguna coacción a la privacidad. De hecho, entre más insidiosa y generalizada sean las tecnologías de recopilación de la información, mayor puede ser la amenaza para la privacidad informacional. Estas tecnologías, por tanto, valen la pena de ser discutidas, aunque solamente sea para comprender cuán dominante es en realidad la amenaza. La información recopilada a través de Internet (o el *Dataverse*) se puede agrupar en dos categorías: (i) la que se da a conocer de forma voluntaria y (ii) la que se divulga involuntariamente. Ambas categorizaciones pueden contribuir a generar un problema. Sin embargo, las revelaciones voluntarias a menudo llevan a las violaciones más insidiosas debido a que la información se presenta, por lo general, con la creencia errónea de que se limita a los fines para los cuales se está dando. Por ejemplo, muchas revelaciones voluntarias se producen a través de las páginas de registro, inscripciones y hojas de pedido. En estos casos, los usuarios a menudo darán datos personales importantes, como su nombre y dirección, con la creencia de que están siendo recopilados solamente para un propósito específico, como el envío de su compra. Esto es con frecuencia falso. Los grupos y blogs son otra fuente de información voluntaria. Estos usuarios probablemente no creen o realmente no se dan cuenta de que sus comentarios se conservarán y pueden llegar a ser distribuidos. Los creadores de páginas Web se incluyen en esta misma categoría.

Las divulgaciones involuntarias en Internet, por lo general, implican algún tipo de seguimiento subrepticio. Los dos métodos más discutidos son la recopilación de datos de navegación y el uso de cookies[16]. Datos de clics es el nombre genérico que se da a la

[16] Más bien, las cookies se asemejan a las bases de datos, ya que facilitan la recopilación de información intertemporal por parte de otras tecnologías, como la supervisión de clics. De hecho, en su publicidad las

información que un sitio Web puede llegar a conocer acerca de un usuario, simplemente porque el usuario ha navegado por dicho sitio, ya que el acceso a este revela la dirección del usuario TCP/IP, el tipo de ordenador y el navegador utilizado y la información limitada acerca de la actividad de navegación (en particular, la fecha y hora de acceso y la dirección de Internet del sitio Web de referencia). Con un pequeño esfuerzo, el sitio puede registrar clics del usuario, lo cual revelará la mayor actividad de exploración detallada, tales como el orden de las páginas visitadas y el tiempo empleado en cada una. Lo anterior es una seria amenaza a la privacidad de la información, ya que hay varias formas en que se puede localizar a un individuo identificable. En primer lugar, un sitio puede requerir el registro de log-in. En segundo lugar, la dirección TCP/IP se puede utilizar para rastrear la información personal de un usuario. En tercer lugar, un sitio Web puede depositar una cookie en el disco duro del usuario, la cual se utiliza para identificar al usuario en una nueva visita.

Las cookies son archivos en los sitios Web que registran los datos que han reunido a partir de cierta información de los usuarios, ya sea voluntaria o involuntariamente revelada y puede ser la forma más insidiosa de recopilación. Un número de otras revelaciones involuntarias por Internet deben ser mencionadas. Por ejemplo, una marca de agua digital permite a los dueños de propiedad intelectual hacer un seguimiento de los documentos. Del mismo modo, el Office de Microsoft etiqueta rutinariamente cada documento con un número de identificación. James Sunosky afirma que el JavaScript en el navegador le permite a los sitios Web recopilar datos en tiempo real sobre las actividades de los visitantes y examinar, a su vez, el directorio del disco duro del visitante.

---

empresas han comenzado a utilizar cookies (o GIF a veces transparentes) como identificadores únicos que les permiten rastrear a los usuarios de sitio en sitio. Cada vez que se hace clic en un anuncio, una cookie se envía al usuario por el proveedor del anuncio, mientras que el usuario se dirige al sitio web de la compañía anunciada.

Mientras tanto, Intel ha incorporado en cada uno de sus Pentium un número único de identificación que, cuando funciona, puede ser accesible a los navegadores Web. Por último, el IPv6, el sucesor del sistema de dirección actual IP, de forma permanente podría incrustar una dirección IP en todos los dispositivos que se pueden conectar a Internet.

1.4. La gran amenaza de Internet y el *Dataverse*

A pesar de que la privacidad de la información abarca una amplia gama de cuestiones. Nos centramos en Internet (específicamente en su relación con el *Dataverse*), ya que es la mayor amenaza que existe hoy en día. Internet fue básicamente diseñada para la recopilación. Las encuestas han encontrado que más del 90% de los sitios Web recopilan cierta información personal. Por otra parte, el uso de Internet como una herramienta para la comunicación, la educación, ir de compras, la banca y para la vida en general, está creciendo y seguirá creciendo. De hecho, el acceso a Internet probablemente se convierta en algo inevitable e indispensable[17]. Por encima de todo, hay corporaciones, agencias y personas que son capaces de procesar toda la información que Internet recoge. En pocas palabras, Internet es la base de datos de computadoras más grande que nunca hayamos visto, con una memoria casi infinita y el acceso a, posiblemente, el más grande banco (casi interminable) de información en el mundo.

Las consecuencias reales y percibidas de la divulgación de la información personal son alucinantes. Sin embargo, ha tomado algún tiempo para que esta toma de conciencia se abra paso dentro del público en general, pero las personas han comenzado a entrar en razón.

[17] El aumento exponencial en la potencia de los procesadores y el descenso dramático en el tamaño físico y en el precio de las computadoras han creado un ciclo frenético en el cual los individuos y las organizaciones utilizan cada vez más a los ordenadores, generando un fenomenal crecimiento y una gran dependencia de los servicios de las computadoras, lo que resulta en una mayor demanda y uso.

Efectivamente, el tema de la privacidad en Internet ha sido un 'tema candente' recientemente para la diplomacia de las potencias mundiales, como es el caso de las acusaciones de Alemania a los Estados Unidos por la interceptación de las comunicaciones de la canciller germana Angela Merkel, al igual que del gobierno brasileño por la misma situación.

Hay indicios, también, que el público ha tomado conciencia de la amenaza específica que Internet plantea para la privacidad informacional. Así pues, la intimidad se ha convertido en la 'principal razón' para que muchas personas eviten dar cualquier tipo de información por Internet. De acuerdo con las Naciones Unidas y Pew Research Internet & American Life Project, 54% de los europeos y estadounidenses consideran el seguimiento en línea una invasión dañina de la privacidad. Lo más significativo en los últimos tiempos, es que ha habido un aumento de la actividad judicial en relación con las violaciones a la privacidad de la información en línea.

1.5. La necesidad de un nuevo derecho

El Internet y el *Dataverse* están creando un interés generalizado en la privacidad de la información y, en consecuencia, la necesidad de que el derecho a la privacidad informacional proporcione una protección real contra estos. A diferencia de las tecnologías anteriores, Internet y el *Dataverse* impregnan todos los aspectos de la vida. La información es 'oro', y como tal, se convertirá en una llave cada vez más necesaria a medida que más procesos y servicios se hayan automatizado e informatizado a un estado puro y en línea.

Por tanto, la colcha de retazos que es en la actualidad la protección de la privacidad de la información ya no es suficiente. Así pues, un interés extendido exige una protección más

popularizada. Más adelante, en el capítulo III, ampliaremos este argumento y demostraremos que un derecho constitucional mejor estructurado puede proveer dicha protección 'generalizada' mediante el establecimiento de una base firmemente arraigada que permita una mayor flexibilidad en el ámbito de aplicación. Asimismo, el derecho constitucional también abordará muchas de las justificaciones para otros métodos de protección de la privacidad informacional, evitando escollos más significativos para dichos métodos. No obstante, como trabajo preliminar, primero se debe demostrar la incapacidad de las leyes actuales para abordar adecuadamente la amenaza planteada por Internet y el *Dataverse* a la privacidad de la información.

1.5.1. El fracaso de las normativas actuales

Dado que la insuficiencia del régimen jurídico vigente en materia de privacidad en Internet es bien reconocida, por tanto, en este estudio nos referiremos de manera breve a la responsabilidad civil. De acuerdo con Rotenberg (2001) los agravios —o daños— a la intimidad se consideran en general la primera parada para la protección contra las intrusiones a la privacidad de los particulares. Estos se clasifican en cuatro reclamaciones relacionadas con: (i) la intrusión en la intimidad; (ii) la divulgación pública de hechos privados; (iii) la apropiación indebida del nombre y demás; y (iv) la publicidad que le proporciona a 'otro' una imagen falsa. Algunas de las particularidades hacen que el derecho de daños actual sea incapaz de proporcionar una mayor protección a la privacidad informacional en Internet y, en especial, el *Dataverse*. Para empezar, los agravios relacionados con Internet son difíciles de demostrar, ya que el consentimiento (que normalmente se proporciona en las transacciones por Internet) a menudo es la mejor defensa ante las reclamaciones de responsabilidad civil. Por ejemplo, para que una reclamación tenga éxito, en los tres primeros agravios, se requeriría que el demandante no estuviera al tanto de la recolección injustificada de sus datos, así como no poder prever dicha recolección. El usuario medio de Internet estaría en apuros para hacer tal afirmación.

Además, los agravios de privacidad tienden a exigir el cumplimiento de los altos estándares que una intrusión o divulgación debe tener para ser altamente ofensiva para una persona razonable. Por último, la protección del derecho de daños avanza lentamente, pero se retrae rápidamente. Esta cualidad hace que los agravios a la privacidad sean de difícil adaptación a las nuevas tecnologías, las cuales cambian rápidamente y se mantienen en un desarrollo constante. A primera vista, la intrusión parece que podría aplicarse a la recolección de información en Internet. Por ejemplo, las cookies se entrometen intencionalmente en la intimidad de otra persona. Sin embargo, tanto la interpretación amplia de la responsabilidad extracontractual de la voluntariedad como su estándar estrecho de altamente ofensivo para una persona razonable hacen que sea casi imposible o extremadamente difícil recurrir a dicha posibilidad. Al respecto, Helms señala que muchas personas son conscientes de las cookies y sus navegadores pueden configurarse para rechazarlas. Además, las cookies y otros recopiladores de información a menudo son de pequeña escala, y, por sí solas, sus intrusiones relativamente son inocuas.

Por último, muchas personas consideran que Internet es un lugar 'público', que está exento de responsabilidad extracontractual. En particular, los tribunales en diversas partes del mundo han rechazado esta teoría en los siguientes casos: la obtención de números de teléfono no listados; la venta de listas de suscripción para empresas de correo directo; y la recopilación y divulgación de la historia laboral de un individuo.

Por su parte, el daño causado por la divulgación pública de hechos privados requiere una divulgación de información privada que sea: (i) de amplia difusión; (ii) altamente ofensiva para una persona razonable; y (iii) que no sea 'noticia' o de 'legítima' preocupación para el público. Este agravio podría ser útil contra los perfiles en línea y los swaps de bases de datos que faciliten tales perfiles. Sin embargo, el estándar para 'amplia difusión' es difícil de cumplir. Las bases que se difunden ampliamente pueden ser consideradas registros públicos, lo que no es ilícito en virtud del hecho de agravio privado. Por el contrario, las

bases de datos que se venden a unos pocos grupos, aparentemente privados, se consideran a menudo de poca difusión. Asimismo, la información contenida en estas bases probablemente no sea considerada altamente ofensiva. De hecho, este agravio ha alcanzado históricamente ante los tribunales un éxito muy limitado.

La apropiación indebida de un nombre o imagen es mejor conocido por su uso para proteger el valor del nombre o la imagen de una persona famosa. Sin embargo, un perfil detallado también podría ser apropiado, debido a que estos perfiles son sin duda parte de la personalidad de la persona. Por tanto, las listas de distribución no deberían ser vendidas. Empero, no está claro que nombre o imagen equivalgan a personalidad. Y de nuevo, el consentimiento también podría ser un punto de fricción, ya que la mayoría de los usuarios de Internet de forma voluntaria o deliberada entregan gran parte de su información personal en la creación de sus perfiles. De hecho, todos los casos en que se ha invocado esta teoría para prohibir la venta directa de nombres y direcciones a empresas privadas han fallado.

