LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA RESPECTO A LAS EMPRESAS TRANSNACIONALES A PROPÓSITO DEL CASO GOOGLE VS SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

The protection of personal data in Colombia with respect to Transnational Corporations regarding the case Google vs Superintendencia de Industria y Comercio

Natalia Serna Molina
Isabela Murillo Quiroz

Trabajo de Grado

Asesor
José Luis González Jaramillo

UNIVERSIDAD EAFIT
ESCUELA DE DERECHO
DERECHO
MEDELLÍN
2025

RESUMEN

La economía digital ha exigido que las empresas presten sus servicios por medios tecnológicos. En el desarrollo de su actividad realizan el Tratamiento de Datos Personales de sus consumidores, con distintos fines y por diferentes medios. En Colombia, dicho tratamiento, es regulado principalmente por la Ley 1581 de 2012. En este contexto, las empresas transnacionales han planteado un reto en cuanto al alcance territorial de la normatividad, tanto en Colombia como en otros Estados. Esta problemática será analizada, a la luz del caso Google LLC vs la Superintendencia de Industria y Comercio, por ser la primera una sociedad representativa en el mercado internacional, y la segunda la entidad encargada de garantizar la protección de los datos personales en Colombia.

Palabras clave: Empresas Transnacionales, Google Colombia Limitada, Google LLC, Ley 1581 de 2012, Protección de Datos Personales, Superintendencia de Industria y Comercio, Territorialidad, Tratamiento de Datos Personales.

ABSTRACT

The digital economy has required companies to provide their services through technological means. In the development of their activity, they process personal data of their consumers for different purposes and by different means. In Colombia, such processing is mainly regulated by «*Ley 1581 de 2012*». In this context, transnational companies have posed a challenge in terms of the territorial scope of the regulations, both in Colombia and in other jurisdictions. This problem will be analyzed in the light of the case Google LLC vs. the «*Superintendencia de Industria y Comercio*», since the first one is a representative company in the international market and the latter is the entity in charge of guaranteeing the protection of personal data in Colombia.

Key words: Google Colombia Limitada, Google LLC, «Ley 1581 de 2012», Personal Data Processing, Personal Data Protection, Territoriality, Transnational Corporations, «Superintendencia de Industria y Comercio».

Tabla de contenido

Introducción

Actualmente la tecnología ha tenido un rol fundamental en la propagación de la globalización. Lo anterior, ha motivado numerosos cambios y evoluciones por parte de los Estados para reglamentar las nuevas dinámicas que se presentan en términos de educación, cultura, comunicación, economía, entre otros. Uno de los desarrollos más significativos que ha traído esta nueva era es el impulso de empresas que desarrollan su objeto social en ámbitos internacionales. Las cuales tienen una estructura centralizada con una base de operaciones regida por la legislación de ese país de origen, y tienen injerencia económica en otros países por medio de inversiones directas o filiales de conformidad con la legislación del país huésped (Teitelbaum, 2012). Adicionalmente, se han adaptado a un modelo de negocio en el cual ofrecen sus bienes o servicios por medio de plataformas digitales.

Ahora bien, el Tratamiento de Datos Personales (en adelante «TDP») ha sido una herramienta, inherente a la actividad comercial de las empresas, que les permite ofrecer nuevos servicios, conocer el mercado y tomar decisiones corporativas de acuerdo con los indicadores que resulten del estudio de estos. No obstante, la recolección de datos ya no se limita a los datos mínimos para identificar al usuario como: nombre, correo electrónico, y edad. Sino que además, comprende datos con mayor grado de privacidad y sensibles, tales como: la ubicación, el historial, la dirección, los chats personales, entre otra información que tiene un carácter comercial para las empresas, consolidándose como bienes transables en el mercado.

Cabe aclarar, que, si bien todo tratamiento de datos no se debe dar en medio de una relación comercial, como, por ejemplo, cuando se llena una encuesta para información estadística del Estado. Para efectos del análisis del presente trabajo y teniendo claro que, el TDP realizado en medio de las relaciones comerciales es uno de los más comunes y frecuentes en la actualidad, el análisis se va a circunscribir a el TDP realizado en medio de una relación comercial entre las

Empresas Transnacionales (en adelante «ETN») y las personas. Es decir, cuando confluyen en las personas la calidad de titular y consumidor.

Cobra especial relevancia estudiar la regulación de los datos personales en cuanto, no solo se tratan más tipos de datos que antes, sino que se recolectan de muchas más personas. En el caso de Colombia para febrero de 2024, según DataReportal, habían 39.51 millones de usuarios de internet, el 70.3% de los mismos usaban al menos una red social (Kemp, 2024).

Resulta evidente la problemática de que los datos sean tratados por ETN sin una jurisdicción clara aplicable. De este modo, el objetivo principal de esta investigación es reflexionar sobre el alcance de la normatividad relativa al tratamiento de datos personales en Colombia aplicable a las empresas transnacionales. En el marco del caso Google LLC vs. la Superintendencia de Industria y Comercio (en adelante «SIC») (y en conjunto «Caso Google vs la SIC») [1].

Este objetivo se alcanzará por medio de una metodología cualitativa, descriptiva y jurídica formal basada en un análisis normativo, jurisprudencial y doctrinal. Adicionalmente, usando como referencia el caso mencionado se expondrán reflexiones que surgen del tema de estudio, resaltando: (i) la legislación nacional actual en materia de TDP; (ii) las prácticas transnacionales de las empresas que recolectan y usan datos personales; (iii) el límite territorial de las normas nacionales; y (iv) las regulaciones internacionales en materia de TDP y ETN.

El presente trabajo se compone de tres secciones divididas en capítulos. En la primera sección, se aborda la legislación aplicable a TDP en el ordenamiento jurídico colombiano con el objetivo de identificar las definiciones, principios, prohibiciones, sujetos, obligaciones, derechos

[1] La Superintendencia de Industria y Comercio (SIC) a propósito de un estudio realizado por la Comisión Federal de Comercio de Estados Unidos requiere, por medio de actos administrativos a Google LLC y a Google Colombia Limitada para que demuestren el cumplimiento de lo establecido en la Ley de Protección de Datos Personales en Colombia. Acto seguido, Google LLC demanda la nulidad de las Resoluciones que fueron emitidas ante el Tribunal Administrativo de Cundinamarca.

y deberes que trae esta. En la segunda sección se estudia el caso Google LLC vs la SIC, donde se expone: (i) la cronología de los hechos y argumentos en medio de esta disputa jurídica; (ii) el papel de las ETN, brindando un contexto general, detectando la normatividad aplicable a nivel nacional e internacional y los efectos de la territorialidad en ellas; y (iii) el sistema normativo de la Unión Europea, Estados Unidos de América y países iberoamericanos indicando obligaciones, consecuencias jurídicas y limitaciones en materia de TDP. Finalmente, en la tercera sección se abordan las reflexiones que suscitan los temas expuestos en las secciones precedentes con el fin de analizar del alcance de la protección de datos personales en Colombia aplicable a las ETN.

Sección I: El Tratamiento de Datos Personales en el Ordenamiento Jurídico Colombiano

La Ley 1266 de 2008 fue la primera normatividad encaminada a proteger el derecho de *habeas data* en Colombia, sin embargo, es una norma sectorial que protege únicamente los datos

que surgen con ocasión de obligaciones dinerarias (Remolina-Angarita, 2010, p.511). Tiene por objeto la regulación y el TDP de las bases de datos financieras, crediticias, comerciales, de servicios y las provenientes de terceros países.

A raíz de la evidente necesidad de proteger los datos personales en los demás sectores y acompañado del aumento exponencial del uso de las tecnologías a nivel global, se comenzaron a implementar normatividades que permitieron regular en abstracto el TDP. En Colombia, por medio del Proyecto de Ley Estatutaria 184 de 2010 se propuso lo que actualmente se conoce como la Ley 1581 de 2012, Ley de Protección de Datos Personales, que tiene por objeto dictar «disposiciones generales para la protección de datos personales».

La Corte Constitucional en la Sentencia C-748 de 2011 realizó un análisis de constitucionalidad extenso y minucioso del articulado del Proyecto de Ley Estatutaria. Inicialmente, hace referencia al origen histórico del derecho fundamental al *habeas data*. Posteriormente, presenta los distintos modelos de protección de datos y concluye que, con esta ley se pretende aplicar un modelo híbrido de protección, «en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato» (p.8).

Por su parte, los siguientes decretos reglamentan los aspectos principales de las leyes mencionadas anteriormente. El Decreto 1074 de 2015 «Por medio del cual se expide el Decreto Único Reglamentario del sector Industria, Comercio y Turismo», en su capítulo 25, presenta: (i) el concepto y el uso de la autorización; (ii) los requerimientos de la política de tratamiento de la , información; (iii) las transferencias y transmisiones de datos internacionales; (iv) la aplicación del principio de responsabilidad demostrada; (v) las normas corporativas vinculantes; entre otros. De

igual manera, el Decreto 1081 de 2015 «Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República» regula entre otros la publicación y divulgación de la información pública y datos abiertos.

Asimismo, el Decreto 090 de 2018 «Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Único Reglamentario del Sector Comercio, Industria y Turismo» reglamenta el registro de bases de datos públicas y privadas. Finalmente, el Decreto 255 de 2022 «Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países» desarrolla con más especificidad las normas corporativas vinculantes y el procedimiento para autorizarlas, así como, la certificación de buenas prácticas.

A partir de las normatividades mencionadas anteriormente, se detallarán las definiciones, principios, prohibiciones, sujetos, derechos, deberes, y el alcance que traen las normas los cuales permiten comprender y especializar el tema de estudio y que son más pertinentes en función de su relevancia para el objetivo del presente.

Capítulo I: Conceptos Introductorios

Para comprender el alcance del TDP este capítulo abordará tres elementos transversales y esenciales: (i) la definición del TDP, por ser el mismo el que delimita las operaciones sujetas a esta legislación; (ii) la definición de la autorización como requisito previo y primordial al TDP,

entendiéndola como mecanismo que legitima la ejecución de este, estableciendo un vínculo entre Titular y Responsable; y (iii) los principios que orientan esta actividad por su carácter general y obligatorio.

Tratamiento de Datos Personales

De acuerdo con lo expuesto al principio de este escrito los datos personales actualmente han cobrado gran relevancia, actualmente los mismos se encuentran en la economía, la política, la salud, la cultura, entre otros. La Ley 1266 de 2008 define los datos personales como la información asociada a una persona natural o jurídica, y aquellos pueden ser públicos[2], privados[3], semiprivados[4] o sensibles[5].

En esta línea, según la Corte Constitucional la jurisprudencia ha resaltado ciertas características que permiten diferenciar los datos personales de otro tipo de dato:

> i) Estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) de su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (C-748, 2011, p.9).

Así pues, el TDP según la Ley 1581 de 2012 es cualquier ejercicio realizado sobre los datos personales del Titular que impliquen, entre otras cosas: (i) su **recolección** por medio de encuestas,

---

[2] Son datos de libre acceso, tratamiento y circulación. Para su identificación, es necesario acudir a la ley o a la Constitución; además, constituye un criterio residual de la clasificación de los datos personales, en caso de no poder catalogarlos como semiprivados o privados (Ley 1266 de 2008, artículo 3 literal f).

[3] Datos que tiene una naturaleza íntima y reservada para el Titular, en este sentido, sólo es relevante para el mismo (Ley 1266 de 2008, artículo 3 literal h).

[4] Son una categoría híbrida, que, por su naturaleza, no son públicos pero su conocimiento y divulgación le interesan no sólo al Titular sino a un grupo de la sociedad por determinadas finalidades. Con mayor frecuencia se evidencia su utilización en el sector financiero y comercial (Ley 1266 de 2008, artículo g).

[5] Son los datos privados que por su contenido en caso de ser indebidamente usados, divulgados o tratados pueden tener consecuencias negativas que den lugar a discriminación del Titular (Ley 1581 de 2012, artículo 5).

fuentes de captura automática, experimentación, entre otros; (ii) su **almacenamiento** en bases de datos físicas o electrónicas; (iii) su **uso** para la toma de decisiones informadas, manejo de preferencias, marketing, investigaciones, entre otros; (iv) la **circulación** en redes públicas o privadas; y (v) la **supresión** de los datos que hayan sido recopilados siempre y cuando no haya prohibición contractual o legal al respecto.

Es necesario resaltar que las normas que buscan regular el TDP pretenden proteger el derecho de *hábeas data*, desarrollado por medio de los artículos 15 y 20 de la Constitución Política de Colombia de 1991, que consagran el derecho a la intimidad, al buen nombre y a la libertad de expresión. Este derecho según la Corte Constitucional se manifiesta por tres facultades concretas referidas a los datos recolectados y almacenados:

> a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad (SU-082, 1995, p. 8).

Es importante resaltar que el TDP por regla general solo se puede realizar previa autorización expresa por parte del Titular.

Autorización

La autorización consiste en el consentimiento previo, expreso e informado, es decir: (i) se debe solicitar por parte del Responsable y/o Encargado antes de llevar a cabo el TDP; (ii) inequívocamente debe expresarse la aceptación; (iii) debe presentar suficiente información para conocer a cabalidad las características, límites y condiciones a los cuales se van a sujetar los datos del Titular; y (iv) la misma puede ser obtenida por cualquier medio que permita su posterior consulta.

Es dable resaltar que, en los casos en los cuales los datos sean: (i) públicos; (ii) requeridos por entidad pública o administrativa; (iii) exigidos en casos de urgencia; (iv) para fines científicos; o (v) relacionados con el Registro Civil[6], no será obligatoria esta autorización.

La autorización que es exigida por el artículo 4 numeral C de la Ley 1581 de 2012 en las relaciones comerciales se puede asimilar a la expresión de voluntad libre de fuerza, error y dolo que debe emitir el Titular para la celebración del negocio jurídico para consecuentemente disfrutar de los servicios ofertados por las empresas. De este modo, para el caso que compete a este escrito, la relación contractual se asimila a un contrato de adhesión, en donde, una parte ofrece sus servicios, bajo una serie de condiciones comerciales que le expone al consumidor, acompañado de un Aviso de Privacidad, por medio del cual el Responsable del TDP informa al Titular: (i) las políticas de tratamiento de información; (ii) los mecanismos para tener acceso a las mismas; y (iii) la finalidad del tratamiento de esos datos. Esta notificación puede realizarse de manera escrita o verbal (Decreto 1074, 2015, artículo 2.2.2.25.1.3). De allí, el Titular acepta o no las estipulaciones planteadas, es decir, no tiene margen de negociación.

Partiendo del entendimiento de las definiciones previamente expuestas es necesario comprender los principios que integran transversalmente las normatividades que regulan el TDP.

Principios

A continuación, se enlistan los principios generales que se pueden identificar dentro de la Ley 1581 de 2012 y de la Ley 1266 de 2008 del TDP. Los cuales como mandato general de optimización instan a los partícipes en las operaciones de TDP a alcanzar los fines propuestos, desplegando las acciones necesarias con la diligencia y cuidado debida. Adicionalmente, revisten

[6] Tomado de la Ley 1581 de 2012 artículos 9 y 10; y la Ley 1266 de 2008 artículo 6.

de una gran importancia ya que son uno de los puntos de interconexión con los ordenamientos internacionales, puesto que, entre ellos coinciden en algunos de estos.

i. Principio de legalidad: es una actividad reglada que se debe sujetar a las normatividades propias de ella.

ii. Principio de finalidad: la administración de datos personales debe obedecer a una finalidad legítima y debe ser informada al Titular de la información por medio de la autorización.

iii. Principio de acceso y circulación restringida: el tratamiento y acceso a los datos personales del Titular sólo podrá realizarse por personas autorizadas por éste o por la ley, en este sentido, no pueden estar disponibles en ningún medio de comunicación masivo abierto al público.

iv. Principio de libertad: el tratamiento, obtención y divulgación de datos personales sólo podrá realizarse con el consentimiento previo, expreso e informado del Titular.

v. Principio de temporalidad de la información: una vez cumplida la finalidad acordada para la recolección de la información del Titular, esta no podrá ser compartida con terceros.

vi. Principio de veracidad o calidad: la información debe ser «veraz, completa, exacta, actualizada, comprobable y comprensible»[7].

vii. Principio de interpretación integral de derechos constitucionales: las normatividades que reglamentan el TDP deben ser congruentes con el derecho de *habeas data.*

viii. Principio de transparencia: el Titular tiene el derecho de acceder en cualquier momento y sin restricciones a los datos que le competen.

[7] Tomado de la Ley 1581 de 2012, artículo 4 literal d.

ix. Principio de seguridad: la información contenida en las bases de datos debe tener «medidas técnicas, humanas y administrativas»[8] que eviten su adulteración, pérdida o acceso no autorizado.

x. Principio de confidencialidad: debe ser garantizada la reserva de la información obtenida antes, durante y posterior al TDP.

xi. Principio de favorecimiento a una actividad de interés público: en las actividades de «administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países»[9] se debe favorecer el interés público y será gratuita.

Aunado a lo anterior, la Corte Constitucional en la Sentencia C-748 de 2011 pone de presente algunos principios jurisprudenciales y constitucionales relevantes en la materia sin que hayan sido incluidos expresamente en la ley:

xii. Principio de individualidad: los datos no podrán ser compartidos entre diferentes bases de información sin autorización expresa del Titular (p.178).

xiii. Principio indemnizatorio: quien trate los datos está llamado a indemnizar los perjuicios causados por las fallas que se ocasionen en su proceso de TDP (p.197).

Además de estas directrices generales las regulaciones establecen para los sujetos involucrados una serie de derechos, deberes y prohibiciones que deben ejecutarse como obligaciones de resultado, es decir deben cumplirse de forma completa, oportuna, y sin defectos.

[8] Tomado de la Ley 1581 de 2012 artículo 4 literal g.
[9] Tomado de la Ley 1266 de 2008, artículo 10.

Capítulo II: Sujetos, Derechos y Deberes

En medio de la relación que surge en el TDP, el Titular es quien posee los derechos frente a los demás actores. A su vez, a estos últimos como sujetos activos del tratamiento se les imponen obligaciones y prohibiciones que rigen su actuar.

En primer lugar, el **Titular** es la «persona natural o jurídica cuyos datos personales son objeto de Tratamiento»[10], en este sentido, es aquel que está expuesto a vulneraciones y al cual correlativamente la ley pretende proteger. A este se le otorgan una serie de derechos que pueden ser ejercidos por: (i) el mismo Titular cuando acredite su identidad; (ii) sus causahabientes; (iii) su representante legal; o (iv) por estipulación de otro o para otro[11]. Estos derechos consisten en: conocer, actualizar, rectificar, controlar, vigilar, añadir, suprimir y modificar datos personales que se encuentren en cualquier base de datos del sector público o privado; y en el registro individual vinculado a la identificación del mismo siempre y cuando no contradigan disposiciones legales o contractuales expresas. Lo anterior, se podrá realizar por medio de los mecanismos gratuitos los cuales están obligados a facilitar tanto el Responsable como el Encargado.

En segundo lugar, el **Responsable del Tratamiento** es aquella «persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos»[12] [énfasis propio]. Este tiene la obligación de suministrar al **Encargado del Tratamiento** la información previamente autorizada por el Titular de manera «veraz, completa, exacta, actualizada, comprobable y comprensible»[13]. Por otro lado, el Encargado es una «persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento» [énfasis propio][14].

---

[10] Tomado de la Ley 1581 de 2012, artículo 3 literal f.
[11] Tomado del Decreto 1074 de 2015, artículo 2.2.2.25.4.1.
[12] Tomado de la Ley 1581 de 2012, artículo 3 literal e.
[13] Tomado de la Ley1581 de 2012, artículo 17.
[14] Tomado de la Ley 1581 de 2012, artículo 3 literal d.

Asimismo, el Responsable y/o Encargado deben proteger integralmente el derecho de *habeas data* del Titular, por lo tanto, proporcional a su naturaleza y riesgo se les exigen una serie de obligaciones encaminadas a este fin. Es importante resaltar que estas calidades pueden confluir o no en la misma persona.

Paralelamente, se les exhorta a incorporar un manual interno físico o electrónico de políticas y procedimientos que sean congruentes con lo que ordena la normatividad vigente y el tipo de datos que van a ser tratados. Igualmente, deben informar al Titular cualquier actualización sobre el mismo, previo a la recolección, por medio de un Aviso de Privacidad. Circunstancia que le permite al Titular conocer conscientemente cómo y cuál es el manejo que le están dando a la información suministrada.

Estos sujetos, tienen que adoptar procedimientos específicos internos para evitar la vulneración en la seguridad de los datos. Además, deben tener comunicación constante y certera con la SIC para alertar posibles transgresiones a la seguridad de los mismos. También, han de suprimir los datos cuya finalidad ya haya sido cumplida. Adicionalmente, en lo que atañe a la autorización están obligados a que pueda ser conocida y revocada por los Titulares en cualquier momento salvo disposición legal o contractual en contrario.

En tercer lugar, la SIC es la entidad encargada de vigilar y sancionar aquellos sujetos partícipes en el TDP por medio de la Delegatura para la Protección de Datos Personales (en adelante la «Delegatura»). Sus funciones se enmarcan en: (i) velar por el cumplimiento de la legislación en materia de protección de datos personales; (ii) adelantar investigaciones de oficio o a petición de parte y ordenar las medidas necesarias para hacer efectivo el derecho de *habeas data;* (iii) sugerir ajustes para adecuar o corregir la normatividad que resulten acordes con la evolución tecnológica; (iv) proferir declaraciones de conformidad con las transferencias internacionales de

datos; (v) administrar el Registro Nacional Público de Bases de Datos; (vi) imponer instrucciones para que las operaciones de los Responsables y los Encargados del Tratamiento se adecúen a la normatividad vigente; (vii) requerir a entidades internacionales en el escenario en el que se vean afectados los derechos de los Titulares fuera del territorio colombiano; y (viii) regular las normas corporativas vinculantes[15].

Así, el actuar de la SIC debe ir encaminado a la prevención y vigilancia. Permitiendo que entre otras cosas, a pesar del carácter de adhesión que tiene la relación comercial que da lugar al TDP, no se instauren cláusulas abusivas ni se dé el aprovechamiento de los Titulares como parte débil de la relación contractual incluso en instancias internacionales.

Finalmente, en las normatividades de protección de datos personales es posible evidenciar algunas prohibiciones: el tratamiento de datos sensibles; el TDP de niños, niñas y adolescentes (en adelante «NNA»); y la transferencia de datos a terceros países cuando estos no tengan una adecuada protección de los datos y establecen las excepciones a cada una de ellas.

En suma, los sujetos[16] que interactúan con los datos objeto de protección de estas normatividades, se encuentran bajo el control, vigilancia y dirección de la SIC. Empero, en la actualidad ante la globalización, la interconexión tecnológica, y la creciente conectividad del país, las funciones de vigilancia y control de la Delegatura hacia los sujetos previamente relacionados se han visto retadas. Lo anterior se debe a que se tratan los datos primordialmente en el ciberespacio, lugar en el que se discute su jurisdicción. Aunado a lo anterior, los medios

[15] Tomado de la Ley 1581 de 2012, artículo 21.

[16] Además de los sujetos mencionados con anterioridad, la Ley 1266 de 2008 también declara que pueden participar en el TDP: la Fuente de Información, el Operador de Información y el Usuario. Los cuales pueden confluir o no en el mismo sujeto. Así, se entiende Fuente de Información como aquella persona natural o jurídica que con ocasión de una relación comercial o legal con el Titular suministra los datos de este último a un Operador de Información que los administra y a su vez los entrega a un Usuario Final.

tecnológicos son utilizados por ETN que no cuentan con un domicilio en el ordenamiento donde recolectan o tratan los datos, tal y como pasa en Colombia.

Capítulo III: Ámbito de Aplicación

En los capítulos anteriores se desarrollaron los conceptos introductorios para esclarecer qué se puede considerar como TDP, los sujetos que intervienen en dicho tratamiento, junto con sus derechos, obligaciones y deberes. Empero, es imprescindible analizar el ámbito de aplicación de la Ley 1581 de 2012 dado que, la misma no contempla ni todos los tratamientos, ni todos los tipos de datos personales y su aplicación varía según el sujeto que realiza el tratamiento.

Así, el artículo 2 de la Ley 1581 de 2012 delimita el ámbito de aplicación de la legislación general sobre protección de datos personales en Colombia. Establece los criterios desde un alcance material, territorial y subjetivo en los siguientes términos:

> **Artículo 2°**. ***Ámbito de aplicación*.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.
>
> La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.
>
> El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:
>
> a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley;

b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;

e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;

f) A las bases de datos y archivos regulados por la Ley 79 de 1993.

Parágrafo. Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley.

En términos del ámbito material esta ley no protege todo tipo de datos, únicamente los personales, que se encuentren registrados en cualquier base de datos, y sean susceptibles de tratamiento. Exceptuando las bases de datos y archivos que son enumerados en los literales a – f del presente artículo, que prevén regímenes jurídicos especiales.

Por su parte, respecto al ámbito de aplicación territorial se afirma que, sólo aplicará al TDP realizado dentro del territorio colombiano, independientemente de la nacionalidad o residencia del Encargado o Responsable. Asimismo, se expone que si el tratamiento, es decir cualquiera de las operaciones que se pueden considerar como tal, se realizan por fuera del territorio colombiano es

necesario analizar si al Responsable o al Encargado del mismo le es aplicable la normatividad nacional en virtud de tratados o normas internacionales.

Así entonces, la Ley 1581 de 2012 establece una serie de parámetros claros para evaluar si un determinado TDP se encuentra amparado por la misma. En primer lugar, se debe analizar el dato que pretende ser objeto de protección ¿es un dato personal? y este ¿se encuentra en una base de datos susceptible de tratamiento y no exceptuada en los literales del artículo? Si las respuestas a estas preguntas son afirmativas, en segundo lugar, se deberá identificar cuál o cuáles son las operaciones o conductas que pretenden ser caracterizadas como tratamiento. Respecto a estas conductas es necesario establecer ¿se están realizando dentro del territorio colombiano? Si la respuesta es afirmativa efectivamente es un tratamiento cobijado por la Ley 1581 de 2012. Sin embargo si la respuesta es negativa, en tercer lugar, será necesario individualizar al sujeto que presuntamente es el Encargado o el Responsable del tratamiento y se debe preguntar si ¿hay alguna normatividad internacional que vincule a este con la legislación colombiana? De igual manera, si la respuesta a esta última pregunta es afirmativa, le aplicará la ley, de lo contrario estas operaciones estarán por fuera de la jurisdicción de la misma.

En resumen, la Ley 1581 de 2012 como ley principal de protección de datos en Colombia al contrario de otras normas, tanto colombianas como internacionales, no limita su aplicación al sujeto de protección, por ejemplo, a las personas residentes, domiciliadas y nacionales colombianas. Por el contrario, lo circunscribe al tipo de dato, el lugar donde se realice el tratamiento y a la vinculación del Responsable o Encargado a la legislación colombiana por un tratado o convenio internacional. Lo anterior, presenta un gran reto en la actualidad entre otras cosas dado que el tratamiento mayoritariamente se realiza en el ciberespacio, lugar en el que se discute la jurisdicción de los países y el efecto del principio de territorialidad.

En este contexto, se han abierto numerosos casos a nivel nacional e internacional en los cuales se pone de presente las malas prácticas en términos de TDP de grandes empresas en el mercado que operan por medios electrónicos. Una de las empresas más representativas no sólo por la cantidad de servicios que ofrece sino por el tamaño e injerencia mundial que tiene la misma es Google, la cual ha sido sujeto de investigaciones en diferentes ordenamientos por no cumplir a cabalidad con las políticas de TDP. Colombia no ha sido la excepción como se desarrollará en la siguiente sección.

Sección II: Caso Google vs Superintendencia de Industria y Comercio

Uno de los gigantes tecnológicos a nivel global de los últimos tiempos es Google. Esta empresa comenzó como un motor de búsqueda y «hoy en día, crea cientos de productos que usan miles de millones de personas en todo el mundo, como YouTube, Android, Gmail y, por supuesto, la Búsqueda de Google» (Google, s.f.). Dentro de cada uno de los servicios que ofrece, se tratan los datos de las personas que los utilizan.

Google, ante la alta recolección, uso y en general TDP ha tenido conflictos con la normatividad actual a nivel mundial por no cumplir con los estándares de protección de datos adecuados en términos de las autorizaciones, los datos recolectados, el uso que se les da a los mismos, entre otros. En Colombia, específicamente ha sido señalado por presuntamente no cumplir con lo establecido en la Ley Estatutaria 1581 de 2012, lo cual ha planteado un debate técnico jurídico sobre el alcance de las regulaciones nacionales de protección de datos personales frente a una ETN.

A continuación, se exponen los elementos jurídicos más relevantes que hasta la fecha de la redacción del presente escrito se han presentado en medio de la disputa entre Google LLC, Google Colombia Limitada (en adelante «Google Colombia») y la SIC; los argumentos de cada uno; la implicación de ser una ETN; la relación con la territorialidad de las normas; y los parámetros internacionales exigidos a este tipo de empresas en términos de protección de datos personales.