El agravio en el último caso, el de la imagen falsa, se aplica cuando se da publicidad de alguien de una manera distorsionada, la cual es altamente ofensiva para una persona razonable, además de ser hecho con conocimiento o imprudencia temeraria en cuanto a la falsedad de la representación. Este agravio probablemente será generalmente inútil en el contexto del *Dataverse* y el ciberespacio porque los problemas de privacidad informacional casi siempre implican que la información es verdadera.

Las carencias de la ley de responsabilidad civil hace necesario el planteamiento de normativas alternativas que sean más atractivas. Muchas normas están diseñadas para tratar problemas específicos, pero lastimosamente hay muy pocas o ninguna que estén relacionadas con las nuevas tecnologías. Por tal motivo, las leyes actuales son ineficaces en cuanto a la privacidad en Internet y el *Dataverse*. Por tanto, antes de analizar las

implicaciones de un derecho constitucional de la privacidad de la información es necesario presentar la normativa internacional actual, basada en las categorías ofrecidas por los derechos humanos, respecto al derecho a la privacidad, con el fin de determinar si dicha normativa representa una solución satisfactoria al problema que traemos entre manos.

CAPÍTULO II

EL *DATAVERSE* FRENTE AL DERECHO A LA PRIVACIDAD EN EL MUNDO

2.1. El *Dataverse*, la autonomía y el derecho a la privacidad

Anteriormente vimos como la aparición del *Dataverse*, un universo amplio y creciente de recopilación, almacenamiento y difusión, ha provocado ansiedad de manera generalizada. En este orden de ideas, vimos como la privacidad se entiende generalmente en términos de control. No obstante, la expectativa parece cada vez más ilusoria e inalcanzable. Esto pone en tela de juicio el ideal de persona autónoma, en relación con uno de sus atributos principales, la intimidad.

Así las cosas, como todas las formas auténticas de los derechos y libertades, la propia autonomía también puede ser caracterizada como la unidad de tipos diferenciados y los grados de los factores internos y externos para un individuo determinado en un momento dado y en circunstancias particulares. Existen varias definiciones de autonomía. El término autonomía proviene del griego antiguo. Se compone de dos palabras: *autos* (propio) y *nomos* (regla). Este término describe la capacidad de una persona para establecer sus propias reglas en la vida para tomar decisiones de forma independiente. La idea de que las personas deben tener la libertad de dar forma a su vida es fundamental para la mayoría de teorías sobre la autonomía.

En general, cualquier acción o acto se puede describir como autónomo solo si el agente da preferencia a esta acción y dicha decisión es independiente y corresponde con su plan de

acción. En otras palabras, podemos hablar de autonomía, tan solo cuando la libertad de elegir y tomar decisiones éticas está garantizada.

Así, para Horowitz, la autonomía:

> [...] es el reconocimiento del derecho de una persona para mantener puntos de vista, de tomar decisiones y tomar acciones basadas en valores y creencias personales (2004, p. 30).

Esto se aplica tanto para el Estado como para los otros miembros de la sociedad: ningún miembro de la sociedad tiene el derecho de violar la autonomía personal de alguien sin una base razonable. Esta base razonable es la autonomía de otra persona, es decir, otro miembro de la sociedad. En el ámbito de la autonomía personal, una persona tiene todos los derechos y solo un deber: no violar la autonomía de los otros individuos. Esto, como lo veremos más adelante, incluye la no violación a la privacidad de los *otros*.

2.2. La privacidad a través de las fronteras

Sorprendentemente, los principales avances en materia de derecho a la privacidad de la información se refieren a una esquina muy específica del mundo: la parte tradicionalmente conocida como ‘occidente’. No obstante, los problemas a los que nos hemos venido refiriendo como Internet (incluido el *Dataverse*), la tecnología, las bases de datos, los derechos humanos, la vigilancia y la privacidad, no son tan geográficamente fáciles de delimitar.

Existen dos posibles razones para que esta situación se presente: (i) la historia de la vida privada y la tecnología es una historia más 'occidental' que ha sido contada y vuelta a contar en occidente desde hace varias generaciones, mucho antes de que se reorientara por la tecnología de la información; (ii) es 'occidental', porque la explosión de las tecnologías informáticas tiene su origen en los países de occidente y hasta hace poco se ha concentrado allí ―aunque esto ya no sea el caso―.

Esta brecha, empero, se ha estado reduciendo, ya que los problemas planteados en este trabajo de grado pueden llegar a ser problemáticos en otras partes del mundo, en parte, por razones relacionadas con la existencia de esta brecha. Esto se debe a que, por razones estructurales (tecnológicas, legales, históricas, políticas, económicas), podríamos esperar que la recolección y vigilancia de datos, estén siendo más invasivas y menos inhibidas por fuera de la tradición occidental, como es el caso de Rusia y China, por ejemplo.

Por otro lado, la brecha también es importante porque muchos de los argumentos y alegaciones que se suelen plantear en el debate sobre la privacidad frente a la tecnología tratan ubicaciones que son geográfica y fundamentalmente incidentales. Ya que consideran una relación entre las ideas, las ideologías y los procesos específicos (por ejemplo, de la participación tecnológica, de construcción de la identidad, de gobierno, entre otros), todos los cuales están hoy en día en circulación más allá de occidente. Por lo menos, en términos de disponibilidad, estas ideas, las ideologías y los procesos pueden hacer un reclamo sólido de universalidad, aunque está claro que ellos tienen más peso en algunos lugares que en otros.

Todo lo anterior, tiene su origen en un conjunto particular de hechos y circunstancias históricas y sociales. Su historia, a pesar de que circula a nivel mundial como una metáfora universal, siendo una narración de modernización que, en principio, podría tener parte en

cualquier lugar, también sigue siendo específica a su localidad. Precisamente, porque es tan fácil moverse a la universalidad en este ámbito, es importante darse cuenta de que, como cuestión de hecho, la ubicación no es casual: tanto la intensidad de Internet y el *Dataverse* varían dramáticamente de un lugar a otro.

La brecha importa por una tercera razón: porque es probable que se mantenga. Las extensiones más ambiciosas de Internet, y en particular del *Dataverse*, es poco probable que sean universalizadas, dada la extraordinaria intensidad tecnológica (y económica) que requieren y las numerosas restricciones al crecimiento de la economía mundial que podemos esperar en el futuro. Por ende, no es impensable que el dramático desequilibrio existente de la riqueza se traduzca en un mundo tecnológico de dos niveles, uno dominado por la autoexpresión tecno-cultural, el otro, por la vigilancia de datos generalizada.

En este trabajo no tratamos de llenar este vacío. Más bien, queremos sugerir algunas áreas de investigación. En primer lugar, mirar a la privacidad desde una perspectiva comparada. Esto allana el camino para un examen futuro, de algunos de los temores y amenazas aparentes que han surgido como consecuencia de los recientes acontecimientos históricos, jurídicos, económicos y tecnológicos.

2.2.1. El derecho a la privacidad en el derecho comparado

¿Es posible comparar las diferentes nociones de privacidad en todo el mundo? Una comparación tiende a presuponer dos objetos fijos. Sin embargo, una mirada superficial a la literatura acerca de la privacidad revela que aparentemente no goza de una significación indiscutible incluso en occidente. De hecho, como hemos visto, parece que está actualmente en proceso de una transformación sísmica y de una re-conceptualización. En

otras partes del mundo, podríamos esperar encontrar un número de diferentes nociones que comparten un 'aire de familia', al estilo wittgensteiniano, con algunas de las ideas centrales que asociamos con la intimidad (de hecho, esto es lo que encontramos). Pero también es esperable que estas nociones todavía se estén transformando, sobre todo en respuesta a la globalización de las ideas 'occidentales' acerca de la vida privada, así como sus normas culturales y las innovaciones tecnológicas, especialmente Internet.

Para complicar más las cosas, el intento de fijar las definiciones a efectos de comparación en sí conlleva serios peligros. Una comparación cultural siempre recae en una cosificación. Se tiende a tratar a los 'países', 'pueblos' o 'grupos étnicos' como 'unidades' culturales, cuando en realidad la 'cultura' en todas partes es bastante fluida. Así pues, un concepto como privacidad, el cual, en un entendimiento común, capta con precisión el espacio dentro del cual las personas se liberen de un determinismo cultural o cualquier forma de fijeza cultural parece particularmente fuera de lugar.

Dicho esto, el hecho de que tantos teóricos estén de acuerdo en la existencia de, por lo menos, dos tradiciones culturales y jurídicas occidentales distintas de privacidad, una europea y una tradición americana, proporciona una base para la comparación. Así pues, esta podrá ayudarnos a aislar lo que es más distintivo de las normativas. Al mismo tiempo, puede ser más productiva cuando se centra en datos interculturales fijos (como la vigilancia, la tecnología de la información, la protección de datos) en lugar de nociones nebulosas (como la privacidad). ¿Cómo es percibida y gestionada la vigilancia y la protección de datos en diferentes lugares? ¿Qué respuestas jurídicas y sociales a estos problemas aparecen en diferentes lugares de formas más o menos comparables?

Hasta la fecha hay muy poca investigación sobre la amenaza de Internet y el *Dataverse* frente a la intimidad. Lo que tiende a confirmar que, la 'privacidad' no se presta a

comparación abstracta entre culturas. Un conjunto similar de problemas, sin embargo, surge en todas partes y plantea temas que recuerdan y nos remiten a las discusiones de la vida privada. La investigación acerca de las comunicaciones e Internet (y un conjunto de cuestiones colectivamente asociadas con la globalización), sugiere que las nociones de privacidad, o lo que una vez pudo haber sido esta, están cambiando en todas partes, en respuesta a estas mismas tendencias globales, como Internet y el *Dataverse*.

Para empezar, las ideas 'occidentales' sobre privacidad se están extendiendo a nivel mundial. Por ejemplo, Yao-Huai Lü describe la forma en cómo China está asumiendo dicha situación:

> las nociones contemporáneas de la vida privada en China como una síntesis dialéctica de ambos énfasis tradicionales chinos en la importancia de la familia y el Estado, y los énfasis más occidentales sobre los derechos individuales, como el derecho a la privacidad (2005, p. 7).

En este orden de ideas, en su investigación en Japón, Makoto Nakada y Takanori Tamura afirman de manera similar haber encontrado una dicotomía en las mentes japonesas hoy en día.

> Seken... consta de cosmovisiones o formas de pensar y de sentires tradicionales e indígenas. Shakai... incluye cosmovisiones modernizadas y formas de pensar influidas en muchos aspectos por los pensamientos y los sistemas importados de los países 'occidentales' (2005, p. 27).

El surgimiento de los nuevos ‘énfasis’ a los que alude Yao-Huai, y tal vez Nakada y Tamura, se atribuyen a la difusión de los medios de comunicación y las tecnologías que incluyen las nociones occidentales de autonomía individual (descrita como el aumento del ‘egoísmo’ en China) y un fuerte aumento en la interacción comercial y la integración en el comercio mundial, con lo que las nuevas protecciones legales adquieren una nueva connotación, como es el caso del *puraibashii*, neologismo japonés, que significa control sobre los datos personales.

Asimismo, en Tailandia, por ejemplo, la noción de los derechos de privacidad apareció por primera vez en 1997, con la ley de información oficial, con referencia específica a la ‘información personal’ en poder de las autoridades públicas. No obstante, el fundamento central de la ley ha quedado en suspenso como consecuencia directa de la extraordinaria e intensa actividad en Internet de la generación más joven. Recalcando que el comercio global aumenta dichas tendencias.

Así pues, en Tailandia,

> [un] poderoso motor del desarrollo de la ley de privacidad [...] es el deseo de participar en el comercio electrónico mundial y el reconocimiento de la confianza de ser un componente fundamental de la nueva economía (Kitiyadisai, 2005, p. 21).