Capítulo I: Desarrollo del caso

Dentro del presente capítulo se hará un breve resumen de las principales actuaciones jurídicas en medio de esta disputa y lo que la originó. En el desarrollo de las mismas los argumentos de cada parte han sido congruentes, por lo tanto y con el objetivo de no caer en la redundancia, posteriormente se expondrán consolidados los argumentos y las posiciones de cada una.

Antecedentes, cronología y principales actores

Motivada por un estudio realizado por la Comisión Federal de Comercio de Estados Unidos sobre la recolección ilegal que estaba realizando YouTube, de la información personal de NNA sin el consentimiento de sus padres, en el 2020 la SIC emitió las Resoluciones No. 53593 del 03 de septiembre de 2020 y la No. 70315 del 04 de noviembre de 2020. Por medio de estos actos la entidad imparte órdenes administrativas a Google LLC y Google Colombia respectivamente, para que informaran y acreditaran el procedimiento de recolección y autorización de los datos personales efectuado en el territorio colombiano y la finalidad del mismo, con especial enfoque en los datos de los NNA. Este trámite administrativo se identifica con el radicado interno de la SIC No. 19-202397.

Posteriormente, en el año 2021 con motivo de los recursos de reposición y en subsidio apelación interpuestos por Google LLC y Google Colombia se emitieron las Resoluciones No. 14010 del 16 de marzo de 2021, No. 38869 del 24 de junio de 2021, No. 60478 del 21 de septiembre de 2021 y la No. 72775 del 11 de noviembre de 2021 que resolvían dichos recursos. Es preciso resaltar que, si bien el énfasis principal de estas resoluciones es YouTube como servicio que ofrece Google y se concentra en el TDP de NNA, el objeto de este escrito tiene un enfoque general al TDP de las personas en abstracto en los distintos servicios brindados en las plataformas digitales.

Acto seguido, en el mes de abril de 2022, Google LLC radicó una demanda de nulidad y restablecimiento del derecho, subsanada el 09 de agosto de 2023, en contra de las Resoluciones No. 53593, No. 14010 y No. 60478. Estos actos administrativos fueron proferidos por la Delegatura de la demandada, la SIC, y solicitan la medida cautelar de suspensión provisional de los efectos de las resoluciones demandadas. Con ocasión de lo anterior se abrió el proceso judicial en el Tribunal Administrativo de Cundinamarca Sección Primera, Subsección C identificado con el radicado No. 25000234100020220044400 el cual es posible consultar en la Sede Electrónica de la Jurisdicción de lo Contencioso Administrativo de Colombia - SAMAI.

Posteriormente, el 07 de marzo de 2024, el Tribunal admitió la demanda instaurada. El 03 de mayo de 2024, la SIC contestó la demanda y solicitó negar todas las pretensiones de la misma. Finalmente, el 18 de febrero de 2025 el Tribunal resuelve negar las medidas cautelares solicitadas.

Es necesario anotar que, Google Colombia también instauró una demanda de nulidad respecto a las Resoluciones No. 70315 y la No. 38869. Sin embargo, para el presente escrito sólo se analizará el expediente de la demanda de Google LLC, debido a que este proceso pone de presente la problemática de las ETN.

En el siguiente apartado, se expondrán los principales argumentos de los tres actores, en medio de esta disputa jurídica de acuerdo con lo que es posible evidenciar del expediente judicial y administrativo de libre consulta. Teniendo especial consideración, de las posturas y argumentos de cada parte sobre el ámbito territorial que delimita el artículo 2 de la Ley 1581 de 2012 que cita:

> [...] La presente ley aplicará al Tratamiento de Datos Personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales [...].

Argumentos de la SIC

La SIC expone que el artículo 21 de la Ley 1581 de 2012 le asigna la facultad de realizar investigaciones de oficio para hacer efectivo el derecho de *habeas data* de los Titulares respecto a los Responsables. Además, le permite solicitar información a los distintos sujetos, y, como consecuencia de ello, impartir órdenes para que se adecúen los lineamientos en referencia al TDP en congruencia con la regulación en este ámbito. Paralelamente, el artículo 17 de la misma ley en el literal «o)» en lo referente a los deberes de los Responsables del TDP, a los cuales les aplique la mencionada ley, señala que estos deben «cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio».

Igualmente, en medio de la actuación administrativa la SIC ha entendido que la Ley de Protección de Datos Personales aplica cuando:

> a.) El Tratamiento lo realiza el Responsable o Encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia. b.) El Responsable o el Encargado no está domiciliado en la República de Colombia ni realiza TDP dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana (Resolución No. 2389, 2022, p.8).

Ahora bien, en el caso puntual, la SIC establece que la Ley 1581 de 2012 tiene efectos sobre Google LLC en virtud del primer supuesto, «aplicará al Tratamiento de Datos Personales efectuado en territorio colombiano»[17]. Dado que, la ley establece en su artículo 3 literal «g)» que

[17] Tomado de la Ley 1581 de 2012, artículo 2.

el Tratamiento es «cualquier operación o conjunto de operaciones sobre datos personales, tales como la **recolección**, almacenamiento, uso, circulación o supresión» [énfasis propio].

Así entonces, parte del supuesto en el que, Google LLC utiliza *cookies* para realizar la recolección de datos, entendiendo aquellas como un mecanismo o dispositivo de texto que se instala al momento de aceptarlas en los aparatos electrónicos ubicados en el territorio colombiano. Consecuentemente, concluye que, como se instalan en Colombia, la recolección la realiza allí mismo. Además la SIC, declara que si «la Ley colombiana no distingue la forma ni los mecanismos cómo se realiza el Tratamiento en el territorio colombiano, pues no le corresponde a esta autoridad excluir el uso de *cookie*s como una de tales herramientas» (Resolución No. 60478, 2021, p.32).

Sumado a ello, si bien acepta que Google LLC es una sociedad extranjera que carece de presencia física en Colombia entiende que bajo el primer supuesto es indiferente el domicilio del Responsable que efectúa el TDP dentro del territorio. Por su parte, en lo relativo a la responsabilidad que le atribuye a Google Colombia la misma se deriva de presumir, sin competencia para ello, un grupo empresarial entre Google LLC y Google Colombia. La misma se puede inferir, cuando por ejemplo, se refiere a ambas sociedades como «grupo Google» en las Resoluciones y cuando sostiene que:

> Es inocultable que GOOGLE COLOMBIA LIMITADA, en el territorio de la República de Colombia, **es una extensión directa** de GOOGLE INTERNATIONAL LLC e. indirectamente, de GOOGLE LLC. Lo anterior, sin perjuicio de la verificación de los requisitos establecidos en el artículo 469 y siguientes del Código de Comercio. Entonces se concluye que, GOOGLE COLOMBIA LIMITADA es una **materialización de la voluntad y finalidad económica de las compañías mencionadas** en el territorio de la República de Colombia [énfasis propio] (Resolución No. 70315, 2020, p.6).

Adicionalmente, considera que, en razón del mencionado grupo, Google Colombia promueve e instruye el uso de los datos que trata Google LLC, es decir, que, «por sí misma o en asocio con otros, decide sobre la Base de Datos y/o el Tratamiento de los Datos que se recolectan por medio de aquellos servicios»[18]. Así entonces, concluye que, por ser Google LLC responsable respecto al TDP efectuado por medio de la plataforma de YouTube y este hacer parte de un grupo empresarial junto con Google Colombia, se consideran corresponsables del correcto o incorrecto Tratamiento que se realice.

Argumentos de Google LLC

Google LLC en distintos memoriales, comunicaciones y escritos recalca que, la Ley de Protección de Datos Personales no le es aplicable al TDP que realiza a través de la plataforma YouTube, y por lo tanto, la SIC no tiene jurisdicción en relación a sus actuaciones.

Así entonces, argumenta que es una sociedad extranjera domiciliada en California, Estados Unidos y no tiene presencia legal ni física en Colombia. Además, que las plataformas de los diferentes servicios que ofrece son prestadas desde el extranjero, a las cuales pueden acceder usuarios ubicados en Colombia, mediante el acceso a Internet que es proporcionado por prestadores de redes y servicios de telecomunicaciones nacionales, respecto de los que Google LLC no tiene ningún tipo de participación[19]. Por lo tanto, como el factor de aplicación es el lugar donde se realiza el TDP y no la nacionalidad de los Titulares, no le es exigible regirse por esta ley.

En lo concerniente al segundo supuesto del artículo 2 de la Ley 1581 de 2012, expresa que, no hay ninguna norma de carácter vinculante que le exija adherirse a la legislación colombiana, como sociedad domiciliada y constituida en Estados Unidos de América, contrario a cómo opera

[18] Tomado de la Resolución 38869 de 2021, p. 5.
[19] Tomado de la subsanación de la demanda de Nulidad y Restablecimiento del Derecho presentada en el expediente digital No. 25000234100020220044400, p. 6. Octubre 12 de 2022.

para por ejemplo los Consulados colombianos en el exterior. Ahora bien, en lo relativo al primer supuesto, en el cual según la SIC se encuadra el TDP expone que, los datos son tratados en el exterior, y asimismo la protección de estos está sujeta a la regulación de donde se trata.

Haciendo énfasis en que aunque no le aplique el régimen de protección de datos personales de la ley colombiana, ilustra que, desde el servicio que presta se solicita «el consentimiento previo expreso e informado para el Tratamiento **relevante** de datos personales» [énfasis propio][20], por medio de los Términos y Condiciones y de la Política de Privacidad que provee. De igual manera, informa que datos son objeto de Tratamiento y la manera en la cual serán recolectados, tratados y usados. Además brinda control sobre la configuración de privacidad para activar o desactivar ciertas funciones. Aunado a lo anterior, afirma que cuando el Titular hace uso de sus servicios e ingresa a las plataformas «clara e inequívocamente está ejecutando una conducta positiva que permite razonablemente concluir que ha consentido el procesamiento de sus datos personales (consentimiento expreso por conducta inequívoca)»[21].

Así pues, considera errónea la interpretación que realiza la SIC sobre el artículo 2 de la Ley 1581 de 2012 para investigarla, dado que, por medio de las resoluciones impone los efectos de la misma «respecto de una sociedad extranjera, sin domicilio ni presencia física en Colombia y sobre una actividad (el Tratamiento de Datos Personales)»[22] que se ejecuta en el extranjero.

En este sentido, alega que: (i) las resoluciones desconocen de plano el principio de territorialidad que rige a la ley colombiana, y se contradicen de manera directa con los límites de soberanía que han sido fijados internacionalmente; (ii) la SIC extralimita su jurisdicción

[20] Tomado de Memorial presentado por Google LLC en el expediente digital No. 19-202397, p. 9. Octubre 16 de 2019.
[21] Tomado de Memorial presentado por Google LLC en el expediente digital No. 19-202397, p. 11. Octubre 16 de 2019.
[22] Tomado de la subsanación demanda de Nulidad y Restablecimiento del Derecho presentada en el expediente digital No. 25000234100020220044400, p. 38. Octubre 12 de 2022.

pretendiendo ejercer vigilancia y control sobre compañías extranjeras no establecidas en el territorio nacional; (iii) como consecuencia de todas las actuaciones por parte de la SIC se están generando daños al buen nombre de la sociedad; (iv) se pretende que se incorpore dentro de su política de protección de datos para Colombia enunciados literales y poco comprensibles tomados directamente de la ley, aun cuando se ha demostrado que materialmente la protección de los datos que ofrece esta sociedad es efectiva; y (v) que la carga impuesta de un mecanismo que permita infaliblemente verificar la identificación de la persona que brinda la autorización es desproporcionada.

Argumentos de Google Colombia

Google Colombia siendo una sociedad de responsabilidad limitada legalmente constituida bajo el régimen societario colombiano, comienza por resaltar que por sí misma trata datos personales en Colombia los cuales están debidamente registrados en el Registro Nacional de Bases de Datos y que, respecto a ellos cumple con toda la normatividad dispuesta en esta materia.

Asimismo, afirma no administrar entornos digitales, y correlativamente no ser la propietaria o administradora de las plataformas que son objeto de investigación, en este caso YouTube. En este sentido, como se evidencia en el Certificado de Existencia y Representación Legal (2020) que reposa en la Cámara de Comercio de Bogotá su objeto consiste en:

> Dedicarse por cuenta propia, de terceros o asociada a terceros, en cualquier parte de la República de Colombia o del extranjero a la venta, distribución, comercialización y desarrollo, en forma directa o indirecta, de productos y servicios de hardware y software, productos y servicios relacionados a internet y publicidad en internet o por cualquier otro medio (p.12) [23].

[23] Tomado del recurso de reposición y en subsidio apelación que reposa en el expediente digital No. 19-202397, Noviembre 24 de 2020.

Haciendo referencia a las consideraciones de la SIC, estima desacertada la decisión sobre la calificación de grupo empresarial y la declaración de situación de control que realiza arbitrariamente. Argumenta que la SIC no tiene facultades para realizar estas declaraciones dado que es competencia de la Superintendencia de Sociedades. Arguyendo además que, aun siendo declaradas estas son presunciones desvirtuables.

Consecuentemente, resulta inmotivado el argumento bajo el cual basta la sola declaración del grupo empresarial y/o situación de control para presumir el surgimiento de obligaciones de corresponsabilidad en torno al TDP. Obligaciones que no tienen origen legal, jurisprudencial o en cualquier otra fuente del derecho. En este mismo sentido, sostiene que el hecho de (i) tener relaciones comerciales con Google LLC; (ii) tener autorización para usar la marca; y (iii) que Google LLC sea uno de sus accionistas, no implica la participación de Google Colombia en el TDP que Google LLC realiza en Colombia.

Finalmente, arguye que no determina las finalidades, los medios o las formas en las que se administran los datos tratados por Google LLC, como para poder afirmar que pudiera ser responsable en los términos de la Ley 1581 de 2012.

Problema jurídico

Teniendo claridad sobre los hechos, actuaciones y argumentos presentados en medio de este caso, se evidencia un problema jurídico concreto: el alcance de la protección de datos personales en Colombia en las ETN. De lo anterior se destacan tres elementos esenciales: (i) las ETN; (ii) el principio de territorialidad; y (iii) las regulaciones extranjeras que reglamentan el TDP en otras jurisdicciones. Los cuales se desarrollarán con la intención de ofrecer consideraciones respecto a este problema jurídico.

De este modo, se planteará el contexto general que rodea a las ETN, la normatividad que les aplica en Colombia, la regulación de las mismas en organizaciones internacionales y, como

ellas presentan desafíos a propósito del principio de territorialidad de las normas. Esto con el objetivo de contar con fundamentos para evaluar las actuaciones de Google LLC siendo una ETN que trata los datos de personas domiciliadas en Colombia, a través de los servicios que ofrece por medio de plataformas digitales sin intermediación de su filial Google Colombia.

Seguido a ello, se acudirá a conjuntos normativos en el ámbito internacional con la intención de: (i) identificar otros ordenamientos que regulen en materia de TDP a Google LLC, tales como las normas de Estados Unidos en especial las del estado de California; y (ii) reconocer las obligaciones, prohibiciones y limitaciones que presentan algunos conjuntos normativos que regulan el TDP a nivel internacional.

Estos tres elementos se analizarán teniendo en cuenta que el proceso judicial en curso dentro del Tribunal Administrativo de Cundinamarca pretende declarar si a Google LLC le aplica la Ley 1581 de 2012. Esto lo tendrá que definir el juez estableciendo, bajo criterios técnicos, si las *cookies* constituyen recolección de datos en el territorio colombiano o no. Ante esta disyuntiva si las *cookies* se consideran dentro del proceso, recolección de datos, a Google LLC le aplica la ley. Si bien este sería el resultado anhelado por los usuarios, considerarlo como el único probable, como lo hace López (2025) en la columna de Dejusticia, solo por el afán proteccionista de salvaguardar los datos, es un análisis meramente superficial que ignora las aristas y grises de la situación.

Así entonces, este escrito pretende posicionarse en el escenario contrario, en el que las *cookies* por criterios técnicos -que no serán abordados- no se consideran como recolección en el territorio colombiano y por lo tanto Google LLC no es sujeto de aplicación de la Ley 1581 de 2012 bajo el primer supuesto del artículo 2. Asimismo, no se evidencia una norma internacional que obligue a la empresa a cumplir con la normatividad de TDP colombiana, lo que implica que

tampoco será aplicable el segundo supuesto que trae el artículo. Bajo esta hipótesis se expondrán las consecuencias, implicaciones y posibles soluciones al problema jurídico subyacente.

Capítulo II: Empresas Transnacionales y Territorialidad

Uno de los problemas jurídicos por examinar a la luz del Caso Google vs. la SIC es la regulación y las limitaciones que presentan las ETN en territorios distintos al de su establecimiento. Dado que, como se expuso anteriormente, Google LLC es una ETN con domicilio extranjero que en Colombia a pesar de tener filiales, en el caso de estudio no actúa a través de ellas. Por lo tanto, no hay claridad concertada a si se le aplica la ley nacional del país de origen, la ley nacional del país de donde tienen incidencia, una mezcla entre ambas, ninguna de las anteriores o si se aplican leyes internacionales. A causa de lo que antes se ha dicho, el propósito de este capítulo es establecer qué se entiende por ETN, cuáles son las principales limitaciones que la comunidad internacional le ha otorgado a las mismas y exponer el alcance territorial de ellas. Adicionalmente, cabe resaltar que esta problemática resulta pertinente analizarla pues, el modelo de negocio en el cual se ofrecen productos o servicios por medio de una plataforma digital es uno de los más usados por este tipo de empresas.

Colombia es uno de los países que circunscribe sus normas a factores territoriales, y por el momento no existe legislación alguna que limite o imponga obligaciones en abstracto a las ETN. Sumado a ello, es evidente el inconveniente a nivel procesal de la imputación de responsabilidad bajo una normatividad local a una sociedad no constituida en el territorio. Empero, es posible identificar ciertas normas específicas donde por medio de las filiales se podrían aplicar las regulaciones nacionales a estos entes extranjeros. Sin embargo, la tesis mayoritaria afirma que si las ETN no actúan a través de sus filiales, sino que su injerencia es directa por medios digitales, no les aplica la legislación colombiana, salvo que, en la ley se disponga lo contrario.

Ante el vacío legislativo en Colombia y en otros países es necesario acudir a lineamientos internacionales que planteen principios y/o directrices que puedan servir de guía para complementar la legislación nacional. Tales como las normatividades de la Organización de

Naciones Unidas (en adelante «ONU»), la Organización de Estados Americanos (en adelante «OEA»), la Organización para la Cooperación y el Desarrollo Económico (en adelante «OCDE») y la Organización Internacional del Trabajo (en adelante «OIT»). Estas limitan el actuar de las ETN en una escala internacional y son normas más robustas, técnicas, y generales, las cuales si bien no son necesariamente vinculantes para Colombia presentan un panorama general al cual se debería acudir para regular el actuar de las ETN en Colombia.

Contexto general de las ETN

Las empresas constituyen el núcleo principal del desarrollo privado de la economía. Con el paso del tiempo se han transformado congruentemente con la evolución social, económica, política y cultural del mundo tendiendo progresivamente a la globalización y con ellas las normas que las regulan. Así pues, en un inicio el comercio y las relaciones culturales y políticas solo se daban entre connacionales dada las limitaciones de comunicación e interacción con otros Estados e incluso ciudadanos. Con posterioridad, las comunicaciones entre países se facilitaron y aumentaron, lo cual permitió que las empresas tuvieran presencia física y jurídica en otros Estados diferentes al de origen, por lo tanto, en donde se encontraren constituidas legalmente eran reguladas. Esto bajo un modelo de gestión y organización centralizada, dando lugar a una mayor exportación e importación de productos, proceso intermediado en su mayoría por los Estados, y promoviendo la creación de filiales o sucursales.

Con ulterioridad a la creación del internet se evidencia la globalización como fenómeno latente en la cotidianidad de las personas, las empresas y los Estados. En cuanto a lo que compete a este escrito, dio origen a un nuevo modelo de negocio en el cual se ofrecen los productos y servicios por medios digitales. En este sentido, las empresas usan la tecnología no solo para la mejora e industrialización de su negocio, sino como plataforma e interfaz que les permite

comunicarse y conectarse con los consumidores alrededor del mundo de manera directa, inmediata, y personalizada.

Es así como, surgieron las empresas internacionales también denominadas empresa multinacional, sociedad transnacional, ETN, entre otras. Para el presente trabajo se tomará el término empresa transnacional dado que este «permite entender que se trata de una empresa con única nacionalidad determinada que desarrolla su actividad en distintos países» (Aramburú 1997 citado en Dargent Bocanegra, 2001, p. 45). En este sentido, se entenderá ETN como: empresas de gran tamaño con sede matriz en un territorio específico en donde tienen los órganos de dirección y administración principales y tienen participación económica en distintos territorios. Esta injerencia la realizan por distintos medios: (i) la creación de entes societarios en cada legislación, es decir filiales; (ii) inversión extranjera; y actualmente (iii) por medio de plataformas en línea en donde ofrecen sus productos o servicios directamente de un país a otro.

En primer lugar, las filiales aun estando vinculadas a la empresa matriz se les otorga la connotación de descentralizadas, en el entendido que tienen libertad para actuar, sin embargo, desde la empresa matriz se les dan unas directrices o lineamientos principales que se deben propender por cumplir. Así entonces, Dargent Bocanegra (2001) resalta la relación jerárquica con una cabeza visible que elabora una estrategia común para sus subordinados y hacen uso de recursos comunes (p.46). Por su parte, Moncada (1982, como se cita en Novak Talavera, 1995) añade que existe una centralización de las decisiones importantes y la delegación de las decisiones ordinarias a las filiales (p. 135).

En segundo lugar, la inversión extranjera se regula por medio del régimen cambiario y tributario de cada país y está controlado por las respectivas entidades. Finalmente, respecto al modelo de negocio que se ofrece a través de las plataformas digitales, este tiene como principal

sustento que al ingresar a una página web de una sociedad o persona natural extranjera, se está rigiendo por la normatividad que aquella tenga en su país. En referencia a este último, es donde se presentan la mayor cantidad de vacíos en las disposiciones normativas.

A pesar de la importancia que tienen estos actores en el comercio a nivel nacional e internacional, las regulaciones en lo tocante a su dinámica extraterritorial no son claras en la legislación colombiana, y aunque los organismos internacionales han hecho un esfuerzo por crear principios que regulen el actuar de las ETN, estos no tienen fuerza vinculante.

Normatividad aplicable

Teniendo claro cuál es la definición, las características y el contexto en el cual se van a entender las ETN y de qué manera tienen injerencia en territorios extranjeros, se procederá a analizar las normatividades vigentes que pueden ser aplicadas a estas.

En Colombia

En lo relativo al régimen aplicable en el supuesto en el cual una ETN realiza inversiones directas en Colombia, este corresponde a un análisis en términos cambiarios y tributarios que no son objeto de este estudio. Por su parte, el régimen de las filiales en términos societarios tiene una vasta regulación en la legislación colombiana tales como el Código de Comercio Colombiano expedido en 1971, la Ley 222 de 1995, la Circular Básica Jurídica de la Superintendencia de Sociedades, entre otras.

En este sentido, es necesario tener claridad cuando, en términos societarios, una sociedad se entiende como filial de otra (que puede tener su domicilio en Colombia o en el extranjero). El Código de Comercio en su artículo 260 determina que «una sociedad será subordinada o controlada cuando su poder de decisión se encuentre sometido a la voluntad de otra u otras personas que serán su matriz o controlante, bien sea directamente, caso en el cual aquélla se denominará filial».

Sumado a lo anterior, el artículo 261, modificado por el artículo 27 de la Ley 222 de 1995 establece los supuestos en los que se presume esta subordinación que da lugar a las filiales o sucursales, entre los cuales se encuentra que «más del 50% del capital pertenezca a la matriz, directamente o por intermedio o con el concurso de sus subordinadas, o de las subordinadas de éstas».

Estos escenarios en los cuales se entiende que una sociedad se califica como filial, tienen implicaciones en el régimen societario para esta y para la matriz. Así, la Circular Externa 100-000008[24] (2022) en el Capítulo VII del Título III «De las Obligaciones Derivadas de la Existencia de Control o Grupo Empresarial, en el punto 7.13 expone cuales son las obligaciones del grupo empresarial con matriz extranjera: (i) declarar mediante documento privado la situación de control o grupo empresarial e inscribirlo en la Cámara de Comercio del domicilio de la controlada; (ii) «la elaboración y presentación del informe especial para grupos empresariales»; (iii) «la combinación de los estados financieros en cabeza de la subordinada en Colombia con el mayor patrimonio»; y (iv) la prohibición de imbricación (p.76).

No obstante, estas obligaciones se predican para que sean cumplidas por las subordinadas, así lo hace entender la Superintendencia de Sociedades en la «Guía Práctica Régimen de Matrices y Subordinadas» (2010), por ejemplo, en lo que concierne a la obligación de realizar el informe especial, son «los administradores de cada una de las subordinadas domiciliadas en el país» los cuales tienen la obligación de «presentar el informe especial a la asamblea o junta de socios» (p.16). Lo anterior es coherente, dado que, en el ámbito societario uno de los principales objetivos de las sociedades es la separación patrimonial del accionista respecto del de la sociedad y viceversa.

[24] Por la cual se reestructura y actualiza la Circular Básica Jurídica de la Superintendencia de Sociedades.

Así entonces, bien sea que el accionista sea colombiano o extranjero, persona natural o jurídica, la Superintendencia de Sociedades en el Oficio 220-034451 de 2024 resalta que «lo que hace que una sociedad sea colombiana no es su conformación accionaria sino el domicilio de la misma, es decir, su ubicación dentro del territorio colombiano» (p.2), por lo tanto en el caso de estudio independientemente del domicilio de sus accionistas si la empresa está constituida en Colombia se regirá por las leyes colombianas. De la misma manera, a las sociedades extranjeras solo por el hecho de ser accionistas en una sociedad domiciliada en Colombia no les aplica la legislación colombiana al giro ordinario de sus propios negocios; por consiguiente, dicha sociedad se seguirá rigiendo por la normatividad del país donde está constituida.

Por ende, es dable entender que las obligaciones antes enumeradas y todas las que suscriba por sí misma y voluntariamente la sociedad constituida en Colombia, son independientes a sus accionistas por ser una persona jurídica autónoma. En consonancia con lo anterior, la Superintendencia de Sociedades en el Oficio 125-1063 «Responsabilidad de Matrices o Controlantes» del 13 de enero de 1999, declara que «dentro de los efectos de la subordinación no se ha establecido la solidaridad de la matriz o controlante en el pago de las obligaciones contraídas por sus filiales o subsidiarias, por el solo hecho de la vinculación» (p.1). Empero, en el mismo oficio se enfatiza sobre la responsabilidad subsidiaria que tiene la matriz en los casos en los cuales las sociedades controladas se encuentren inmersas en procesos concursales salvo que se pruebe que los mismos no fueron consecuencia de los actos de dirección de la matriz. Adicionalmente, cabe resaltar que el artículo 207 de la Ley 222 de 1995, establece que de probarse que fue usada la sociedad para generar de mala fe perjuicios a los acreedores, los socios, incluyendo el socio controlante, podrían responder con su patrimonio.

Es necesario señalar que, la situación de control que se presenta en las filiales es una figura jurídica diferente a los grupos empresariales, que según el artículo 28 de la Ley 222 de 1995 ocurren cuando, además de la subordinación existe entre las sociedades unidad de propósito y dirección.

Igualmente, se distingue de las sucursales, las cuales a diferencia de las filiales no tienen personería jurídica, sino que consisten en un establecimiento de comercio de una sociedad. El artículo 471 del Código de Comercio plantea una hipótesis en la cual una sociedad extranjera estaría obligada a abrir una sucursal en el país bajo el supuesto en el que la misma desarrolle actividades permanentes en Colombia, y el artículo 474 ejemplifica lo que podría llegar a considerarse como una actividad permanente:

> 1) Abrir dentro del territorio de la República establecimientos mercantiles u oficinas de negocios aunque éstas solamente tengan un carácter técnico o de asesoría; 2) Intervenir como contratista en la ejecución de obras o en la prestación de servicios; 3) Participar en cualquier forma en actividades que tengan por objeto el manejo, aprovechamiento o inversión de fondos provenientes del ahorro privado; 4) Dedicarse a la industria extractiva en cualquiera de sus ramas o servicios; 5) Obtener del Estado colombiano una concesión o que ésta le hubiere sido cedida a cualquier título, o que en alguna forma participe en la explotación de la misma y, 6) El funcionamiento de sus asambleas de asociados, juntas directivas, gerencia o administración en el territorio nacional (Código de Comercio Colombiano, 1971).

Lo anterior, acarrea múltiples problemáticas de aplicación práctica. Ni la doctrina ni la jurisprudencia se ha decantado por criterios consonantes respecto a qué se puede entender como actividad permanente y en este mismo sentido queda a criterio de la ETN definir subjetivamente

si está ejerciendo este tipo de actividades o no. Adicionalmente, subyace la problemática expuesta en el acápite anterior del límite territorial que tienen los Estados para responsabilizar a las sociedades domiciliadas por fuera de su territorio, incluso cuando por ejemplo con esta norma hay obligaciones claras frente a ellas.