Después del foro de la APEC (Asia-Pacific Economic Cooperation) “Hacer frente a la protección de la privacidad: trazando un camino para la APEC” de 2003, Tailandia redactó una ley de protección de datos que se ha basado en las directrices de la OCDE (Organización para la Cooperación y el Desarrollo Económico) y la *Directiva sobre la*

protección de datos de la Unión Europea, por lo que en el espacio de una o dos décadas, todos los argumentos acerca de las amenazas a la intimidad y los derechos a la privacidad parecen haber sido importados y asimilados casi a nivel mundial o, por lo menos, entre los países más desarrollados económicamente y que comparten amplias relaciones comerciales.

Yao-Huai también cita a la Organización Mundial del Comercio (OMC) como una fuente indirecta de legislación relacionada con la privacidad. Ciertamente, las protecciones de la propiedad intelectual (en la forma del Acuerdo de la OMC sobre los Aspectos de los Derechos de Propiedad Intelectual) tienden al denominado 'ring-fence', es decir, a poner serias restricciones sobre sí mismo, por lo que solo se puede utilizar para un propósito particular, en este caso, la actividad inversionista, aunque no debemos olvidar que los tratados bilaterales de inversión poseen un mayor alcance en cuanto a protección para el inversionista. En conjunto, estos instrumentos no solo protegen contra la apropiación de fondos, beneficios, propiedades y efectos, sino sobre la construcción de narrativas acerca de la inviolabilidad de lo privado (persona, inversionista, empresa), que se reforzó aún más con la aplicación de este arsenal de protección por parte del derecho internacional.

Desde esta última perspectiva, la relación de larga data (de hecho constitutiva) entre la privacidad y la propiedad en el derecho occidental encaja, pero necesita mejorar el 'Estado de derecho' en muchos de los países del mundo, incluido Colombia, utilizando los presupuestos de ayuda que propone el desarrollo. Así pues, la protección de la privacidad que aquí se asocia a una tendencia global de profundizar y consolidar la división entre lo público y lo privado y, en general, acordonar lo privado (esfera, sector y ámbito) de la intrusión del público en la medida de lo posible, por lo que para los presentes efectos, y extrapolando a partir de una amplia base de conocimientos ciertamente pequeña, en espera de nuevas investigaciones, la perspectiva intercultural parece tener cuatro líneas principales, a saber:

(i) las nociones de privacidad difieren entre los países, a menudo de manera gradual;

(ii) las nociones 'occidentales' de privacidad, sin embargo, se extienden en muchas otras regiones, impulsadas por la expansión de Internet, los objetivos de desarrollo y el comercio mundial;

(iii) la legislación sobre privacidad adoptada recientemente en gran parte del mundo, refleja, por tanto, concepciones —legales— predominantemente occidentales de la vida privada;

(iv) como la privacidad se internaliza en la forma descrita, se percibe en todas partes como 'amenazada'. De hecho, un marcador de privacidad al estilo occidental puede ser que ésta siempre se encuentra en un estado de crisis.

2.3. En busca de una normativa para la privacidad

En el desarrollo de este trabajo de grado hemos descrito algunas de las maneras en que la aparición de Internet y de un *Dataverse* floreciente, a saber, un universo amplio y creciente de la recopilación, almacenamiento y divulgación de datos, ha provocado una gran ansiedad para la población. A su vez, se han documentado dos aspectos principales del fenómeno: el aumento de la vigilancia tanto por organismos públicos y privados y el aumento de la auto-proyección en Internet, un proceso que implica la creación y el descarte constante, tanto deliberada e incidentalmente, de información personal. La angustia producida en ambos casos es generalmente articulada en el lenguaje de la vida privada. Hemos intentado llegar a

la superficie de este término opaco para aclarar su evolución histórica y su papel en ciertos procesos políticos y económicos, subrayando su carácter relacional y maleable.

Como vimos anteriormente, la privacidad se entiende generalmente en términos del control que una persona ejerce sobre su propia información. Asimismo, hemos sugerido que la intimidad se ha convertido en un foco de tensión en relación con Internet y el *Dataverse*, ya que cada vez son más omnipresentes, precisamente, porque estos socavan dicho control y, tal vez, de manera más crítica, hace que sea difícil de creer que es posible seguir sosteniendo dicho modelo de control. Esto es en parte debido a que algunas funciones cruciales de la recopilación de información hoy en día, sobre todo en el ámbito de la vigilancia pública y privada, dependerá de que la persona afectada tenga un conocimiento limitado o nulo de los datos contenidos por ellos. También es en parte porque los sujetos dejan una gran cantidad de datos atrás de forma tan amplia y difusa que no se prestan para un fácil manejo.

La expectativa de que las personas puedan ejercer el control sobre toda la información sobre ellos mismos —'allá afuera'— parece cada vez más ilusoria e inalcanzable. Esto pone en tela de juicio el ideal de persona autónoma y privada en relación con uno de sus atributos principales. En este orden de ideas, un principio fundamental de asociación política contemporánea parece en peligro de ser transformado o, estar colapsando, más allá de su reconocimiento. Esto, es la fuente subyacente de la ansiedad contemporánea: las arenas bajo nuestras (en gran parte) tácitas categorías políticas están cambiando, pero hasta el momento no existe un modelo plausible de reemplazo para dar sentido al lugar y momento en el que estamos ahora y hacia dónde nos dirigimos en el futuro.

Por tal motivo, evaluaremos el grado en el que la arquitectura legal vigente que rige el derecho a la privacidad de la información afronta esa ansiedad que hemos identificado.

También evaluaremos hasta qué punto Internet, *Dataverse* y los procesos asociados a estos constituyen una amenaza para los derechos humanos, preguntándonos si la lente de los derechos humanos puede ayudar u obstaculizar los esfuerzos para hacer frente a sus efectos negativos. A continuación consideraremos si el marco de la ley internacional está debidamente equipado para este conjunto de preocupaciones, dónde es deficiente y cómo podría mejorarse.

En el tratamiento de la privacidad nos hemos centrado en la 'privacidad de la información'. Sin embargo, un término más preciso sería el de control de la comunicación, un término que también reconoce la relacionalidad y la intersubjetividad de la vida privada. Privacidad implica relacionarse con los demás: si pensamos en los 'otros' como vecinos, amigos, familia, sociedad, público, nación o Estado, la negociación de dichas relaciones es fundamental e inevitablemente intersubjetiva. Hablar de control de comunicación, sin embargo, también se centra en las nociones de autonomía e intencionalidad. Se supone que la 'información' tiene un valor, que no es más que la significación de la libre flotación. Por tanto, para ser una persona autónoma y privada, entonces, se debe tener la capacidad de establecer el valor a la información relativa a sí mismo, es decir, decidir lo que esta significa para cada uno, antes de que sea subida a Internet y esté a merced del *Dataverse*.

En este trabajo de grado hemos puesto en duda los principios subyacentes sobre la privacidad. Dean sugiere que la tecno-cultura materializa la esfera pública: los particulares están representados en este espacio público en forma de clones digitales o 'individuos' con imágenes de datos o 'identidades vigiladas'. Existen nuestros perfiles digitales en el ciberespacio, registrándose y almacenándose en las diferentes bases de datos a lo largo de Internet y aunque es posible que podamos ajustar ciertos elementos de la información que circula sobre nosotros, parece poco probable que alguna vez podamos estar en condiciones de determinar en qué forma nosotros como 'individuos' tomamos o limitamos cuánto y qué tipo de información puede y debe ser abarcada. En última instancia, los 'individuos' tienen

una vida propia, por lo que ni siquiera pueden llegar a conocer sus parámetros completos. También esto es, inevitablemente, una fuente de ansiedad.

Sin embargo, si la intimidad es de hecho un bien público, deberíamos esperar protecciones públicas y judiciales contra tales resultados. Si existe un derecho a la privacidad de la información, el cual debe significar sin duda, como mínimo, que conservamos un tipo de control básico sobre nuestros seres digitales. Una lectura superficial de la *Directiva de protección de datos* de la Unión Europea parece apoyar este punto de vista. Dado que un perfil de 'individuo' puede llegar a tener serias consecuencias en el mundo real, es aquí donde el cuerpo de leyes destinadas a proteger la privacidad debería ser más relevante. Vamos a examinar la legislación pertinente con eso en mente, empezando por los Estados Unidos y luego, respectivamente, en Europa.

2.3.1. El derecho a la privacidad en los Estados Unidos, en pos de lo razonable

El derecho a la privacidad ha tenido una historia difícil, una situación incierta y una dosis de esquizofrenia transatlántica. En los Estados Unidos tiene una genealogía muy clara que data desde 1890 por un artículo de revisión legislativa realizado por dos juristas, Samuel Warren y Louis Brandeis. Mucho más tarde, como juez de la Corte Suprema en 1928, Brandeis le otorgó a su postura facultades constitucionales en un fuerte disenso ante un pronunciamiento sobre las escuchas telefónicas, en el caso *Olmstead vs. Estados Unidos*. La esencia de la famosa y amplia intervención de Brandeis consistía en que los derechos de privacidad se extendían más allá de los controles propiamente a la propiedad. Finalmente, esta postura fue aprobada por la Corte en 1965, en el caso *Griswold vs. Connecticut*, el cual trata del uso de una pareja casada de anticonceptivos. Griswold estableció el patrón para una rama de la interpretación del derecho a la intimidad en la jurisprudencia de la Corte

Suprema, que en su mayoría se centró en la ‘intimidad decisional’. Aquí privacidad aparece como el derecho a elegir, sobre todo, en lo concerniente al propio cuerpo.

Una segunda rama de la jurisprudencia comienza con una decisión sobre las escuchas telefónicas (*Katz vs. Estados Unidos*), la cual anuló a Olmstead. En este caso, una intervención telefónica del FBI en una cabina de teléfono público se encontró ilegal porque, parafraseando al juez Marshall Harlan en un lenguaje que desde entonces se ha convertido en una posición estándar, en las circunstancias de que se trate de una persona, esta tiene una ‘expectativa razonable de privacidad’. Esta sigue siendo la prueba máxima de la vida privada en los casos relacionados con la vigilancia, pero su eficacia más consistente ha sido la de distinguir entre el espacio ‘público’ (la cabina de teléfono público en este caso particular) y ‘privado’ (es decir, el hogar), en este sentido, la implicación parece ser que el ‘hogar’ para el ciudadano americano es su ‘castillo personal’, no obstante, la decisión está claramente enraizada en la ‘intimidad local’, en lugar de privacidad de la información.

El derecho a la privacidad en estos casos se deriva de la Cuarta Enmienda de la Constitución de los EE.UU., la cual dice:

> *El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas y embargadas.*

La enmienda aborda explícitamente la propiedad (por tanto, su vinculación, en la jurisprudencia, a la intimidad del hogar), la seguridad personal y la legalidad (por ello, ordena una serie de 'afirmaciones' con serias instrucciones específicas). La enmienda incluye una serie de términos, basados en derechos, que han proporcionado un excelente forraje para las disputas legales. ¿Qué es un registro o una incautación 'verosímil' o 'razonable'? ¿Qué evidencia indica una causa 'probable' para justificar su realización?

La expectativa razonable de privacidad es, por supuesto, un criterio subjetivo de interpretación. Como Solove señala, 'expectativa razonable' suena igual que 'blanco móvil'. Sabemos que nuestra presencia en Internet deja un rastro de datos significativos, además que la magnitud y el contenido de este sendero de datos no es conocido por nosotros en su totalidad. ¿Podemos esperar que no se conozca por alguien más? ¿Eso sería 'razonable'? Ante la gran cantidad de información de carácter personal, en la era tecno-cultural, es difícil saber qué expectativas podrían tener los demás, como para querer y poder acceder a nuestra imagen de datos, así como determinar su 'razonabilidad'. El punto, tal vez, es que en el mundo actual el parámetro de nuestras expectativas debe ser bastante diminuto: no esperamos mucho de la 'privacidad informacional' en la actualidad, por lo que es difícil ver nuestras expectativas en aumento. Esto entra en contraste con la privacidad o la 'toma de decisiones' de carácter local, donde nuestras expectativas pueden permanecer y ser más robustas.