Por su parte, el modelo de negocio actual por medio del cual las ETN ofrecen sus servicios por canales digitales ha suscitado múltiples debates. Dado que, entre otras cosas la ETN le ofrece un servicio directamente a los ciudadanos de otro país y pacta en medio de este negocio entre otras cosas cláusulas según las cuales la jurisdicción aplicable será la del país de origen de dicha sociedad. Suscitando como principal problemática la posibilidad de que se vulneren los derechos de los usuarios pues, sus diferencias se resuelven en un ordenamiento ajeno al de aquellos.

En conclusión, si bien no hay una normatividad general que regule en abstracto el actuar de las ETN en Colombia es posible identificar que normas de distintas temáticas su ámbito de aplicación puede extenderse a las ETN. Por ejemplo, cuando se opta por constituir filiales y es por medio de aquellas que realizan las operaciones económicas en el otro territorio, hay claridad consolidada acerca de las características, limitaciones y regulaciones que les corresponde. Es decir, la normatividad societaria que se le aplicaría a cualquier otra sociedad nacional. Sin embargo, ante el Caso Google vs la SIC se plantea un nuevo interrogante sobre el funcionamiento o regulación de las ETN que teniendo o no filiales en el territorio extranjero, de igual manera tienen incidencia y comercian en el mismo por medios digitales. Esto no solamente es recurrente en Colombia, la injerencia de las ETN es trasversal en la actualidad económica de los Estados.

Ámbito internacional

El TDP entre ETN y Titulares no domiciliados en el país de la empresa es relevante y recurrente en la esfera internacional y resulta indispensable realizar un análisis desde esta perspectiva.

Si bien las ETN no han sido consideradas como sujetos por el Derecho Internacional Público, no se puede obviar la importancia que tienen ellas, y es por ello que la comunidad internacional ha realizado esfuerzos tendientes a fijar unos parámetros comunes que sirvan para la regulación de las mismas. Como lo establece Sepúlveda Amor (1981) «la influencia de las grandes corporaciones internacionales, y su injerencia política en asuntos internos de los estados, trajo como consecuencia el esfuerzo de la comunidad internacional por establecer normas de conductas para esas empresas» (p. 445).

Debido al gran impacto que ha tenido la globalización y la interconexión, las empresas están acudiendo en menor medida a constituir filiales en un país extranjero y optan por que sus operaciones e interacciones con el consumidor sean por medios tecnológicos. Ante este modelo, organismos internacionales como la ONU, la OEA, la OCDE y la OIT emitieron una serie de instrumentos internacionales que toman la forma de directrices para brindar una normatividad general internacional de las ETN.

> Las resoluciones emitidas por estas organizaciones están dirigidas a los Estados como sujetos dentro del Derecho Internacional Público. Estas resoluciones son guías, directrices o recomendaciones para que los mismos ajusten y complementen progresivamente la legislación interna para lograr que las ETN se comporten según una estrategia global. Seguidamente, se analizará dicha normatividad sobre las ETN dentro de los cuatro organismos mencionados con anterioridad de los cuales Colombia hace parte.

En primer lugar, la ONU que fue creada en 1945, actualmente cuenta con 193 Estados Miembro y es considerada como uno de los referentes internacionales más importantes. Como se establece en el artículo 59 de la Carta de las Naciones Unidas «la Organización iniciará, cuando hubiere lugar, negociaciones entre los Estados interesados para crear los nuevos organismos especializados que fueren necesarios (...)» (Organización de Naciones Unidas [ONU], 1945). Así pues, dentro del Consejo Económico y Social de las Naciones Unidas (en adelante «ECOSOC»), se propuso la creación de un grupo intergubernamental el cual tenía el objetivo de estudiar los efectos de las ETN en el ámbito internacional. Dicho grupo en 1974 recomendó la creación de: (i) la Comisión de Empresas Transnacionales con el fin de «actuar como foro de las Naciones Unidas para el examen de las ETN y asistir al ECOSOC en la preparación de posibles acuerdos en la materia» (Berdeja Prieto, 1979, p. 188); y (ii) el Centro de Información e Investigación Sobre Empresas Transnacionales que tiene como objetivo «el desarrollo de un sistema de información, la organización de programas de cooperación técnica con los gobiernos y la realización de investigaciones sobre diversos aspectos políticos, jurídicos, económicos y sociales relacionados con las empresas transnacionales» (Berdeja Prieto, 1979, p. 189).

El 21 de julio de 1988 se aprobó la Resolución E/CN.4/Sub.2/1988/22 «*Guidelines for the Regulation of Computerized Personal Data Files*», aprobada por la Asamblea General por medio de la Resolución A/RES/45/95. Dentro de esta se enlistan principios entre los cuales se encuentran: (i) principio de licitud y lealtad; (ii) principio de finalidad; y (iii) principio de seguridad que incluye la supervisión, sanciones y el flujo de datos a través de las fronteras, entre otros (Consejo Económico y Social [ECOSOC], 1988). Aunque la tecnología y la capacidad de recolección de datos de las ETN ha evolucionado considerablemente, estos principios no pierden vigencia y deben seguir siendo tenidos en cuenta.

En el mismo sentido, el ECOSOC durante el 55° Período de Sesiones aprobó la Resolución E/CN.4/Sub.2/2003/12/REV.2 del 26 de agosto de 2003 «*Norms on the Responsibilities of Transnational Corporations and other Business Enterprises with Regard to Human Rights*» con el objetivo de fijar las obligaciones que tienen las Empresas (incluidas las transnacionales) de garantizar los derechos humanos de las personas que interactúan con ellas. En el preámbulo se expresa que, las empresas tienen una doble perspectiva, por un lado, tienen la capacidad de beneficiar a las personas e impulsar la economía tanto en el Estado donde están domiciliadas como en los Estados donde tienen injerencia. Por otro lado, si no tienen unas regulaciones o límites claramente establecidos pueden llegar a causar perjuicios a la ciudadanía con sus actuaciones. Es por esto que existe la obligación en materia de protección al consumidor donde se establece que:

> Las empresas transnacionales y otras empresas comerciales actuarán en consonancia con las prácticas mercantiles, comerciales y publicitarias leales y adoptarán cuantas medidas sean necesarias para garantizar la seguridad y calidad de los bienes y servicios que proporcionen, incluso observarán el principio de precaución (ECOSOC, 2003, p.5).

Aunque esta obligación no habla específicamente del TDP es dable concluir que, las empresas tienen la obligación de proteger al consumidor entendiendo para efectos de este trabajo el consumidor como el Titular de los datos.

En segundo lugar, la OEA fundada en 1948 la cual está compuesta por 35 Estados Miembro de las Américas, es el «principal foro gubernamental político, jurídico, y social del Hemisferio», y tiene como objetivo, entre otros, robustecer la colaboración de los Estados Miembro (Organización de Estados Americanos [OEA], s.f.). En el ámbito del TDP, esta Organización ha trabajado con el fin de que la región tenga unas directrices generales consolidadas para regular los datos que son transferidos por las ETN entre los Estados. Dado que, entre otras cosas, el nivel

adecuado de protección ha causado debates dentro de los Estados Miembro, puesto que, no ha sido posible concretar con certeza cuando otro país tiene un nivel adecuado de protección.

Desde 1996 la OEA ha trabajado en esta materia, primero, con la Asamblea General mediante Resolución AG/RES. 1395 (XXVI-O-96) la cual solicitó al Comité Jurídico Interamericano (en adelante «CJI») realizar un estudio sobre el acceso a la información y la protección de datos (OEA, 1996). Así, en 2010, se aprobó el texto titulado «Ley Modelo Interamericana sobre Acceso a la Información Pública»[25], que tiene como objetivo proteger derechos individuales y colectivos, así como garantizar estándares de protecciones comunes a la región.

En el mismo sentido, la Asamblea mediante la Resolución AG/RES. 2661 (XLI-O-11) aprobada en el 07 de junio de 2011, le requirió al Departamento de Derecho Internacional del Secretariado de Asuntos Jurídicos (en adelante «SAJ») que realizara un «estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos, inclusive las leyes, reglamentos y autorregulación nacionales, con miras a explorar la posibilidad de un marco regional en esta área». Y tomando en cuenta los documentos que posteriormente serían entregados producto del estudio, la Asamblea le solicitó al CJI presentar una serie de principios generales sobre la privacidad y la protección de los datos en la región (OEA, 2011, p.3).

Consecuentemente, se aprobó la Resolución CP/CAJP-2921/10 rev.1 corr.1 del 17 de octubre de 2011 el documento titulado «Principios y Recomendaciones Preliminares sobre la Protección de Datos (La Protección de Datos Personales)». En el mismo, se reconoce la necesidad de proteger los datos personales en un contexto en el cual el uso de los sistemas electrónicos crece

[25] Resolución AG/RES.2607 (XL-O/10) del 08 de junio de 2010.

exponencialmente «para el procesamiento, recolección, almacenamiento, transferencia y divulgación de información personal», y de la misma manera crece la cantidad de datos procesados. Lo cual deja en evidencia la creciente imposibilidad de determinar a ciencia cierta los datos que se están recolectando y quienes tienen acceso a ellos (OEA, 2011, p.4).

Esta Resolución además de algunos de los principios que se mencionan en las normatividades de protección de datos colombianas trae a colación otros que vale la pena destacar. Por ejemplo, el Principio número 8, «Transferencias Internacionales». El cual afirma que, estas solo se podrán realizar si se cumple con al menos uno de estos tres criterios: (i) si la persona que envía los datos se hace responsable de la protección; (ii) si el país que recibe los datos para el Tratamiento cumple como mínimo con un nivel adecuado de protección que será analizado por factores como: el propósito del TDP; la naturaleza de los datos (públicos o privados); las medidas de seguridad implementadas tanto para la transferencia como la protección, entre otras; y (iii) la existencia de otras razones legítimas (p.17-18). Respecto al nivel adecuado de protección existen excepciones en donde, aunque no lo haya, se permite la transferencia. Tales como: que en un contrato existente se acuerde el cumplimiento así sea en un nivel mínimo de protección; que la transferencia sea necesaria para proteger un interés vital del Titular; que el Responsable se comprometa con la protección de los datos; y cuando el Titular consienta expresa e inequívocamente la transferencia (p.18).

En este mismo sentido, el 27 de marzo de 2015 se aprobó el documento «Privacidad y Protección de Datos Personales» mediante la Resolución CJI/doc. 474/15 rev. 2 con la finalidad de servir de fundamento para que los Estados legislaran acorde a los intereses de privacidad y protección de los datos de los ciudadanos de la región (OEA, 2015).

Por último, en el 98° Período Ordinario de Sesiones del CJI se aprobó la Resolución CJI/doc.638/21 del 08 de abril de 2021 llamada «Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y Protección de Datos Personales, con Anotaciones». Donde se amplió de 11 a 13 principios, y se agregó la Autoridad de Protección de Datos y las Excepciones. Además, se desarrolló el Principio 8[26], el Principio 10[27],, y el Principio 11[28] en donde se hace especial énfasis en que hay un indudable crecimiento en el uso de tecnologías y por ende «el almacenamiento de datos está volviéndose geográficamente indeterminado. (...) y la prevalencia creciente de servicios móviles implican necesariamente el intercambio y el almacenamiento remoto de datos a través de fronteras nacionales» (OEA, 2021, p.25).

De este modo, por medio de los documentos aprobados, se recomienda a los Estados implementar las directrices dentro de sus legislaciones nacionales para así garantizar un nivel adecuado de protección de datos dentro de la región y que se puedan realizar transferencias internacionales de forma segura.

En tercer lugar, la OCDE creada en 1961, la cual tiene como objetivo «elaborar políticas que fomenten la prosperidad y las oportunidades, basadas en la igualdad y el bienestar». Desde esta óptica trabaja la privacidad y la protección de los datos, debido a que, para ésta cuando el Titular de los datos está informado y considera que sus datos están seguros, este se incursionará en mayor medida en el mundo tecnológico, lo que promueve el flujo transfronterizo de datos y dinamiza la economía. (Organización para la Cooperación y el Desarrollo Económico [OCDE], s.f.). Así entonces, el 23 de septiembre de 1980 se aprobaron las «*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*»[29]. Estas fueron importantes en la

[26] Principio Ocho de Acceso, Rectificación, Cancelación, Oposición y Portabilidad.
[27] Principio Diez de Responsabilidad.
[28] Principio Once Flujo Transfronterizo de Datos y Responsabilidad.
[29] Directriz C(80)58/Final de Septiembre 23 de 1980.

época debido a la carencia de regulación internacional dirigida a los Estados sobre el TDP, lo cual obstaculizaba el comercio al no poder asegurar la seguridad en las transferencias internacionales de datos.

Como consecuencia de lo anterior, se establecen una serie de principios comunes a los miembros, tales como: (i) el principio de limitación de recogida y uso; (ii) principio de seguridad; (iii) principio de responsabilidad, entre otros. Adicionalmente, se encuentra un apartado de los Principios Básicos de la Aplicación Internacional, especialmente relevantes para el tema de estudio, donde se establece, entre otros: (i) que el Responsable de los datos seguiría siendo responsable de ellos sin importar si se encuentra en lugares geográficamente diferentes; (ii) que los Estados no deben restringir la transferencia internacional de datos, si el Estado receptor cumple con las directrices o se demuestra que existen mecanismos que aseguren la protección de los datos; y (iii) que de imponer alguna restricción, esta debe ser proporcional a los riesgos que pueda generar la transferencia por ejemplo, si se transfieren datos sensibles (OCDE, 1980).

En el año 2013, se formulan unas enmiendas a las Directrices C(80)58/Final por medio del documento C (2013)79 del 11 de julio de 2013, debido a que se evidenció una creciente utilización de la tecnología y por ende «los datos pueden ser procesados simultáneamente en múltiples locaciones; dispersas para almacenamiento alrededor del mundo (...)» (OCDE, 2013, p.29). Dentro de estas enmiendas se mantienen los mismos principios de la original, pero se agregan deberes adicionales tanto para los Estados como para los Responsables de los datos.

En relación con las ETN, la OCDE en el año 2000 emite la «Decisión sobre las Líneas Directrices para Empresas Multinacionales sobre Conducta Empresarial Responsable»[30] las cuales fueron enmendadas en 2023 por las Líneas Directrices OCDE/LEGAL/0144. Teniendo en cuenta

[30] OCDE/LEGAL/0307 de Junio 27 de 2000.

el objeto de estudio de este trabajo, interesa el 8° capítulo llamado Intereses de los Consumidores. Dentro de este, se establecen regulaciones para las empresas de cómo debería ser su actuar frente a los consumidores específicamente, el párrafo 6 establece que las empresas deben:

> Proteger la privacidad de los consumidores velando por que las prácticas empresariales relativas a la recopilación y uso de datos de los consumidores sean legales, transparentes y justas, permitan la participación y elección de los consumidores y tomen todas las medidas razonables para garantizar la seguridad de los datos personales que recopilan, almacenan, procesan o difunden (p.47).