El principio de legalidad es de vital importancia para la determinación de una 'expectativa razonable'. Las expectativas se establecen en función de la legislación pertinente. Aunque pocas personas conocen bien la ley, la mera existencia de una ley es generalmente vista como adecuada para establecer sus 'expectativas'. En los EE.UU., las escuchas telefónicas están autorizadas de diferentes maneras: (i) sobre la base de una orden judicial otorgada previamente por un tribunal federal o estatal (en las investigaciones criminales); (ii) por orden de un Tribunal de Vigilancia de Inteligencia Extranjero Especial (en los casos de

espionaje o terrorismo) o por orden presidencial, sin orden judicial, en algunos casos, por lo general en forma de Cartas de Seguridad Nacional. La normativa, la Ley Federal de escuchas telefónicas y la Ley de Vigilancia de Inteligencia Extranjera (FISA), modificada por la Ley de Comunicaciones Electrónicas (1986), la Ley Patriótica (2001) y las Enmiendas a la FISA (2008), conceden excepciones a las investigaciones de seguridad nacional para interceptar y vigilar determinadas actividades privadas. Los tribunales han sido generosos con el gobierno en este tema, ya que rara vez obstruyen las solicitudes de interceptaciones, pero la gran mayoría de la vigilancia llevada a cabo en los últimos años, sin embargo, parece haber sido realizada sin una orden judicial. Por otra parte, se cree que cada intervención telefónica que abarca las comunicaciones de aproximadamente 100 personas, haría posible que las comunicaciones de más de un millón de personas fueran intervenidas simultáneamente por las autoridades estadounidenses en su territorio, es decir, por cada persona que se intercepta, es posible conocer aleatoriamente las comunicaciones de otras 10.000. Aun así, algunos creen que las excepciones permitidas por la ley son demasiado estrechas. El juez Richard Posner, por ejemplo, argumentó en el *Wall Street Journal*, que la FISA es deficiente, ya que requiere una 'causa probable' para creer que el objetivo de la vigilancia es un terrorista, mientras que lo primordial seria averiguar quién es un terrorista. A juicio de Posner, para un solo caso se pueden emitir muchas órdenes de más, lo que tendría el efecto principal, presumiblemente, de vigilancia e interceptación sin una orden judicial.

No obstante, un área importante de la recolección de datos tiende claramente a escapar de esta discusión: la relevancia de este cuerpo normativo para los ciudadanos no estadounidenses y no residentes. En su mayor parte, los no ciudadanos no están cubiertos por muchas protecciones legales en los Estados Unidos. La preocupación fundamental, sin embargo, debe referirse a la extraordinaria capacidad del gobierno estadounidense para recoger información personal sobre individuos por fuera de su país. Tradicionalmente, dicho control siempre ha estado sujeto a menos controles, así es como el *New York Times* lo informó por primera vez en 2001 acerca del programa de la Agencia de Seguridad Nacional

(NSA), para la vigilancia de las comunicaciones que afectaban los intereses de los Estados Unidos.

Bajo las reglas de larga data de la agencia, la NSA puede apuntar a la vigilancia e interceptación de las llamadas telefónicas o mensajes de correo electrónico en suelo extranjero, incluso si los destinatarios de dichas comunicaciones se encuentran en Estados Unidos. Sin embargo, generalmente el gobierno solo podría vigilar los teléfonos y mensajes de correo electrónico en los Estados Unidos obteniendo previamente una orden judicial.

En esencia, todas las comunicaciones realizadas por 'personas no estadounidenses' por fuera de los EE.UU., son presa fácil para la interceptación, esto es conocido como la red Posner.

De manera similar, la información que las empresas estadounidenses reúnen de los extranjeros en el extranjero (es decir, personas no estadounidenses por fuera de los EE.UU.) y que a menudo se encuentra en bases de datos con sede en EE.UU., está sujeta a menos controles en virtud de la ley estadounidense sobre recolección de información. Esto plantea una serie de preguntas jurisdiccionales intrigantes acerca de la aplicabilidad de la ley extranjera, ya que por lo general es más difícil para los extranjeros poder ejercer sus derechos en los tribunales norteamericanos en los casos en que sus tribunales domésticos (o gobiernos) no están dispuestos o son incapaces de controlar legalmente a las empresas estadounidenses.

En la mayoría de los países, las personas dependen de la reglamentación nacional local sobre la empresa correspondiente (ilustrativos son los casos de Yahoo! en Francia y China) para proteger sus datos de este tipo de investigación por parte del gobierno de los EE.UU.

Así, en la práctica, esta especie de 'salvaguarda' se complica cuando los datos en sí se encuentran físicamente en los EE.UU. Además, simplemente no es el caso de que todos los países estén igualmente equipados para poder exigir a las empresas extranjeras no cumplir con las peticiones del gobierno EE.UU. sobre vigilancia y recolección de datos, en caso de producirse. Por tanto, los controles de este tipo solo funcionan en caso de que las empresas tengan activos significativos en el país afectado, los cuales puedan ser embargados en caso de incumplimiento. En otras palabras, las normas nacionales pueden no coaccionar a las empresas de Internet que prestan servicios en los países donde no tienen ninguna presencia física.

En consecuencia, es probable que la *Directiva de Protección de Datos* de la Unión Europea de 1995, proporcione los más altos niveles de protección de datos de carácter personal para los nacionales en cualquier parte del mundo preocupados por la vigilancia de EE.UU. Esto debido a que la mayoría de las grandes empresas de recolección de datos tienen activos en Europa y el mercado europeo es demasiado grande como para renunciar a este. Por tanto, esta ley permite solicitar todas las actividades de recopilación de datos de las compañías estadounidenses realizadas en cualquier parte del mundo.

2.3.2. Europa, protección de datos, 'vida privada y familiar'

El derecho a la privacidad ha tenido una vida activa en el Tribunal Europeo de Derechos Humanos de Estrasburgo. En un caso célebre, *S. y Marper vs. el Reino Unido*, el Tribunal declaró que el concepto de vida privada es un término amplio no susceptible de definición exhaustiva. Por lo que se enumeraron las distintas categorías contempladas en el artículo 8 y en la jurisprudencia hasta la fecha: (i) privacidad 'física' e integridad psicológica de una persona; (ii) múltiples aspectos de la identidad física y social de la persona; (iii) identificación de género, orientación y vida sexual; (iv) identidad étnica; (v) el derecho al

desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y el mundo exterior; (vi) el derecho de la persona a su imagen.

No obstante, vale la pena señalar que la lista anterior, no es exhaustiva. También podría haberse mencionado la ausencia de contaminación, por ejemplo, entre otras protecciones al 'hogar' y a la vida familiar.

Retomando a *S. y Marper*. El amplio campo de aplicación del artículo 8 es sin duda atribuible a una visión arraigada en la tradición jurídica en la cual la privacidad, es la base de la libertad cívica en un Estado moderno. Esto explica la recurrencia a los principios de identidad y el amplio espectro sobre temas de privacidad como toma de decisiones en el ámbito del artículo 8. Sin embargo, el tono un poco autocomplaciente del Tribunal no se debe interpretar como una señal de que la pertinencia del derecho a la privacidad para muchos de sus casos indica necesariamente su primacía. Esto es así incluso con respecto a la 'intimidad decisional', lo que podría ser descrito como el derecho de una persona de ser la directora en la toma de decisiones en asuntos de importancia fundamental para su autonomía. Por ejemplo, el Tribunal de Justicia ha afirmado que el estatuto jurídico de los transexuales es una cuestión de privacidad planteada en el artículo 8, pero hasta ahora no ha aceptado que los Estados deban reconocer el género post-operatorio de los transexuales en la ley. El Tribunal afirma que la eutanasia cabe dentro del alcance del artículo 8, pero no se ha promulgado sobre las prohibiciones del suicidio asistido que violan el derecho a la privacidad.

Los casos que plantean cuestiones acerca de privacidad de la información se han presentado ante el Tribunal, aunque muy recientemente. Los argumentos jurídicos han dependido de las diversas excepciones generales incorporadas en la formulación del derecho a nivel europeo y en particular (como en los EE.UU.) con la condición de legalidad. El artículo 8

del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales (1950) utiliza este formato de declaración del derecho seguido de excepciones. El artículo afirma lo siguiente:

> *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*.

> *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esté prevista por la ley y sea necesaria en una sociedad democrática en interés de la seguridad nacional, la seguridad pública, el bienestar económico del país, para la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás*.

El primer caso importante sobre vigilancia fue *Malone vs. el Reino Unido*, en el que el Tribunal criticó al gobierno por la 'oscuridad e incertidumbre' de sus justificaciones legales para interceptar las comunicaciones del Sr. Malone. En buena medida el Tribunal señaló que la legislación detallada debería ser más eficiente, lo que es más, las estadísticas publicadas muestran la eficacia de estos procedimientos para mantener el número de órdenes judiciales otorgadas relativamente bajo, especialmente en comparación con el aumento del número de delitos procesables comprometidos y los teléfonos instalados. Su punto no era simplemente que una ley debía existir, sino que debería ser lo suficientemente detallada como para indicar con claridad razonable el alcance y la forma de ejercicio de las facultades atribuidas a los poderes públicos. Como dijo el Tribunal en un caso posterior en 2008, cuando se pronunció sobre la Instalación de Pruebas Electrónicas en Capenhurst, Cheshire (Inglaterra), que supuestamente interceptaba todas las llamadas entre Irlanda y el Reino Unido, allí los jueces fueron capaces de dibujar un elaborado conjunto de principios jurídicos derivados de su jurisprudencia.

En su jurisprudencia relativa a las medidas secretas de vigilancia, el Tribunal ha desarrollado las siguientes garantías mínimas que deben ser establecidas por la ley estatutaria con el fin de evitar los abusos de poder: (i) la naturaleza de los delitos que pueden dar lugar a una orden de interceptación; (ii) una definición de las categorías de personas que pueden tener sus teléfonos o PC intervenidos; (iii) un límite en la duración de las escuchas telefónicas; (iv) el procedimiento que debe seguirse para el examen, el uso y el almacenamiento de los datos obtenidos; (v) las precauciones que deben tomarse cuando se comunican los datos a otras partes; y (vi) las circunstancias en que las grabaciones pueden o deben borrarse.

Se trata de criterios estándar de un Estado liberal de derecho, es decir, instrucciones detalladas destinadas a garantizar que los funcionarios estatales actúen de acuerdo a la ley, con un mínimo de discreción y diseñados para maximizar la eficiencia. No obstante, el Tribunal pretende eludir la cuestión más complicada, a saber, si las 'interceptaciones' (que se encuentra en cada uno de estos ejemplos) son en un caso determinado necesarias en una sociedad democrática o poseen interés para la seguridad nacional, la seguridad pública, el bienestar económico y así sucesivamente. Por ello, es apropiado volver a *S. y Marper* en esta coyuntura. Dicho caso se refería a la retención por parte de las autoridades inglesas de las huellas dactilares, datos de ADN y muestras de células de individuos acusados de crímenes, pero posteriormente absueltos (en ese momento, *S.* tenía 12 años de edad). El Tribunal consideró una violación al artículo 8, ya que la retención del Estado debido a su naturaleza 'indiscriminada' no pudo encontrar un justo equilibrio en la competencia entre intereses públicos y privados.

Tres aspectos de la decisión del Tribunal valen la pena ser analizados un poco más en detalle:

1. El tribunal se refirió a la *Directiva de Protección de Datos* de la Unión Europea de 1995 y la aplicación de la legislación del Reino Unido de 1998, de una manera curiosamente concluyente. Dado que la Directiva se refiere directamente al 'derecho a la privacidad', esto parece ser una de las pocas áreas en las que el Consejo de Europa y los organismos de la Unión Europea comparten explícitamente en cómo debería llevarse a cabo la supervisión y vigilancia. Curiosamente, sin embargo, la Ley de Protección de Datos de 1998, no merece una mención en los propios procesos judiciales en el Reino Unido sobre la materia. Esto puede ser debido a la amplia excepción de la Directiva en relación con el proceso penal y la seguridad nacional.

2. El Tribunal volvió a la práctica general de los otros Estados miembros del Consejo de Europa. El Reino Unido resulta ser un caso atípico, ya que expresamente permite en su legislación la retención sistemática e indefinida de los perfiles de ADN y las muestras celulares de las personas que han sido absueltas. Sin embargo, el Reino Unido no es el único país del continente europeo en retener información. Dinamarca mantiene los perfiles de ADN durante 10 años, Francia durante 25 años incluso en caso de absolución, y numerosos países permiten que el ADN se mantenga cuando las sospechas permanecen sobre la persona o si es necesario realizar más investigaciones en un caso separado, o donde el demandado es absuelto. Entonces, ¿cómo decidir qué clase de base de datos de ADN es aceptable? En última instancia, el Tribunal evitó la expresión 'sistemática e indefinida' en su fallo sobre la legalidad de la recolección y retención de datos, eligiendo en su lugar fallar en contra de la naturaleza 'indiscriminada' de la política.

3. ¿Qué se entiende por 'indiscriminada'? El Tribunal sugiere que las medidas podrían ser legales, pero de hecho, ¿también pueden 'discriminar'?. La respuesta es claramente afirmativa, dado que el Tribunal de Justicia ya ha declarado que las leyes

> que sancionan interceptaciones deben incluir una definición de las categorías de personas que pueden tener sus comunicaciones intervenidas. La conclusión es bien explícita. Los enfoques Dragnet (red que se utiliza para rastrear o localizar personas) son injustificables e ineficientes. El Estado infringe los derechos cuando intercepta y analiza las comunicaciones de personas que claramente no son su objetivo. En otras palabras, al centrarse en la discriminación en lugar de la sistematicidad, el Tribunal regresó de nuevo a un criterio de legalidad y no de fondo (un enfoque supuesto en la sistematicidad habría requerido de decidir si las medidas de vigilancia particulares violan la privacidad *a priori*).

Pero si los Estados deben discriminar en la recolección y retención de datos, por lo menos según el Tribunal Europeo de Derechos Humanos, ¿cómo deben hacerlo? Esto plantea la cuestión de los derechos humanos como veremos en el capítulo final.

CAPÍTULO III

LA PRIVACIDAD DE LA INFORMACIÓN EN COLOMBIA A PARTIR DEL 2010. LA NECESIDAD DE UN NUEVO DERECHO CONSTITUCIONAL

3.1. La normativa de la privacidad en Colombia

A nivel nacional, e incluso latinoamericano, no existe una legislación o normativa expresa (tipo Directiva de la Unión Europea) que regule el derecho a la privacidad y el uso de la información de manera expresa. Sin embargo, tomaremos como referente la normativa internacional en derechos humanos al respecto, así la *Declaración Universal de Derechos Humanos*, promulga:

> ***Artículo 12.*** *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

Mientras que el *Pacto Internacional de Derechos Civiles y Políticos*, establece lo siguiente:

> ***Artículo 17.*** *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*

> *2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*.

A nivel regional la *Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica*, en materia del derecho a la privacidad estableció:

> ***Artículo 11.*** *1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*
>
> *2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*
>
> *3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*.

No obstante, y a pesar del bloque de constitucionalidad promulgado por el artículo 93, a nivel nacional la legislación ―sobre privacidad de la información― es nula, por lo que es menester recurrir a la jurisprudencia de la Corte Constitucional para encontrar luces en materia de la aplicación y garantía del derecho a la privacidad en Colombia.

En este orden de ideas, la jurisprudencia ha establecido que el derecho a la privacidad tiene diversas facetas, a saber: (i) intimidad personal; (ii) intimidad familiar; (iii) intimidad social. En cuanto a la intimidad personal esta abarca todo lo concerniente a la privacidad de las personas, entre otras: relaciones familiares; costumbres y cultura; prácticas sexuales; salud; comunicaciones personales; creencias religiosas; secretos profesionales; y todo comportamiento del individuo que solo le compete a él, todo lo anterior está sujeto al más

alto grado de protección, a menos que su titular decida revelar y permitir su acceso al público o al Estado.

En cuanto a la intimida familiar, esta responde al secreto y a la privacidad en el núcleo familiar, una de cuyas principales manifestaciones es el derecho a la inmunidad penal. Mientras que la intimidad social involucra las relaciones del individuo en un entorno social determinado, como por ejemplo su entorno laboral. Así las cosas, la protección a la privacidad en el hogar es mucho más amplia que aquella que protege las situaciones laborales o de relaciones interpersonales.

No obstante, en la Sentencia C-640 de 2010, la Corte promulgó, que el interés público está por encima del derecho a la privacidad en cualquiera de sus manifestaciones:

> *[…] en reiterada jurisprudencia […] la Corte ha establecido que uno de los límites admisibles del derecho constitucional a la intimidad es la existencia de un interés general en la divulgación de la información personal o familiar, esto es, de una circunstancia que le imprima relevancia pública al dato analizado. En este caso -a diferencia de otros en los que a la Corte también se le ha planteado si la existencia de un registro o base de datos vulnera el derecho a la intimidad-, no es necesario demostrar que el tema al que se refiere el Registro aquí analizado es de "interés público", pues tal carácter viene dado expresamente por la propia Constitución* (Sentencia C-640 de 2010).

Concluyendo,

> *[…] Por consiguiente, una segunda conclusión al estudio de la intimidad, permite fijar la siguiente regla: El alcance del derecho a la intimidad de un sujeto, depende de los límites que se impongan a los demás, como exigencia básica de respeto y protección de la vida privada de una persona. La existencia del núcleo esencial de dicho derecho, exige que existan espacios medulares en donde la personalidad de los sujetos pueda extenderse en plena libertad, pues deben encontrarse excluidos del dominio público. En aquellos espacios la garantía de no ser observado (el derecho a ser dejado solo) y de poder guardar silencio, se convierten en los pilares esenciales que permiten asegurar el goce efectivo del derecho a la intimidad* (Sentencia C-640 de 2010).

Por su parte, en cuanto a los datos, es decir, la información, la Corte ha ligado su protección a la intimidad individual, ya que la protección del dato no es tomada de forma independiente, sino como un aspecto fundamental de la identidad, estableciéndolo de la siguiente manera:

> *[…] el dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos* (Sentencia T-414 de 1992).

Agregando en la misma sentencia,

> *[…] el problema del "poder informático" existe siempre que se poseen datos sobre las personas bien sea en forma manual o por medios electrónicos. Con el desarrollo de estos últimos, las posibilidades de acción de ese poder en contra de la libertad de las personas se magnifican y harían necesaria una legislación especial.*

> *El "perfil de datos" de la persona se constituye entonces en una especie de "persona virtual" sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u "ostracismo" social […] Un "buen" manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente peligro de control social de aquellos que ostentan "poder informático", no solamente contra la libertad de las personas individuales sino contra la de sectores sociales más amplios*.

Asimismo, el derecho a la privacidad es tomado por la Corte como un aspecto central del desarrollo de la persona y de carácter *erga omnes*, a saber:

> *[…] se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e*

> *imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada.*
>
> *Esta Sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991.*
>
> *Ante un eventual conflicto insuperable entre el derecho a la información y el derecho a la intimidad en donde no pueda ser posible un equilibrio o coexistencia, la intimidad deberá prevalecer* (Sentencia T-414 de 1992).

Posición respaldada en la sentencia T-437 de 2004, la cual, a su vez, tiene en cuenta la normativa internacional al respecto, otorgándole la categoría de derecho fundamental, prevaleciendo sobre cualquier manejo que se le dé a la información, sin importar que sea un organismo público o privado:

> *[…] la intimidad ha sido reconocida por la Constitución como un derecho de carácter fundamental en el artículo 15. En esa disposición, el constituyente dispuso que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar". En esa misma norma, la Carta previó*

una protección reforzada de la intimidad, en aquellos casos en los cuales está de por medio (i) el conocimiento, actualización y rectificación de informaciones recogidas en bancos de datos y en archivos de entidades públicas y privadas, (ii) la correspondencia y (iii) los libros de contabilidad y demás documentos privados, de los que eventualmente podrá exigirse su presentación para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado [...].

El derecho a la intimidad también está consagrado en múltiples instrumentos internacionales de protección de derechos humanos, como por ejemplo en el artículo 12 de la Declaración Universal de Derechos Humanos, en donde se señala que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación" indicando a su vez que "Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". De igual forma en el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos que prescribe lo siguiente: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". También fue consagrado en el artículo 8.1 del Convenio para la protección de los Derechos Humanos y las libertades fundamentales, donde se dispuso que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" y el artículo 11.2 del Pacto de San José de Costa Rica dispone a su vez que "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la

protección de la ley contra esas injerencias o esos ataques (Sentencia T-437 de 2004).

El concepto de intimidad, o privacidad, precisamente comporta según la Corte Constitucional un reconocimiento de reserva, de cierta información que es de uso exclusivo de la persona, lo cual implica un reconocimiento del contexto en el cual operaría dicho derecho. A su vez, establece un área restringida que solo puede transgredirse con el conocimiento del titular o por mandato judicial, pero sin cometerse injusticias y arbitrariedades.

La intimidad ha sido entendida por esta Corte como aquel ámbito que las personas reservan del conocimiento de los demás, aquel "el espacio exclusivo de cada uno, aquella orbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo (...). Es el área restringida inherente a toda persona o familia, que solamente puede ser penetrada por extraños con el consentimiento de su titular o mediando orden dictada por autoridad competente, en ejercicio de sus funciones y de conformidad con la Constitución y la ley". La jurisprudencia constitucional ha señalado que el derecho a la intimidad protege precisamente la indebida injerencia en ésta esfera privada del individuo y su familia, la cual está conformada por diversas situaciones y hechos reservados principalmente para sí o para el núcleo familiar, "y frente a los cuales no pueden interferir terceros.

Únicamente en aquellos casos en los cuales existe de por medio una aceptación expresa o tácita en dar a conocer informaciones o circunstancias que recaen en ésta esfera íntima, podría aceptarse la

intromisión de un tercero. Así, la Corte en la sentencia SU-056 de 1995, señaló que si bien "El derecho a la intimidad hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños" éste debe mantenerse reservado "a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho o por que han trascendido al dominio de la opinión pública.

Con base en los anteriores criterios, la Corte en la sentencia T-696 de 1996, decisión reiterada en las sentencias T-169 de 2000 y T-1233 de 2001, ha indicado que el derecho a la intimidad es vulnerado por lo menos de las siguientes maneras. Primero, cuando puede corroborarse una intromisión irracional en el ámbito reservado de las personas. Segundo, cuando son divulgados hechos privados sin que medie un consentimiento o aceptación clara. Y tercero, cuando aún a pesar de la aprobación por parte de una persona, de divulgar hechos o circunstancias personales o íntimas, éstos son presentados de forma tergiversada o mentirosa. Bajo estas circunstancias, la acción de tutela es el mecanismo principal con el cual buscar su protección (Sentencia T-437 de 2004).

Así, en la sentencia T-1202 de 2012, en la que se reiteró la decisión promulgada en la sentencia T-066 de 1998, la Corte señaló:

[…] cuando se presentan conflictos entre el derecho a la información y los derechos a la honra, el buen nombre y la intimidad, en el caso de las personas y los hechos de importancia públicos, predomina prima facie el primero. En estos eventos, el derecho de información debe ser preferido, en principio, en razón del papel de control del poder que se asigna socialmente a los medios de comunicación. Del reconocimiento de que los medios cumplen en este campo una función importantísima para la vigencia del sistema democrático se deriva que ellos deben gozar de amplia libertad en la tarea de supervisión de las entidades estatales - y de los poderes privados. Si se impusieran fuertes restricciones sobre la prensa en estas áreas se perjudicaría en medida notable su capacidad de vigilancia sobre el correcto desempeño de estos poderes. No desconoce la Corte que la referida amplitud de la libertad de prensa en estos campos puede llegar a afectar los derechos de las personas que se desempeñan en posiciones de notoriedad e interés público. No obstante, en principio habrá de responderse que estas personas, al aceptar su situación social, han consentido tácitamente en una cierta restricción de esos derechos. En efecto, su papel de figuras públicas los convierte en objeto del interés general, por lo cual es de esperar que tanto sus actividades públicas como su vida privada sean observadas de manera minuciosa por parte de la sociedad.