Por último, la OIT creada en 1919 es una organización establecida con el fin de fomentar «la cooperación entre gobiernos y organizaciones de trabajadores y empleadores en la promoción del progreso social y económico» (Organización Internacional del Trabajo [OIT], s.f.). En el año 1977, fue aprobada por esta la «Declaración Tripartita de Principios sobre las Empresas Multinacionales y la Política Social», la cual es un instrumento internacional de incorporación voluntaria. A lo largo del tiempo ha sido sujeta a diversas enmiendas y se han tomado en consideración Directrices de otras organizaciones. En la versión enmendada de esta Declaración (2022) se establece que tiene como objetivo principal:

> Fomentar la contribución positiva que las empresas multinacionales pueden aportar al progreso económico y social y a la consecución del trabajo decente para todos, así como minimizar y resolver las dificultades a que pueden dar lugar las operaciones de estas empresas (OIT, 2022, p.7).

Aragón y Rocha (2004, como se cita en Hernández Zubizarreta, 2009, p. 386) cuestionan este instrumento pues, no hace referencia a la relación entre las ETN con sus filiales, proveedores o contratistas. En el sentido de no estar claro quién tendría la responsabilidad ante un eventual

conflicto, como lo es el TDP por fuera de la jurisdicción de un Estado sin la debida regulación. Si bien, esta declaración no habla expresamente del TDP que realizan las ETN, al interpretar integralmente las políticas generales de las ETN dentro de este organismo, se puede concluir que estas deben «tener en cuenta los objetivos de la política general establecida en los países en que realicen sus operaciones» y «sus actividades deberían ser acordes a la legislación nacional» (OIT, 2022, p.10).

En síntesis, se concluye que, a pesar de la innegable importancia de las ETN en la sociedad actual, el nuevo modelo de negocio digital por medio del cual están operando aquellas a nivel nacional e internacional, ha presentado retos evidentes en las normatividades. El principal desafío se concreta ante el principio de territorialidad de las normas y la soberanía de los Estados.

Territorialidad

Las empresas son un factor determinante en la sociedad y las mismas por su poder económico e influencia social confrontan al Estado y sus organismos. Esto se constata en la difícil implementación de los distintos factores de aplicación de las normas entre los cuales se encuentra el factor territorial, el subjetivo, el temporal, el material, el funcional, entre otros. En este sentido se esbozará cómo se entiende a nivel teórico el principio de territorialidad y los dilemas que la misma presenta en la era digital.

Todos estos factores son determinantes para identificar los sujetos objeto de responsabilidad que pretenden regular las normas. Con ocasión del presente escrito, el análisis no se centrará en cómo afecta el factor territorial en la aplicación a personas naturales sino a personas jurídicas como lo son las ETN. Es claro que, las sociedades constituidas dentro de un ordenamiento específico se rigen bajo las normas societarias del mismo. Empero, sin dejar de un lado que la atribución de la responsabilidad a las personas jurídicas por sí misma ha presentado un sin número

de desafíos por ser una ficción jurídica con una estructura organizacional compleja. Actualmente las ETN han puesto a prueba la capacidad sancionatoria y regulatoria del Estado por la problemática de la aplicación del factor territorial de las leyes. Este delimita la frontera material en donde es aplicable la normatividad, y coherentemente hace referencia a la restricción que tiene el poder regulatorio del Estado, es decir, la soberanía inherente al mismo.

La territorialidad es un factor transversal a todas las normas jurídicas, es decir, fija una limitación en términos civiles, penales, constitucionales, tributarios, entre otros. En esta línea según la Corte Constitucional:

> (…) el principio de territorialidad se ha entendido tradicionalmente como la posibilidad de que un Estado aplique las normas de su ordenamiento dentro del territorio bajo su dominio, sin interferencia alguna de otros Estados [...] se trata de un criterio relativo al ámbito espacial de aplicación de la ley, diferente a otros criterios como el estatuto personal o el real (T-612, 2003, p.11).

En la legislación colombiana este principio se consagra en el artículo 18 del Código Civil Colombiano (CCC) donde se establece que «la ley es obligatoria tanto a los nacionales como a los extranjeros residentes en Colombia» lo cual de acuerdo con la Sentencia 00208 de 2016 del Consejo de Estado, instituye a la territorialidad en términos subjetivos en cuanto a la posibilidad que tiene el Estado de asumir jurisdicción respecto de los actos que inician en el territorio y finalizan en otro Estado. Contrario *sensu*, la Sentencia afirma que en el artículo 19 y siguientes del Código Civil, se enumeran las excepciones a este principio, llamadas supuestos de territorialidad objetiva o extraterritorialidad de la jurisdicción, según las cuales el Estado tiene facultad en términos civiles en lo relativo a:

> (i) al estado de las personas y su capacidad para efectuar actos que hayan de tener efecto en Colombia (artículo 19 C.C.). (ii) En ciertas obligaciones y derechos que nacen de las relaciones de familia (artículo 19 C.C.). (iii) En relación con los actos que recaigan sobre bienes ubicados en el territorio nacional o en los cuales tenga interés la Nación (artículo 20 C.C.). (iv) En cuanto a la forma de los instrumentos públicos, la cual se determina por la ley del país en que hayan sido otorgados, aun cuando su autenticidad se rige por la ley colombiana si el acto produce efectos en el territorio nacional (artículo 21 C.C) (p.2).

Ahora bien, como ya se mencionó cada norma establece en su articulado los criterios según los cuales las personas, naturales o jurídicas se deben someter o no al determinado régimen. Por ejemplo, en materia de TDP, la Ley 1581 de 2012, define su alcance subjetivo y territorial a los «datos personales registrados en cualquier base de datos que los haga susceptibles de Tratamiento por entidades de naturaleza pública y privada» bien que su Tratamiento sea «efectuado en territorio colombiano o cuando al responsable del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales»[31].

Sin embargo, condicionarlo de tal manera tiene un problema evidente y es que, por la época en la que fue creada, está limitada a fronteras físicas y espaciales. En el pasado resultaba impensable la omnipresencia que permite la era digital, en la cual actos como la celebración de contratos y reuniones se realizan a través de medios virtuales. Por esta razón, surgen inquietudes y nuevos espacios por regular, por ejemplo, en aquellos casos en los que las partes involucradas en una relación contractual o en la prestación de un servicio se encuentran en lugares distintos, o si se quiere, comparten un espacio virtual. Esto genera problemas jurisdiccionales, dada la dificultad de definir la ubicación geográfica de las actividades que se desarrollan en el

[31] Tomado de la Ley 1581 de 2012, artículos 2 y 3.

«ciberespacio», debido a su carácter descentralizado y transfronterizo. Lo anterior, deja inoperante e insuficiente la regulación meramente nacional, que se limita en términos territoriales, y como consecuencia, es indiscutible la necesidad de realizar un esfuerzo comunitario a nivel internacional por la regulación transfronteriza de protección de los datos personales de los individuos.

En este sentido, Novak Talavera (1995) argumenta que, las ETN debido a su modelo de negocio pueden llegar a tener tal supremacía que cuestione la soberanía y la seguridad de los Estados donde éstas operan (p. 139).

Capítulo III: Contexto Internacional

El presente capítulo tiene como objetivo vislumbrar un panorama general del estado actual de la protección de datos personales en otras jurisdicciones. Para identificar en qué aspectos el ordenamiento jurídico colombiano tiene oportunidad de mejora con ocasión de las recientes problemáticas en términos de ETN.

Es necesario aclarar que, no se realizará el análisis ya efectuado por la SIC tendiente a establecer que Estados cuentan con un nivel adecuado de protección, los cuales para el año 2019 según la «Guía para la Implementación de Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales» son: (i) Alemania; (ii) Estados Unidos de América; (iii) Perú; (iv) Costa Rica; (v) España; (vi) México; (vii) Portugal; (viii) Reino Unido, entre otros (Superintendencia de Industria y Comercio [SIC], 2019).

Regulaciones Extranjeras

A continuación, se enuncian las regulaciones de la Unión Europea, los Estados Unidos de América, y la Red Iberoamericana, en las cuales se destacarán las principales obligaciones, principios y limitaciones que presentan.

Unión Europea – UE

La Unión Europea (en adelante «UE» o «Unión») cuenta actualmente con 27 Estados Miembro. La Unión por medio de todas sus entidades principales ha procurado la seguridad de sus ciudadanos por medio de la protección de sus datos personales. El Tratado de Funcionamiento de la Unión Europea establece en su artículo 16 el derecho que tiene cada persona a la protección de los datos personales asimismo establece que, el Parlamento Europeo y el Consejo deben emitir normas sobre la protección de las personas en el TDP realizado por instituciones, organismos o Estados de la Unión (Parlamento Europeo, 2012, p. 9). De igual modo, el Parlamento Europeo en

la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8° dispone que «los datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley», así como, «toda persona tiene derecho a acceder a los datos recogidos que la concierne y a su rectificación» (Parlamento Europeo, 2000, p. 10).

El modelo europeo de regulación de TDP es considerado un modelo universal debido a que el mismo ha sido aplicado en otros ordenamientos para regular la materia. Según Ximena Puente (2011, como se cita en Rueda Gómez, 2012) es una de las pocas regulaciones que legisla en torno a todos los tipos de datos que pueden ser objeto de tratamiento por parte de terceros, no de manera sectorial como lo hacen otras regulaciones, asegurando así las garantías de los Titulares (p.16). Así mismo, el modelo europeo desarrolla ampliamente las transferencias internacionales de datos, siendo enfáticos en que el país al que se le vaya a hacer dicha transferencia debe tener un nivel adecuado de protección, de lo contrario prohíbe dicha práctica.

La creación de la Comisión Consultiva para estudiar las tecnologías de la información y la Resolución 509 de 1968 dieron impulso a que los Estados miembro de la UE comenzaran a redactar leyes relativas a la protección de datos.

Convenio 108 de 1981 y Convenio 108 + de 2018. El «Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal» (en adelante «Convenio 108») y «*Modernised Convention for the Protection of Individuals with Regards to the Processing of Personal Data*» (en adelante «Convenio 108 +») emitidas por el Consejo de Europa tienen por objeto principal la protección de los individuos en el TDP, independientemente de su nacionalidad o residencia, amparando derechos fundamentales tales como la privacidad y la libertad. Sin embargo, es importante

resaltar que, por medio del Convenio 108 + , manteniendo la esencia del Convenio 108, se propusieron cambios con la intención de actualizar la normatividad para que corresponda al contexto tecnológico actual que se dirige a un tratamiento automatizado y digital de los datos personales.

En este sentido, los Convenios proponen una serie de principios y regulaciones básicas sobre las cuales incitan a los Estados Miembro a construir su propia legislación. Entre los que se destacan: (i) velar por la calidad de los datos en su registro, obtención, conservación y tratamiento; (ii) tomar las medidas de seguridad apropiadas para la protección de los mismos; (iii) orientarse hacia la transparencia en sus operaciones; (iv) rendir cuentas; y (v) minimizar los datos que son tratados. Sumado a ello, declaran que los Titulares tienen una serie de garantías complementarias que les permite «conocer la existencia de un fichero automatizado de datos de carácter personal» (Consejo de Europa, 1981, p. 4); rectificarlos datos tratados; y disponer de medidas para hacer efectivo sus derechos.

Adicionalmente, exhortan a los Estados Miembro a conceder asistencia para el cumplimiento del Convenio por medio de autoridades designadas para ello. En este sentido, hace especial énfasis en la asistencia que se le debe brindar a los Titulares que tengan residencia en el extranjero para el ejercicio de los derechos previstos en su derecho interno (Consejo de Europa, 1981, p.6).

Finalmente, en el artículo 24 del Convenio 108, se establece el alcance territorial de las normas declarando que, «**cualquier Estado podrá designar**, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, **el territorio o los territorios a los cuales se aplicará el presente Convenio**» [énfasis

propio] (p.9) esta designación podrá ser objeto de ampliación o retracto según se considere conveniente.

Ahora bien, estas normas son directrices, es decir, presentan una serie de recomendaciones y principios orientadores que deben ser aplicados por sus Estados Miembro. Sin embargo, no establecen obligaciones tajantes o consecuencias jurídicas precisas ante la inobservancia de los mismos.

Reglamento General de Protección de Datos - RGPD. Con ocasión al Convenio 108 fueron emitidas por parte del Parlamento Europeo múltiples Directivas que pretendieron llenar los vacíos fácticos y normativos que presentaba el Convenio, las mismas se consolidaron en el 2016 en el Reglamento General de Protección de Datos (en adelante «RGPD»), que presenta una serie de obligaciones claras y exigibles para propender por la unidad legislativa.

En el RGPD se resalta que, la protección otorgada debe «aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales» (Parlamento Europeo, 2016, p. 3). Adicionalmente, en el artículo 3 se establece el ámbito de aplicación territorial material de la norma el cual los circunscribe a tres factores fundamentales: (i) cuando el Responsable tiene domicilio en la UE independientemente que el tratamiento se realice en otro lugar; (ii) cuando el Responsable no tenga el domicilio en la Unión pero su actividad recaiga en oferta de bienes o servicios de interés en la UE; (iii) cuando el Responsable esté en uno de los Estados Miembro cuya aplicación se pueda extender en virtud del derecho internacional público (Parlamento Europeo, 2016, p.32-33).

Acoge los principios mencionados en los Convenios 108 y 108+, y adiciona entre otros el principio de exactitud, y el de limitación del plazo de conservación y de finalidad. Por su parte el Capítulo IV sección 1, incorpora obligaciones tales como: (i) la solicitud del consentimiento y sus condiciones; (ii) la aplicación de medidas técnicas y organizativas para garantizar y demostrar el correcto TDP; (iii) la adhesión de códigos de conducta; (iv) la designación de un representante en la UE cuando el RGPD se aplica al TDP de personas que residan en la Unión por un responsable no establecido en la misma pero que sus actividades estén relacionadas con la oferta de bienes y servicios de interés en ella o el control de su comportamiento tenga lugar en ella, salvo que no se realice a gran escala o se realice por parte de autoridades u organismos públicos; (v) la notificación ante posibles violaciones de seguridad; entre otras (p.47-51). Por otra parte, el RGPD presenta una serie de derechos para los Titulares que son la materialización concreta de los principios.