La sociedad de la información y el conocimiento y en especial herramientas como el internet y las redes sociales digitales, han generado un medio social más a través del cual se puede compartir, comunicar y entretener. Ello ha traído como consecuencia un aumento exponencial de sus usuarios que tienen la posibilidad de intercambiar información, propagar ideas, participar activamente y facilitar relaciones personales.

> *A pesar de que las redes sociales digitales –generalista o de ocio y profesionales– se consolidan como un espacio en el que rigen normas similares a las del mundo no virtual, el acceso a la misma acarrea la puesta en riego de derechos fundamentales, pues el hecho de que algunas de ellas se manejen a través de perfiles creados por los usuarios, por medio de los cuales se pueden hacer públicos datos e información personal, puede traer como consecuencia la afectación de derechos como la intimidad, la protección de datos, la imagen, el honor y la honra.*
>
> *La afectación de estos derechos va de la mano, en gran medida, del desconocimiento de los usuarios acerca del funcionamiento y reglamentación de estas plataformas, pues la falta de privacidad en los perfiles y la publicación de información personal y datos especialmente protegidos como vivencias, gustos, ideología y experiencias sin ninguna restricción, se constituye en una fuente de riesgo para los derechos fundamentales de los usuarios* (Sentencia T-260 de 2012).

Agregando, en relación con el *Dataverse* y los riesgos a los que este conlleva frente al derecho a la privacidad, al igual que a la falta tanto de conciencia en el manejo de la información como de normativa para su protección y del uso indebido que podría llegar a dársele a esta, lo siguiente:

> *[…] los riesgos a los derechos fundamentales en las redes sociales pueden estar generados entre otros por las siguientes situaciones:*
>
> *- Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por*

cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado. En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa etc.

- Los datos personales pueden ser utilizados por terceros usuarios malintencionados de forma ilícita.

-Existe la posibilidad de que traten y publiquen en la red información falsa o sin autorización del usuario, generando situaciones jurídicas proseguibles que pueden llegar a derivarse de este hecho.

-El hecho de que, a través de las condiciones de riesgo aceptadas por los usuarios, estos cedan derechos plenos e ilimitados sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que puedan ser explotados económicamente por parte de la red social.

La afectación de los derechos fundamentales en redes sociales como el Facebook puede generarse en el momento en el cual el usuario se registra en la red escogida, durante su participación en la plataforma, e incluso en el momento en que decide dejar de utilizar el servicio.

En el estudios sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line, realizado por el Instituto Nacional de Tecnologías de la Comunicación, Agencia Española de

> *Protección de Datos, se señala que el primer momento crítico se sitúa al momento del registro del usuario y la configuración del perfil, pues este incidirá en el derecho a la intimidad y en el honor y la honra en caso de que el usuario no establezca adecuadamente su perfil de privacidad en el momento del registro, ya sea por desconocimiento o porque la red no disponga de estas opciones de configuración* (Sentencia T-260 de 2012).

Sin embargo, a pesar de los avances en materia jurisprudencial en los últimos años, es necesario dotar de mejores mecanismos a la protección de la información en Colombia, por ende, proponemos que el derecho a la privacidad de la información debe adquirir un carácter constitucional, apartándose de su dependencia del derecho a la intimidad individual como tal.

3.2. Privacidad de la información, un compromiso constitucional

El fracaso del sistema jurídico actual en algunos casos o la ausencia total de normativa en otros ―caso Colombia― han llevado a la sugerencia de diversas soluciones, que incluyen, entre otras: la expansión del derecho de daños; una normativa integral para Internet y los derechos de propiedad de la información personal en el *Dataverse*. Sin embargo, estas sugerencias no se enfocan en el punto central del debate.

Todas ellas tratan de proteger la privacidad de la información de las amenazas de Internet, las bases de datos informáticos, la recolección de datos de tecnología avanzada o alguna combinación de los mismos, en lugar de abordar el problema de manera integral. Esto no quiere decir que un enfoque integral resolverá todas las amenazas. De hecho, una solución diseñada para responder a una amenaza particular, probablemente, será mejor en evitar

dicha amenaza particular, de lo que sería una solución generalizada. El punto, más bien, es que estas propuestas de solución, por muy eficaces que parezcan tienen un alcance limitado, es decir, no son más que pañitos de agua tibia en un paciente terminal.

El problema es que el efecto de Internet y el *Dataverse* en la privacidad informacional es mayor que la amenaza que Internet, como tecnología, plantea a la privacidad de la información. Como tecnología, el Internet plantea problemas, ya que en la 'era de la comunicación', se ha creado una plataforma para los sitios Web que recopilan información más detallada acerca de las personas, proporcionando un medio para difundir una mayor cantidad de datos en menos cantidad de tiempo, con un menor número de errores y en distancias más grandes que nunca.

Si pudiéramos conocer la 'parte de Internet' que afecta la vida de cada uno, esto no sería más que un bache, aunque un gran bache, en la pantalla del radar de la privacidad informacional. Pero esto no es posible. Porque con la digitalización de la información, Internet y el *Dataverse* invaden incluso la vida de aquellos que no envían correos electrónicos o no utilizan la World Wide Web.

Las bases que almacenan estados de cuenta bancarios, registros de asistencia social, transacciones de tarjetas de clientes frecuentes, están todas conectadas por Internet. Así pues, el efecto de Internet sobre la privacidad de la información es mayor que la amenaza de Internet, como tecnología, porque incluso aquellos que evitan la tecnología ven en la Internet una mayor amenaza para la privacidad informacional. Debido a que el *Dataverse* ha cambiado la naturaleza misma de la vida en una era de la información, que va más allá de su red de computadoras y su amalgama de sitios Web, creando una mayor preocupación en la privacidad de la información para todo el conjunto de la sociedad.

Como resultado, el nuevo régimen legal, que es menester entablar en Colombia, debe mirar más allá de la protección contra amenazas particularizadas y hacía el establecimiento de un compromiso con la privacidad de la información. Esto requiere de un derecho constitucional centrado en ésta.

La Constitución es la infraestructura de todo régimen legal. Proporciona los contornos básicos en los que los detalles pueden ser conformados y determinados. Como tal, la protección constitucional es simultáneamente uniforme y flexible. Los derechos constitucionales constituyen un compromiso fundamental, ya que la línea de base se puede ampliar mediante la interpretación judicial y legislativa. Este tipo de compromiso es necesario para aquellos intereses que son tan ubicuos que se han convertido en parte del marco de una sociedad. Estos intereses son una preocupación fundamental y general en todos los contextos y, sin embargo, tienen el potencial de convertirse en preocupaciones particularizadas en ciertos contextos.

El *Dataverse* ha elevado la privacidad de la información a este nivel. La penetración de Internet en nuestra vida diaria ha hecho que ésta sea una preocupación en casi todas las facetas de la vida. La privacidad informacional ya no es simplemente una cuestión discreta de cómo controlar el acceso a ciertos tipos de datos, tales como registros financieros, archivos médicos o números de teléfono. Por lo que tan solo un derecho constitucional puede garantizar la privacidad de la información, de hecho, puede ser parte de la estructura del debate. Sin embargo, la amenaza puede ser mayor o menor en diferentes contextos, sobre todo con los cambios tecnológicos, tal como lo expresó la Corte en la sentencia T-260 de 2012. Como tal, la protección jurídica debe ser adaptable. Así pues, un derecho constitucional también puede proporcionar dicha adaptabilidad. Por tanto, se requiere de un compromiso constitucional para el nuevo interés generalizado en la privacidad de la información.

Un compromiso constitucional evitaría muchos escollos de las soluciones alternativas. Por ejemplo, los críticos de un régimen de derechos de propiedad argumentan que las asimetrías de información, costos de transacción, racionalidad limitada, llevará a los consumidores a renunciar a su información con demasiada facilidad. De hecho, algunos teóricos como Solove han señalado que el principal problema con Internet, tan solo surge después de la divulgación.

Un derecho constitucional, sin embargo, es inalienable. Incluso la actual debilidad del derecho constitucional a la privacidad, refleja su función como válvula de seguridad. Así, mientras un consumidor aún podría renunciar a su derecho constitucional, al igual que podría renunciar a un derecho de propiedad, la inalienabilidad constitucional crea una presunción perdurable contra toda divulgación que no existe con este último tipo de derecho. La Constitución, que ha sido comparada con la manera en que Ulises se ató al mástil, nos protege en contra de nuestros propios caprichos fugaces. La siempre presente sombra de una reclamación como resultado de un fuerte derecho constitucional, probablemente, influirá en los recolectores de la información y difusores para que reevalúen sus métodos, además de educar a los consumidores.

Un derecho constitucional también evitaría muchas de las críticas que rodean las soluciones legales. Los críticos como Pollack consideran que el enfoque de arriba hacia abajo obligatorio de cada norma es sofocante y autoritario. Otros como Fromkin sostienen que una norma quedaría mutilada debido a la incapacidad de ir a la par con los constantes avances de las nuevas tecnologías, por lo que sería inaplicable en determinado momento, tal cual como sucede en hoy en día en los países que la poseen.

Las normativas también pueden llegar a ser fácilmente dejadas de lado por un sentimiento público cambiante y no pueden compensar otros valores importantes. Por el contrario, la

decisión de acogerse al derecho constitucional recae en última instancia en el individuo, ya que las protecciones constitucionales no están vinculadas a tecnologías específicas, debido a que su aplicación se basa en la interpretación judicial y, por tanto, tendría la capacidad de adaptarse a estas.

Finalmente, una de las mayores ventajas de un derecho constitucional es que este es permanente e inalienable, sólido contra el sentimiento público que es voluble. Esto ha permitido que los principales derechos constitucionales puedan coexistir. Por otra parte, un compromiso constitucional abarcaría una serie de temas que los investigadores de privacidad de datos consideran necesarios en una solución. Se aclararía un sesgo hacia la privacidad de la información, colocando la responsabilidad última con el individuo y obligando a los recolectores de datos y difusores a internalizar el valor de la privacidad informacional. Como punto final, es importante señalar que este argumento no afirma que el derecho constitucional resuelva todos los problemas planteados por Internet y el *Dataverse*. Al respecto, Froomkin concluye acertadamente, "[n]o hay una varita mágica, esto no es la panacea" (2000, p. 1543).

Por ejemplo, una de las mayores amenazas que plantea Internet es la transferencia encubierta de la información recopilada. No está claro cómo un derecho constitucional puede llegar a corregir esta situación. Tampoco este trabajo de grado tiene la intención de emitir un juicio sobre cualquier solución. Por el contrario, un compromiso constitucional es exactamente eso: un compromiso. La dinámica de la intimidad ha cambiado y todo ordenamiento jurídico requiere de un compromiso con la privacidad de la información. Un derecho constitucional establece que el compromiso es una garantía básica, ya que sería como un puente que, naturalmente, uniría tanto a las dificultades como a los beneficios, enfocando a cada una de las alternativas unilaterales en busca de una solución. En última instancia, desde la línea de base constitucional, podría surgir un número de protecciones más fuertes y estables.

3.3. El derecho constitucional a la privacidad de la información

Los actuales derechos a la privacidad informacional en el mundo son débiles. Aunque la Corte Suprema de los Estados Unidos ha reconocido un interés constitucional sobre la privacidad de la información. Sin embargo, la fuerza de dichos derechos y su aplicación sigue siendo dudosa.

A la luz de la necesidad de un compromiso constitucional a la privacidad de la información en Colombia como respuesta al *Dataverse*, también es necesario aclarar que la protección constitucional a la intimidad sigue siendo débil y poco utilizada en nuestro medio. Por tanto, terminaremos donde empezamos, con Internet como una gran amenaza a la privacidad informacional, creando la necesidad de un compromiso constitucional más fuerte. No obstante, la discusión parece haber llegado a un callejón sin salida. Una amenaza que plantea la necesidad de un derecho constitucional, pero como lo hemos demostrado anteriormente el derecho a la privacidad de la información no es una solución última, a pesar de la normativa del derecho internacional para protegerlo.

Evidentemente, hay que abogar por un cambio en la doctrina constitucional, pero ¿por dónde empezar? Internet y el *Dataverse* representan una grave amenaza para la privacidad de la información. La normativa internacional, sin embargo, ha tratado de cambiar más de lo que la mayoría reconoce. La privacidad informacional, en lugar de ser un interés que se centra, principalmente, en evitar la divulgación, representa una preocupación por las consecuencias reales y percibidas de la divulgación. Así que Internet, como la más extensa base de datos de computadoras que existe en el mundo, ha hecho más que representar una amenaza para esta forma de privacidad. Debido a su introducción en la vida de todos, aunque para los anti-tecnófobos más radicales, Internet ha elevado la preocupación por la privacidad de la información a una preocupación generalizada. Así las cosas, el régimen

legal actual es impotente, en su lugar, un compromiso más fuerte debe ser hecho a una escala constitucional. Tan solo entonces el panorama legal obtendrá un mayor fundamento y la flexibilidad necesaria para proteger un interés generalizado suficiente acerca de la privacidad de la información.

A pesar de lo anterior, el derecho constitucional sobre la privacidad informacional a escala mundial sigue siendo débil. La Corte Suprema de EE.UU. en el caso *Whalen vs. Roe*, parece haber establecido no más de un interés constitucional en la privacidad de la información.

Un compromiso constitucional, entonces, debe ser iniciado. Debido a la naturaleza transfronteriza única de Internet, un derecho internacional sería más preferible. Por el momento, sin embargo, ambos esquemas son débiles y es la normativa de la ONU, la única que ofrece una mayor promesa en el corto plazo. Algunos de los Estados ya están iniciando el debate acerca del derecho constitucional a la privacidad de la información, y Canadá, posiblemente sea el precursor, ya que su postura promulga una concepción que refleja fielmente la definición adoptada por el presente trabajo de grado. Por otra parte, los Estados son terrenos fértiles para la experimentación tradicionalmente constitucional. Entonces, se debe tratar de reforzar el derecho constitucional como un derecho que se enfoca en la privacidad informacional de los Estados, los cuales vigilan, a su vez, la privacidad de sus ciudadanos.

Vivimos en una era de las comunicaciones, una era que llega a una conclusión. Con la proliferación de Internet, la revolución digital se ha convertido en nuestra realidad digital diaria. La transformación de la información, y su nuevo adquirido valor, está en un crescendo constante. Como resultado, la privacidad de la información se ha convertido en una prioridad permanente. Para eso, debemos ofrecer una respuesta constitucional que vaya

más allá de la mera protección de la intimidad individual, por tanto, estamos atrasados en plantear una reforma constitucional al artículo 15 de la Constitución, con el fin de que abarque a cabalidad todo lo referente al derecho humano a la privacidad de la información, adaptándose a la problemática de las nuevas tecnologías.

CAPÍTULO IV

PROPUESTA FINAL: EL DERECHO A LA PRIVACIDAD DE LA INFORMACIÓN Y SU VÍNCULO CON LOS DERECHOS HUMANOS

¿Qué significa todo lo anterior para los derechos humanos? Entre los desafíos más graves a los derechos humanos en los últimos años están las prácticas que aparentemente se remontan a dos de las tendencias antemencionadas aquí, a saber: la vigilancia y la recolección de datos.

Desde el 2010 en adelante muchos individuos han sido aprehendidos sin duda, sobre la base de las comunicaciones interceptadas —especialmente en Internet— o los datos descubiertos en las computadoras portátiles incautadas al igual que en los teléfonos móviles. En la práctica, sin embargo, estas técnicas no son muy diferentes a sus precursoras, tales como: interceptación de comunicaciones postales y lo que se llama 'inteligencia humana'. En última instancia, las decisiones sobre si se debe violar o no la privacidad de un individuo no parecen haber sido impulsadas o particularmente influenciadas por las nuevas tecnologías de vigilancia o de recopilación de datos, tan solo estas las han hecho más fáciles, rápidas y eficientes.

No obstante, otros derechos humanos a parte de la privacidad también parecen estar en juego. Una conexión preocupante puede rastrearse entre la 'memoria perfecta' del *Dataverse* y las amenazas a la 'libertad de expresión'. En particular, la preocupación de que las estructuras de Internet animarán gradualmente a la autocensura parece, a primera vista, como una cuestión de derechos humanos. En una mirada más cercana, sin embargo, esto también es difícil de sostener. Las interpretaciones de las disposiciones pertinentes de

derechos humanos como la Corte Europea de los Derechos Humanos, el *Pacto Internacional de Derechos Civiles y Políticos* y, en particular, la jurisprudencia de la Corte Suprema de los EE.UU. sobre la libertad de expresión, tienden a ver a la libertad de expresión como un derecho negativo: el Estado no debe imponer restricciones sobre la 'libertad de expresión'. Donde los silencios surgen debido a factores estructurales o de mercado, o como resultado de la interacción entre los actores privados de no divulgar su propia información.

Así pues, una preocupación más fundamental de los derechos humanos se refiere al Estado de derecho en sí mismo, en una situación en la que lo público y lo privado parecen estar colapsando en una visión borrosa y convergente. Diversos comentaristas, como Peter Ramsay, han llamado la atención acerca de lo que Anastassia Tsoukala denominó como el "desvanecimiento de los derechos humanos" (2008, p. 5).

En este punto de vista, el aumento de la recopilación de datos por parte del Estado (en el contexto de un movimiento foucaultiano hacia la seguridad) ha tendido a disolver el marco de derechos y obligaciones que se funda en el contrato social liberal, al reemplazarlo por uno basado en la evaluación de riesgos, que involucra a empresas del sector privado. La recopilación de datos personales permite a un Estado evaluar el riesgo individual de antemano y agrupar a los individuos en categorías de riesgo, en vez de (como las normas de derechos humanos espera) presumir la inocencia y la libertad de cada individuo hasta la comisión de un delito.

Una visión semejante subyace a la pregunta de Peter Ramsay sobre el uso de órdenes preventivas en el Reino Unido: la Ordenanza sobre Comportamientos Antisociales (ASBOs) y la Orden Preventiva Civil (CPO). Estos mecanismos no requieren de catalogar a una persona como 'delincuente' o que haya realmente cometido un delito, sino

simplemente evidenciar un comportamiento que manifiesta una disposición que no logra tranquilizar a los demás con respecto a su futura seguridad.

Ramsay retoma, como ya lo hicimos anteriormente, el principio de la autonomía privada como base de una sociedad liberal contemporánea. De acuerdo con una interpretación común, la autonomía es vulnerable. Sus condiciones previas son la autoestima, la autoconfianza y la responsabilidad del Estado para intervenir cuando estas son, o parecen ser, amenazadas. Por tanto, el Estado tiene un interés en la vigilancia y la previsión de la conducta de las personas que puedan suponer un riesgo para la autonomía de los demás.

Así para Ramsay,

> el propósito de la CPO no es el propósito de la ley penal liberal de castigar a la invasión de los intereses protegidos de los sujetos individuales autónomos, un propósito que toma forma en la igual protección de las leyes generales. El propósito de la CPO es proteger la 'avanzada' del liberalismo subjetivo de la 'infraestructura del reconocimiento' vulnerable de la autonomía. Por tanto, toma la forma de evaluación de riesgos y la distribución deliberadamente discriminatoria de las obligaciones penales y civiles (2008, p. 28).

Podemos preguntarnos, además, si la 'amenaza' a los derechos humanos está vinculada, en cada uno de estos ejemplos, al supuesto de la autonomía individual necesario para los derechos humanos tanto conceptualmente como en la práctica. Por lo que la recopilación y análisis de datos son esencialmente los síntomas de un cambio más amplio en la reflexión sobre el papel del Estado en la gestión del espacio público.

La evaluación de riesgos y medidas preventivas requieren datos, por tal motivo los datos se adquieren. También puede darse el caso de que el aumento del acceso a los datos en sí genera nuevos enfoques de la aplicación de la ley, en particular mediante la ampliación de la capacidad de análisis de riesgo. Aquí, la amenaza a los derechos humanos no se debe a un cambio de política hacia el control de 'riesgo', pero se puede encontrar en la erosión, el desplazamiento o la desestabilización de la división público-privado.

En tal ambiente, los derechos humanos no dan una respuesta obvia, ya que su autoridad es igualmente amenazada por los mismos acontecimientos. El 'derecho a la privacidad' continuara defendiendo y proclamando la primacía de la persona como un 'sujeto de derechos' (es decir, cuya autonomía se puede suponer) mientras que proporciona poca o ninguna protección de las diversas fuentes de inestabilidad que afectan o desestabilizan al individuo como un ser efectivamente autónomo.

En la medida en que la recolección de datos plantea riesgos para la autonomía individual y los derechos que la abarcan, la ley actual de los derechos humanos y la práctica no ofrecen remedios obvios. ¿Cómo responder a este desafío? Si insistimos en el derecho a la privacidad y a la libertad de información, estos no parecen entrar en sintonía para hacer frente a la inestabilidad de un mundo saturado de datos. Por tanto: ¿debemos apuntar a alguno de los nuevos instrumentos que nos proporcionan los derechos humanos?, o tal vez ¿los litigios que desarrollan la ley?, o ¿exigir un nuevo examen acerca de los principios básicos de los derechos humanos en sí mismos, es decir, una renovación de los derechos humanos? Como una especie de vuelta a lo básico.

En este último sentido, podría ser posible examinar los derechos humanos como una fuente de autonomía, en el espíritu habermasiano. Habermas argumenta a favor de una forma fuerte de interdependencia e indivisibilidad de los derechos humanos. En esta visión, los

derechos sociales y económicos, así como los derechos civiles y políticos, proporcionan la base de la autonomía. Tal argumento sugiere que el 'interés público' requiere del apoyo y la preservación de la autonomía de cada miembro del público, entendido este como persona privada. Por el contrario, el fracaso constante para cumplir con los derechos sociales y económicos podría, en este punto de vista, socavar la pretensión de que el Estado sea garante del interés público.

El incumplimiento de los derechos sociales y económicos universalmente o incluso para su consecución de manera significativa en el ámbito local indica que la privacidad y la autonomía de todos no se conservan en todo caso como una cuestión de orden público y de derecho. La ruta hacia la revitalización del poder privado, se encuentra, paradójicamente, al reafirmar el interés público y, en particular, los derechos que se pretenden a menudo oponerse a lo privado: los derechos sociales y económicos.

En resumen, no está claro que la legislación y práctica de los derechos humanos están equipados para hacer frente a la serie de problemas destacados en el presente trabajo de grado, a saber: la desestabilización o reconfiguración de los límites personales; de la frontera entre lo privado y lo público; y de la que existe entre el nivel nacional e internacional. Asimismo, no es claro cómo un sistema de derechos humanos centrado en el Estado puede hacer frente a las asimetrías producidas por flujos masivos de datos transnacionales. El presente trabajo no se ha ocupado sistemáticamente de las deficiencias de las leyes pertinentes de derechos humanos en cada dominio en cuestión. El siguiente paso en la investigación podría apuntar a delinear esto de una manera más precisa, además de sugerir cómo los derechos humanos u otras armaduras normativas podrían ser reconfiguradas para responder mejor a las ansiedades y vulnerabilidades identificadas aquí.

Finamente, el presente trabajo ha sugerido que la situación actual en este ámbito se caracteriza principalmente por su novedad, además de mostrar la brecha que se ha abierto en el plano normativo, así que para abordar esta brecha se requerirá recurrir a una nueva arquitectura normativa, mejor equipada para desafiar tanto a la vigilancia como a la seguridad de la información.

CONCLUSIONES

En el transcurso de este trabajo de grado hemos sugerido que las ansiedades asociadas con la recolección de datos son profundas e importantes, pero que no se articulan con facilidad en términos de derechos humanos, en especial, con el 'derecho a la privacidad'. Esto es en parte debido a que la articulación jurídica del derecho a la privacidad es inadecuada para este tipo de ansiedades contemporáneas.

Sin embargo, también se hace un reclamo mayor, a saber: que la experiencia contemporánea de la recolección y acumulación de datos está transformando nuestras nociones de privacidad más allá de su reconocimiento, ya que la exposición de la inestabilidad de la base filosófica e ideológica sobre la que se asienta, la hacen inoperante en esta 'era de la comunicación'.