Cabe aclarar que el RGPD pretende tener un carácter complementario a las demás directrices, convenios y normatividades en la materia y promueve la creación de mecanismos de cooperación internacional para prestar asistencia mutua y promover el robustecimiento legislativo entre países.

Estados Unidos de América

Otro de los sistemas normativos más relevantes, es el de Estados Unidos como domicilio principal de una gran cantidad de las empresas que tienen injerencia en niveles trasnacionales, tales como Google LLC. Es importante resaltar que Estados Unidos es una República Federal, en la cual desde el Gobierno central se emiten normativas generales que priman y le son aplicables a todos los estados. A su vez, cada Estado tiene la facultad de emitir sus propias regulaciones con alcance territorial limitado a su frontera.

Ahora bien, en materia de protección de datos personales tanto las normatividades estatales como las federales, por medio de normas sectoriales de acuerdo al tipo de dato se describen las condiciones en las cuales se da el TDP. Adicionalmente, enfatizan en las garantías a la libre circulación de los datos.

Freedom of Information Act (FOIA) y Privacy Act. Estas dos normatividades constituyen factores claves en términos de regulación federal. El «*The Freedom of Information Act*» es una de las primeras normatividades que propenden por la protección de los datos, la misma concede a las personas el derecho a conocer la información contenida en bases de datos federales (Congreso de los Estados Unidos de América, 1966), lo anterior sin perjuicio de tener o no la calidad de estadounidense.

Por su parte, el «*The Privacy Act*» complementa la normatividad anterior, imponiendo restricciones a las entidades federales en términos de recolección y conservación de los datos. Innovando, por ejemplo, en términos de: (i) limitaciones en razón del consentimiento brindado por el Titular; (ii) imposición y estandarización de códigos de conducta o de buenas prácticas respecto a los registros de datos manejados; y (iii) restricciones estrictas en términos de seguridad de los datos. Aunado a lo anterior, detalla las obligaciones que recaen en cabeza de los entes públicos a nivel federal: (i) la notificación sobre la recolección de los datos que se efectúa sobre los Titulares; (ii) mantener la información precisa, importante y actualizada de los registros que contienen los datos; y (iii) ante la solicitud de un Titular se les obliga a dar acceso y permiso a la corrección de los registros; entre otros (Congreso de los Estados Unidos de América, 1974, p.155-182).

Finalmente, en lo relativo a la aplicación subjetiva, según el artículo 5 U.S.C. § 552a(a)(2) los Titulares objeto de protección son ciudadanos y residentes permanentes legales de Estados Unidos (Congreso de los Estados Unidos de América, 1974, p. 22).

California Consumer Privacy Act - CCPA. El «*California Consumer Privacy Act*» (en adelante «CCPA») expedido por el Senado Estatal del Estado de California, es congruente con el objetivo de la normatividad federal en cuanto a la amplia flexibilidad en la venta y la transferencia de los datos. El mismo solo le es aplicable a los residentes del estado de California y tiene como objetivo proteger los siguientes derechos de los consumidores que correlativamente serían los Titulares: (i) conocer y acceder a la información personal que está siendo recolectada sobre ellos mismos y si la misma está siendo vendida o divulgada y a quién; (ii) decidir si autorizan la venta o divulgación de sus datos; entre otros (Senado Estatal del Estado de California, 2018).

Adicionalmente, los sujetos que tiene esta ley en mente para el cumplimiento de las normas son los entes privados que tratan los datos en California, siempre y cuando desarrollen su actividad en el mismo estado y cumplan con los topes financieros que exige el artículo 1798.140(c)(1) (2018). Sus obligaciones principales son: (i) condicionar la recopilación de la información de los Titulares a una notificación previa y expresa donde se presente específicamente qué datos son objeto de recolección y su finalidad; (ii) fortalecer los sistemas de seguridad para proteger la información recolectada; (iii) instaurar herramientas y mecanismos accesibles a los Titulares para que estos ejerzan sus derechos; entre otros (Senado Estatal del Estado de California, 2018).

Tal y como se describió en la presente sección, por ejemplo, en el caso de estudio, si bien Google LLC es una empresa constituida en el estado de California, cumple con los

requisitos financieros exigidos por el CCPA, y aunque tratara los datos de los colombianos en ese estado (de esto no se tiene certeza) la normatividad no le es aplicable en el caso concreto pues los datos que trata no son de las personas con domicilio en California.

Red Iberoamericana de Protección de Datos- RIPD

Ante la continua y abundante transferencia de datos por medios digitales es cada vez más relevante la protección de los mismos por el uso de estos nuevos canales. En este sentido, la Red Iberoamericana de Protección de Datos (en adelante «RIPD») como foro integrador del sector público y privado y mediante diálogos, iniciativas y políticas comunes se pretende estandarizar las regulaciones de la protección de datos personales en los países iberoamericanos por medio de la autoridad competente en cada país (Red Iberoamericana de Protección de Datos [RIPD], s.f.). Teniendo como fuente principal las regulaciones Europeas antes mencionadas.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos. El objetivo principal de estos estándares es fijar una serie de principios y derechos básicos que los Estados Iberoamericanos puedan acoplar a su legislación interna y consecuentemente, favorecer el flujo de datos personales entre los mismos (RIPD, 2017, p.4).

Estos estándares delimitan con claridad los ámbitos de aplicación. Sobre el de aplicación territorial se señala que estarán sujetos los Responsables que: (i) estén domiciliados en uno de los Estados Iberoamericanos; (ii) no estén domiciliados en uno de los Estados, pero, la oferta de sus bienes o servicios se dirija a los residentes de los Estados Iberoamericanos; (iii) no estén domiciliados en uno de los Estados, pero, les sea aplicable la legislación nacional de dicho Estado o, por medios digitales se sitúe en el territorio para tratar datos personales (RIPD, 2017, p.15).

En el Capítulo II se declara que «en el Tratamiento de Datos Personales, el Responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad» (2017, p. 17), las definiciones de dichos principios son congruentes con las de la Ley 1581 de 2012. En cuanto a los derechos de los Titulares, estos se concentran en el «acceso, rectificación, cancelación, oposición y portabilidad de los datos» (2017, p.24).

En estos también se aplica lo relativo al nivel adecuado de protección, y se motiva a la implementación de mecanismos dentro de la legislación interna que promuevan el cumplimiento de los principios aplicados al contexto del país miembro. Adicionalmente, es importante resaltar el Capítulo IX, el cual trata el derecho de indemnización de los Titulares. Este materializa un hecho generador de responsabilidad civil ante la causación de daños por la violación al derecho de protección de datos personales (2017, p.33). Derecho que no se encuentra en ninguna de las regulaciones estudiadas.

Así entonces, es dable concluir que las regulaciones internacionales han tenido como finalidad principal la estandarización de las normatividades en términos de TDP. Previendo la realidad incuestionable según la cual la transferencia internacional de datos se produce cada vez en mayor escala y con mayor frecuencia, ante el nuevo modelo de negocio de las grandes empresas.

Sección III: Consideraciones Finales

Para concluir se plantean una serie de consideraciones e interrogantes que surgen de los temas anteriormente expuestos, desde la hipótesis sobre la cual la Ley de Protección de Datos Personales a Google LLC como ETN domiciliada en California, Estados Unidos, no le es aplicable. Por no realizar TDP en el territorio colombiano ni existir normatividad vigente que la vincule a la legislación colombiana, tal y como se desarrolló en la Sección II, Capítulo I, Subtítulo Problema Jurídico.

Bajo este enfoque y conforme al análisis normativo de las leyes de protección de datos de Estados Unidos haciendo especial énfasis en la regulación del estado de California, es pertinente inferir que, el TDP que está realizando Google LLC respecto de los datos de las personas domiciliadas en el territorio colombiano no está amparado por esta normatividad, dado que, el CCPA solo protege a las personas residentes de dicho estado.

De lo anterior, se desprende la inquietante conclusión desde un enfoque descriptivo y no prescriptivo que, el TDP que hace Google LLC, sobre los datos de las personas domiciliadas en Colombia, no se encuentra tutelado por ninguna jurisdicción. Esta conclusión se fortalece al evidenciar afirmaciones como las que realizó la SIC en el Concepto 14-2183 frente a los servicios digitales sin domicilio en Colombia:

> En consecuencia, el tratamiento de los datos personales registrados en las redes sociales no encaja dentro del ámbito de competencia de la Ley 1581 de 2012, pues la recolección, el uso, la circulación, el almacenamiento o supresión de los datos personales no se realiza dentro del territorio Colombiano, puesto que las redes sociales no tienen domicilio en Colombia (SIC, 2014, p.4) [énfasis propio].

Ahora bien, tal y como se esbozó con anterioridad la conclusión respecto del caso analizado si bien es preocupante y relevante no se extiende necesariamente a todas las ETN que ofrezcan sus bienes o servicios por medio de plataformas digitales.

Sin embargo, se resalta que las mismas representan un reto para el ámbito de aplicación de la Ley 1581 de 2012 pues a pesar de que traten datos registrados en las bases de datos susceptibles de tratamiento según el artículo 2, por factores técnicos puede que no se considere que las operaciones, que se concluyen que sean tratamiento, estén realizadas **en Colombia.** Asimismo, de acuerdo con la revisión normativa expuesta no existen en la actualidad tratados o convenios internacionales que vinculen en abstracto a las ETN con la regulación colombiana ni en términos de TDP.

Lo anterior, no es un problema inocuo y meramente teórico, la realidad latente es que los datos de los colombianos están siendo tratados y bajo algunos supuestos no están siendo protegidos por vacíos normativos de la ley en contextos contemporáneos ante el limitado ámbito de aplicación de la misma.

Estas insuficiencias requieren actualizaciones, en especial en el ámbito de aplicación tanto territorial como subjetivo de la norma. Así entonces a continuación, se enuncian oportunidades de mejora que tiene la Ley 1581 de 2012 en contraste con las normas internacionales enunciadas en la sección anterior. En primer lugar, de la UE como una de las normatividades más longevas, proteccionistas y completas, es posible rescatar el criterio según el cual la ley le aplica a aquel Responsable cuya oferta de bienes y servicios sean de interés para el país, aun cuando no esté domiciliado en este. También se puede recurrir a los estándares que instaura la RIPD por ser ésta la organización más cercana en términos de vinculación a la legislación colombiana, debido a que, la misma SIC como autoridad competente en materia de protección de datos personales en

Colombia hace parte de la organización. Así, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, bajo la óptica de la aplicación territorial establecen que, la ley se aplicará a aquel Responsable que aunque no esté domiciliado en el país por medios digitales se sitúe en el territorio.

En el mismo sentido, también es rescatable el criterio de aplicación subjetivo que trae el CCPA, sujetando la aplicación a los Responsables que traten los datos de las personas que se encuentren domiciliadas en el país de la regulación. Consecuentemente, si una ETN quiere tratar los datos de las personas domiciliadas en Colombia, entonces se debería de regir por las normatividades de Colombia independientemente de donde efectúe el tratamiento.

Por las razones anteriormente expuestas, una vez actualizado el criterio subjetivo y territorial de la ley de protección de datos personales, habrá un consenso respecto a la aplicación de las normatividades nacionales en las ETN y volverá inoficioso el análisis de corresponsabilidad respecto de las matrices, filiales, o grupos empresariales extranjeros.

Es importante también destacar la obligación que trae el CCPA que se puede extrapolar para robustecer la nacional, la cual consagra que los Responsables del Tratamiento deben de comunicar si los datos, aparte de ser transferidos[32] y/o transmitidos[33] están siendo vendidos. Con la intención de acoplarse al contexto actual en el cual los datos son bienes sujetos de transacciones económicas. Por otro lado, es rescatable el supuesto de responsabilidad civil que instituye los Estándares de la RIPD cuyo hecho generador es la vulneración a la protección de datos personales. Esto en consonancia con el principio de indemnización planteado por la Corte Constitucional en

[32] Transferencia: es la acción por medio de la cual los datos del Titular son enviados por parte de un Responsable y/o Encargado del TDP establecido en territorio colombiano a otro, llamado receptor, que puede estar dentro o fuera del territorio (Decreto 1074 de 2015, 2.2.2.25.1.3 numeral 4).

[33] Transmisión: implica la *transferencia* de datos a un Encargado de TDP, por cuenta del Responsable del cuando tenga por objeto realizar el Tratamiento los mismos (Decreto 1074 de 2015, 2.2.2.25.1.3 numeral 5).

la Sentencia C-748 de 2011. Pudiendo dar pie incluso a plantear la posibilidad de un régimen de responsabilidad objetiva en el cual el Responsable asuma los riesgos de la actividad que está ejerciendo, como garante de los derechos inherentes a los datos personales de los Titulares.

Todo lo anterior permite concluir que carece de sentido el esfuerzo de la SIC por acoplar la normatividad a las dinámicas contemporáneas exhibidas en el caso. El problema no es la capacidad operativa ni sancionatoria de la entidad como mal lo entiende López (2025) en su columna en Dejusticia, sino el alcance que tiene la ley respecto de las ETN en los casos en los cuales por términos técnicos no se entiende que realizan el tratamiento **en** el territorio. De esta manera, Google no puede ser responsable de incumplir una ley que no le aplica.

No hay que olvidar que la razón de la desactualización normativa es el hecho innegable y recurrente de que la evolución tecnológica en términos de economía digital, inteligencia artificial, digitalización de los procesos, entre otros incide en la forma en la que se recolectan, almacenan, transfieren, transmiten y usan los datos personales. Congruentemente, la sociedad evoluciona con más rapidez que las legislaciones. Sin embargo, cuando se sujeta la aplicación de las normas nacionales a sus mismos ciudadanos, los cuales son finalmente los sujetos de protección, esta desactualización no es tan apresurada, pues a pesar de las evoluciones tecnológicas los sujetos siguen siendo los mismos.

Por ser esta una problemática que traspasa fronteras pone de manifiesto la necesidad urgente de la cooperación interestatal. Sin embargo, este no es un trabajo sencillo dadas las dimensiones de la situación que cuestionan la capacidad individual de los Estados de monitorear, regular y someter el TDP. Son millones de Titulares que simultáneamente están celebrando contratos con ETN de los cuales el Estado no tiene control, así mismo, por la accesibilidad que permite el internet, hay cada vez más posibles Responsables del TDP que ofrecen sus servicios y

bienes por las plataformas digitales, sin acudir a filiales u otras figuras jurídicas de los ordenamientos nacionales.

Una solución viable ante lo que exige la nueva realidad son acuerdos, tratados, y convenios internacionales que estandaricen las regulaciones, y permitan una judicialización de los entes transnacionales que participan en el TDP. Lo anterior considerando que, el TDP no es sólo común, sino necesario e importante para el ofrecimiento de servicios a nivel global, los cuales en conjunto hacen crecer y dinamizar la economía. Así, el uso de estas tecnologías es cada vez más necesario para actividades cotidianas volviéndose una extensión misma de la vida, dejando en evidencia, la inviabilidad de exigirle a los Titulares el no uso de estas.