En particular, las alegaciones a la autonomía en la que la privacidad estaba destinada a garantizarla, funcionaba más bien como una 'idea regulativa', que como un estado alcanzado. No obstante, no solo tenemos poco o ningún control sobre los datos que se recopilan acerca de nosotros, ni siquiera podemos controlar los datos que generamos nosotros mismos. Las tendencias recientes han debilitado nuestra sensación de control en muchos aspectos, al tiempo que nos obliga a reconocer que nuestro 'control' en cualquier caso es más una aspiración, que una realidad.

El grado en que estos acontecimientos afectan a los individuos varía ampliamente. En términos de especificidad, sin embargo, el efecto es probablemente caracterizado como una pérdida efectiva o aparente de la autonomía, es decir, se produce una noción de vulnerabilidad o precariedad en el individuo. Cuatro factores pueden ser identificados como

posibles y pertinentes a este respecto, además podrían estar ubicados como causas que contribuyen a la mencionada ansiedad, siendo las fuentes potencialmente acumulativas de la vulnerabilidad individual. Estos son:

(i) El grado en que las personas se proyectan en Internet o se encuentran ampliando progresivamente sus datos personales en la esfera pública a través de los procesos cotidianos de la vida diaria (banca, compras, viajes, y así sucesivamente). Podríamos llamar a esto el peso específico del *Dataverse*.

(ii) El grado en que los individuos están sujetos a una vigilancia proactiva tanto pública como privada. Como ya hemos visto, esta vigilancia hoy en día es demasiado amplia y si bien pueden existir reglamentos que rigen los medios disponibles para la recolección de datos y las circunstancias del almacenamiento, retención y uso, estos reglamentos no han impedido la expansión exponencial de la recopilación de datos en sí. Por otra parte, la base normativa para restringir la recolección de datos, parece incierta en este momento.

(iii) El grado en que los individuos se adaptan a ciertos perfiles o categorías de datos. Asimismo, dichas categorías se escapan a las prohibiciones del derecho, de los derechos humanos o de las restricciones de la ley de protección de datos (en las que se tratan como 'categorías especiales' de datos), es decir, la información de estos perfiles afecta a los individuos sustantivamente.

(iv) El grado de asimetría de la información entre los particulares y las entidades de procesamiento de datos, públicas o privados: esto puede, a su vez, ser una función del territorio en el que viven los individuos o de la disponibilidad de un marco

jurídico para salvaguardar sus intereses. Como hemos visto, la asimetría de la información es fundamental para la recopilación de datos en el sector privado, así como la esfera pública y una fuente omnipresente de la mencionada ansiedad.

El derecho a la privacidad no ha demostrado ser muy útil en la lucha contra las asimetrías de la información y las vulnerabilidades identificadas aquí. Esto es en parte debido a que, en su encarnación más temprana (como un 'derecho a ser dejado solo') no fue concebido en el marco de un mundo de datos ubicuos, por una parte, y, por otra, porque se ha convertido en gran medida en una respuesta a un conjunto diferente de problemas que son tratados como un todo y no como una parte. Sin embargo, el derecho a la privacidad sigue evolucionando en respuesta a la vigilancia contemporánea (en particular) y, sin duda, seguirá teniendo un papel importante en la formación del comportamiento del Estado en este sentido. Aunque no queda claro en la actualidad si está equipado conceptualmente para hacer frente a las principales fuentes de ansiedades contemporáneas acerca de la privacidad, en especial, de la información.

La ley de protección de datos también ha jugado un papel importante en el manejo eficiente de la información. Esta parece estar mejor equipada jurídica y conceptualmente, sin embargo, presenta falencias para orientar los límites de la recolección, análisis, almacenamiento y uso de los datos personales. La ley de protección de datos tiende a requerir burocracias para tratar los datos con cuidado, anonimizar cierta información, agregando y analizando cuidadosamente, notificando a ciertos titulares de los usos a los que su información puede ser expuesta. Como libro de reglas de la mediación entre el ciudadano y el Estado, la ley de protección de datos, al estilo europeo, está diseñada para generar confianza. Sin embargo, nuestras ansiedades se deben a una percepción de la saturación de los datos o la sensación de que hemos perdido el control de la extensión y localización de la información relativa a los mismos, por tanto, dicha ley no está bien equipada para dar una solución real al problema.

En este trabajo de grado señalamos que las preocupaciones acerca de la privacidad surgen en diversos campos, en algunos de éstos los demás derechos humanos podrían ser más relevantes que el propio derecho a la privacidad. Ya que la privacidad es conceptualmente cercana a un amplio espectro de los derechos humanos. En este orden de ideas, Jenny Thompson señaló que el derecho a la privacidad podría articularse mejor a través de otros derechos humanos, como son: derechos de propiedad; libertad de expresión y de asociación; libertad de información; prohibición de la discriminación; el debido proceso; incluso el derecho a no ser torturado.

Si es así, surgen dos hipótesis. La primera, es si las amenazas y preocupaciones asociadas con el auge de Internet y el *Dataverse* podrían ser mejor abordadas o incluso evitarse con el uso de otras protecciones de los derechos humanos en vez que las protecciones del derecho a la privacidad. Empero, se necesitará de una mayor investigación para responder a esta afirmación, pero sobre la base de la investigación superficial hecha en estas páginas, hay pocas razones para ser optimistas.

La segunda, es si la transformación de la vida privada representa una amenaza más amplia a los derechos humanos. Esto sería así si la pérdida de la autonomía individual o la dilución de la noción de persona privada autónoma, debilitan o amenazan con socavar la coherencia de los derechos humanos o la práctica de los derechos humanos en sí misma. Por ello, una amenaza más amplia sobre los derechos humanos requerirá una respuesta que se base en recursos distintos a los derechos humanos por sí solos y, en última instancia, el objetivo hacia la reconstitución de los propios derechos humanos, como un recurso político y legal.

Estas preocupaciones se agudizan cuando consideramos la vigilancia de datos en el resto del mundo. Los derechos humanos, en general, y el derecho a la intimidad, en particular, es probable que sean de gran valor en el tratamiento del fenómeno creciente de extensa

recopilación, intercambio, almacenamiento y análisis transnacional de datos. Internet y el *Dataverse* tienden a escapar a una regulación nacional. Así pues, cuando se produzcan casos de acoso o confusión de identidad, derivada de la vigilancia de datos de cualquier tipo, estas siguen siendo mejor abordadas a través del lente de los derechos humanos básicos tradicionales.

El aumento de la recolección de datos, el énfasis en una concepción aparentemente superficial de la vida privada, la falta de voluntad de algunos Estados a adherirse a muchos derechos humanos estándar, la promoción de la expansión de Internet y el *Dataverse*, el grado de liberación y el deseo que las personas experimentan cuando participan en la tecno-cultura, el grado en que la vigilancia de datos reconfigura el concepto de persona y objetiviza las categorías de privacidad y persona (a través de gestión de riesgos y análisis de datos): todos estos elementos parecen apuntar a una relación cada vez más compleja entre el interesado y el *Dataverse*, cuyas implicaciones tan solo ahora estamos empezando a comprender.

No obstante, los defensores de los derechos humanos captan las herramientas disponibles y las aplican a las complejidades florecientes del *Dataverse* a pesar de sus limitaciones. Esto puede abrir un espacio para que los principios básicos de los derechos humanos fundamentales sean reconsiderados y actualizados a esta nueva problemática.

Por tanto, hemos tratado de presentar la discusión acerca de la recopilación de datos, planteando algunas de las cuestiones más amplias en cuanto a sus impactos sobre los derechos humanos. Se ha indicado un espectro de problemas de derechos humanos relacionados con este dominio, cuestionando el grado en que el derecho a la privacidad (y sus protecciones afines) es adecuado para el problema, articulando la preocupación más

amplia de que el desafío de los datos en todas partes es un desafío a los derechos humanos en su conjunto.

No se ha llevado a cabo un análisis detallado de cada uno de los derechos afectados, ni tampoco buscamos articular las recomendaciones para los derechos humanos o incluso el tratamiento del *Dataverse*. Estas tareas podrán realizarse mejor en una siguiente etapa.

BIBLIOGRAFÍA

Álvarez, Rafael (1994). *Estadística multivariante y no paramétrica con SPSS.* Madrid: Ediciones Díaz de Santos, S.A.

Allen-Castellitto, Anita (2001). *Privacy Law and Society*. New York: Thomson West.

Arendt, Hannah (2001). *Public goods, private goods*. Princeton: Princeton University Press.

Branscomb, Anne W. (1983). "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition". En: *Vanderbilt Law Review*, No. 36. pp. 985-312.

Cate, Fred (1997). *Privacy in the information age*. Washington D.C.: Brookings Institution Press.

Froomkin, Michael (2000). "The Death of Privacy?" En: *Stanford Law Review*, No. 52. pp. 1461-1543.

Gormley, Ken (1991). *One Hundred Years of Privacy*. Pittsburgh: University of Pittsburgh Press.

Habermas, Jürgen (1994). *Structural transformation of the public sphere*. New York: Polity Press.

Hixson, Richard (1987). *Privacy in a public society: Human rights in conflict*. London: Pan.

Horowitz, Shale (2004). *Human rights and societies in transition: Causes, consequences, responses*. Tokyo: Tokyo University Press.

James, Michael (1994). *Privacy and human rights*. New York: UNESCO.

Kitiyadisai, Krisana (2005). "Privacy rights and protection: Foreign values in modern Thai context". En: *Ethics and Information Technology*, Vol. 7, No. 1. pp. 17-26.

Litman, Jessica (2000). "Information Privacy/Information Property". En: *Stanford Law Review*, No. 52. pp. 1283-1313.

Mayer-Schönberger, Viktor (2009). *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

Mell, Patricia (1996). "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness". En: *Berkeley Technology Law Journal*, Vol. 11, No. 1. pp. 3-92.

Nakada, Makoto & Tamura, Takanori (2005). "Japanese conceptions of privacy: An intercultural perspective". En: *Ethics and Information Technology*, Vol. 7, No. 1. pp. 27-36.

Overton, Ben & Giddings, Katherine (1997). "The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion". En: *Florida State University Law Review*, Vol. 25. pp. 25-56.

Pogge, Thomas (2002). *La pobreza en el mundo y los derechos humanos.* Barcelona: Editorial Paidós.

Posner, Richard (2013). *Reflections on Judging*. Cambridge: Harvard University Press.

Ramsay, Peter (2008). "The Theory of Vulnerable Autonomy and the Legitimacy of the Civil Preventative Order". En: *LSE Legal Studies Working Paper*, No. 1. pp. 2-29.

Rotenberg, Marc (2001). *Consumer Privacy in the E-Commerce Marketplace*. Las Vegas: EPIC Publishing.

Schwartz, Paul M. (2000). "Internet Privacy and the State". En: *Connecticut Law Review*, Vol. 32. pp. 815-859.

Solove, Daniel (2001). "Privacy and Power: Computer Databases and Metaphors for Information Privacy". En: *Stanford Law Review*, Vol. 53. pp. 1393-1462.

Yao-Huai, Lü (2005). "Privacy and data privacy issues in contemporary China". En *Ethics and Information Technology*, Vol. 7, No. 1. pp. 7-15.

Tsoukala, Anastassia (2008). "Security, Risk and Human Rights: A Vanishing Relationship?" En: *CEPS Special Report/September*. pp. 2-17.

Warren, Samuel and Brandies, Louis. (1890). "The right to privacy". En: *Harvard Law Review*, No. 193. Harvard University Press.

Jurisprudencia

Corte Constitucional. Sentencia T-414 de 1992. Magistrado Ponente: Ciro Angarita Barón.

Corte Constitucional. Sentencia T-1202 de 2000. Magistrado Ponente: Vladimiro Naranjo Mesa.

Corte Constitucional. Sentencia T-437 de 2004. Magistrado Ponente: Clara Inés Vargas Hernández.

Corte Constitucional. Sentencia C-640 de 2010. Magistrado Ponente: Mauricio González Cuervo.

Corte Constitucional. Sentencia T-260 de 2012. Magistrado Ponente: Humberto Antonio Sierra Porto.