Se quiere resaltar la pertinencia de evaluar que el origen del TDP en estos servicios digitales ofrecidos por las ETN constituyen contratos de servicio como cualquier otro. En el cual, Google LLC como empresa oferente que ejerce una actividad lucrativa pone a disposición del mercado sus servicios gratuitos y las condiciones en las cuales los consumidores pueden usar el servicio y se van a tratar sus datos. En este escenario, se acoge la posición que establece que cuando «el producto es gratis el precio eres tú», pues en el mercado actual los datos son bienes transables que se ofrecen a cambio de poder utilizar el servicio, en razón de que estos pueden ser vendidos a terceros con fines de marketing y publicidad. Otra característica de esta relación contractual es que funciona como un contrato de adhesión donde la autorización se asimila a la aceptación de la oferta planteada. Respecto a esta autorización surgen problemáticas en ambos extremos de la relación contractual.

Frente a los Titulares se presenta el desconocimiento del verdadero uso y tratamiento de sus datos por factores como la longitud y tecnicidad en las que se presentan estas autorizaciones, el desinterés hacia la divulgación de sus datos personales, y la inevitable obligatoriedad de la

aceptación para el uso de los servicios. Circunstancia que los induce en un error, siendo este la disparidad entre la realidad y lo que se pretende representar. En relación con los Responsables se les impone una exigencia desbordada que consiste en asegurar que el Titular conozca de manera íntegra y consciente el TDP. Obligación que a pesar de la máxima diligencia y cuidado desplegada por las empresas, no es posible cumplir a cabalidad pues no pueden asegurar que la información contenida dentro de la autorización sea leída por el Titular y éste comprenda las implicaciones, métodos, derechos, obligaciones y mecanismos dentro del Tratamiento de sus datos. Todo lo anterior, resulta en que las empresas por cumplir obligaciones formales proporcionen autorizaciones complejas y desgastantes que los Titulares aceptan en abstracto.

De igual manera, subyace la problemática respecto a las ETN en cuanto a que se pretende que cumplan simultáneamente múltiples normativas a nivel global, que pueden ser incluso contradictorias entre ellas, sólo por el hecho de ofrecer sus servicios por medios digitales. Aun cuando no se tiene relación directa con aquellos Estados que pretenden regularlos.

Es indiscutible la relevancia de la protección de datos personales a nivel nacional e internacional, sin embargo, la misma plantea exigencias en la era digital por un entorno cada vez más globalizado. En el contexto colombiano el marco normativo vigente no proporciona protección suficiente, efectiva, ni completa a los datos personales de los individuos domiciliados en el territorio colombiano, comprometiendo la seguridad de aquellos. Es imperativa, la adopción de medidas legislativas a nivel interno y en conjunto con otros Estados que fortalezcan la protección del TDP como concepto transversal a las dinámicas comerciales contemporáneas.

Referencias

Berdeja Prieto, T. G. (1979). *Código de Conducta para Empresas Transnacionales: los esfuerzos de la Comisión designada por Naciones Unidas.* Revista Jurídica de la Universidad Nacional Autónoma de México - UNAM, 11, 185-208, http://historico.juridicas.unam.mx/publica/librev/rev/jurid/cont/11/pr/pr7.pdf

Código Civil Colombiano [C.C.C.]. Ley 74 de 1873. Art. 18. Mayo 31 de 1873. (Colombia). D.O. N2867.

Código de Comercio [C.Co.]. Decreto 410 de 1971. Arts. 260, 261, 471,474. Junio 16 de 1971. (Colombia). D.O. N33339.

Congreso de los Estados Unidos de América. (1966). *The Freedom of Information Act* 5 U.S.C. § 552. Julio 05 de 1967. https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf

Congreso de los Estados Unidos de América. (1974). *The Privacy Act* 5 U.S.C. § 552a. Septiembre 27 de 1975. https://www.justice.gov/Overview_2020/dl?inline

Consejo de Estado, Sala de Consulta y Servicio Civil (2016). Sentencia 00208 de 2016 (C.P. Edgar González López; Diciembre 16 de 2016). https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=88999

Consejo de Europa. (1981). *Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal* [Convenio 108]. Enero 28 de 1981. https://rm.coe.int/16806c1abd

Consejo de Europa (2018). *Modernised Convention for the Protection of Individuals with Regards to the Processing of Personal Data* [Convenio 108 +]. Junio de 2018. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Consejo Económico y Social. (1988). Resolución E/CN.4/Sub.2/1988/22. *Guidelines for the Regulation of Computerized Personal Data Files.* https://digitallibrary.un.org/record/43365?ln=es&v=pdf

Consejo Económico y Social. (2003). Resolución E/CN.4/Sub.2/2003/Rev.2. *Norms on the Responsibilities of Transnational Corporations and other Business Enterprises with Regard to Human Rights.* https://docs.un.org/en/E/CN.4/Sub.2/2003/12/Rev.2

Constitución Política de Colombia [Const]. Art. 15, 20. Julio 07 de 1991 (Colombia).

Corte Constitucional Colombiana. Sentencia de Unificación SU- 082 de 1995 (M.P. Jorge Arango Mejía; Marzo 01 de 1995).

Corte Constitucional Colombiana. Sentencia T- 612 de 2003 (M.P. Marco Gerardo Monroy Cabra; Junio 24 de 2003).

Corte Constitucional Colombiana. Sentencia C-748 de 2011 (M.P. Jorge Ignacio Pretelt Chaljub; Octubre 06 de 2011).

Dargent Bocanegra, E. (2001). *Las Empresas Multinacionales en el Derecho Internacional Público Contemporáneo.* Ius et Veritas, 12(23), 42-58 https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/16016/16440

Decreto 1074 de 2015. *Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo*. Mayo 26 de 2015. D.O. N49523.

Decreto 1081 de 2015. *Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República*. Mayo 26 de 2015. D.O. N49523.

Decreto 090 de 2018. *Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto número 1074 de 2015- Decreto Único Reglamentario del Sector Comercio, Industria y Turismo*. Enero 18 de 2018. D.O. N50480.

Decreto 255 de 2022. *Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.* Febrero 23 de 2022. D.O. N51957.

Google. (s.f). *Nuestra Historia. [Página web]* https://about.google/intl/es-419/our-story/

Hernández Zubizarreta, J. (2009). Códigos Externos. *Inter* jurídico-político. *Las Empresas Transnacionales Frente a los Derechos Humanos: Historia de una Asimetría Normativa. De la responsabilidad social corporativa a las redes contrahegemónicas transnacionales nacionales.* Hegoa; Observatorio de las Multinacionales en América Latina Asociación Paz con Dignidad. pp. 357-518. https://publicaciones.hegoa.ehu.eus/uploads/pdfs/79/Empresas_transnacionales_frente_a_los_derechos_humanos.pdf?1488539221

Kemp, S. (2024). *Digital 2024: Colombia.* https://datareportal.com/reports/digital-2024-colombia

Ley 222 de 1995. *Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones.* Arts. 27, 28, 207. Diciembre 20 de 1995. D.O. N42156.

Ley 1266 de 2008. *Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*. Diciembre 31 de 2008. D.O. N42219.

Ley 1581 de 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales*. Octubre 18 de 2017. D.O. N48587.

López, V. (2025). *Y ahora, ¿quién podrá defender nuestros datos?* Dejusticia. https://www.dejusticia.org/column/y-ahora-quien-podra-defender-nuestros-datos/

Novak Talavera, F. (1995). *La Contratación entre Estados y Empresas Transnacionales.* Agenda Internacional, 2(5), 133-162. https://revistas.pucp.edu.pe/index.php/agendainternacional/article/view/7160/7360

Organización de las Naciones Unidas. (1945). *Carta de las Naciones Unidas.* https://www.un.org/es/about-us/un-charter

Organización de los Estados Americanos. (s.f.) *¿Quiénes somos?* https://www.oas.org/es/acerca/quienes_somos.asp

Organización de los Estados Americanos. (1996). Resolución AG/RES. 1395 (XXVI-O-96). *Informe Anual del Comité Jurídico Interamericano.* https://www.oas.org/juridico/spanish/ag-res97/Res1395.htm

Organización de los Estados Americanos. (2010). Resolución AG/RES.2607 (XL-O/10) *Ley Modelo Interamericana sobre Acceso a la Información Pública.* https://www.oas.org/es/sla/ddi/docs/acceso_ley_modelo_libro_espanol.pdf

Organización de los Estados Americanos. (2011). Resolución AG/RES. 2661 (XLI-O/11). *Acceso a la Información Pública y Protección de Datos Personales*. https://www.oas.org/dil/esp/AG-RES_2661_XLI-O-11_esp.pdf

Organización de los Estados Americanos. (2011). Resolución CP/CAJP-2921/10 rev. 1 corr. 1. *Principios y Recomendaciones Preliminares sobre la Protección de Datos (La Protección de Datos Personales)*. Comisión de Asuntos Jurídicos y Políticos [CAJP]. https://www.oas.org/dil/esp/cp-cajp-2921-10_rev1_corr1_esp.pdf

Organización de los Estados Americanos. (2015). Resolución CJI/doc.474/15 rev. 2. *Privacidad y Protección de Datos Personales. https://www.oas.org/es/sla/cji/docs/CJI-doc_474-15_rev2.pdf*

Organización de los Estados Americanos. (2021). Resolución CJI/doc.638/21 . *Informe del Comité Jurídico Interamericano: Principios Actualizados del Comité Jurídico Interamericano Sobre La Privacidad y la Protección de Datos Personales, con Anotaciones.* Comité Jurídico Interamericano [CJI]. https://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf

Organización Internacional del Trabajo. (s.f). *Acerca de la OIT.* https://www.ilo.org/es/acerca-de-la-oit

Organización Internacional del Trabajo. (2022). *Declaración Tripartita de Principios sobre las Empresas Transnacionales.* https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_emp/%40emp_ent/documents/publication/wcms_124924.pdf

Organización para la Cooperación y el Desarrollo Económico. (s.f.) *Sobre nosotros.* https://www.oecd.org/en/about.html

Organización para la Cooperación y el Desarrollo Económico. (1980). Directriz C (80)58/Final. *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Organización para la Cooperación y el Desarrollo Económico. (2013). Directriz C (2013)79. *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013).* https://www.oas.org/es/sla/ddi/docs/oecd%20guidelines%20governing%20the%20protection%20on%20privacy%20and%20transborder%20flows%20of%20personal%20data.pdf

Organización para la Cooperación y el Desarrollo Económico. (2023). *Líneas Directrices de la OCDE para las Empresas Multinacionales sobre Conducta Empresarial Responsable.* OCDE/LEGAL/0144. https://www.oecd.org/content/dam/oecd/es/publications/reports/2023/06/oecd-guidelines-

for-multinational-enterprises-on-responsible-business-conduct_a0b49990/7abea681-es.pdf

Parlamento Europeo (2000). *Carta de los Derechos Fundamentales de la Unión Europea.* Diciembre 18 de 2000. D.O. N2000/C 364/01. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Parlamento Europeo (2012). *Versión Consolidada del Tratado de Funcionamiento de la Unión Europea.* Octubre 26 de 2012. D.O. No. 2012/ C 326/47. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT

Parlamento Europeo (2016). *Reglamento General de Protección de Datos.* Abril 27 de 2016. D.O. N2016/ L 119/1. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Red Iberoamericana de Protección de Datos. (s.f.) *¿Quiénes somos?* https://www.redipd.org/la-red/quienes-somos

Red Iberoamericana de Protección de Datos. (2017) *Estándares de Protección de Datos Personales para los Estados Iberoamericanos.* https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Remolina-Angarita, N. (2010). *¿Tiene Colombia un Nivel Adecuado de Protección de Datos Personales a la Luz del Estándar Europeo?* International Law Revista Colombiana de Derecho Internacional, 489-524. http://www.scielo.org.co/pdf/ilrdi/n16/n16a15.pdf

Rueda Gómez, D. (2012). *Regulaciones Nacionales e Internacionales en Materia de Protección de Datos Personales. Retos Globales en la Actual Era Digital.* [Trabajo de Grado, Universidad de los Andes]. Repositorio Institucional- Universidad de los Andes. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/b15eb3d0-9657-4485-bc89-c6606f970da6/content

Senado Estatal del Estado de California. (2018). *California Consumer Privacy Act* [CCPA]. Septiembre 23 de 2018. SB. 1121. https://theccpa.org/

Sepúlveda Amor, B. (1981). *La Regulación Internacional de las Empresas Transnacionales México ante Diálogo Norte-Sur.* Revista Colmex, *21*(4), 443-453, https://hdl.handle.net/20.500.11986/COLMEX/10002939

Superintendencia de Industria y Comercio. (2014). Concepto 14-218349 de 2014. [PDF]

Superintendencia de Industria y Comercio. (2019) *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales.* https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

Superintendencia de Industria y Comercio. (2020). Resolución 53593 de 2020. *Por la cual se imparten órdenes dentro de una actuación administrativa*. https://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/ORDEN%20GOOGLE(1).pdf

Superintendencia de Industria y Comercio. (2020). Resolución 70315 de 2020. *Por la cual se imparten órdenes dentro de una actuación administrativa*. https://www.sic.gov.co/sites/default/files/normatividad/082021/RE70315-2020.pdf

Superintendencia de Industria y Comercio. (2021). Resolución 14010 de 2021. *Por la cual se resuelve un recurso de reposición y se concede el recurso de apelación.* https://protecdatalatam.com/wp-content/uploads/2022/03/GOOGLE-RE14010-2021.pdf

Superintendencia de Industria y Comercio. (2021). Resolución 38869 de 2021. *Por la cual se resuelve un recurso de reposición y se concede el recurso de apelación.* https://www.sic.gov.co/sites/default/files/normatividad/082021/RE38869-2021.pdf

Superintendencia de Industria y Comercio. (2021). Resolución 60478 de 2021. *Por la cual se resuelve un recurso de apelación.* https://www.sic.gov.co/sites/default/files/files/2021/Resoluci%C3%B3n%2060478%20de%2021%20de%20septiembre%20de%202021%20(GOOGLE%20LLC).pdf

Superintendencia de Industria y Comercio. (2021). Resolución 72775 de 2021. *Por la cual se resuelve un recurso de apelación.* https://www.sic.gov.co/sites/default/files/estados/072022/RE72775-2021.pdf

Superintendencia de Industria y Comercio. (2022). Resolución 2389 de 2022. *Por la cual se resuelve una solicitud de revocatoria directa.* https://www.sic.gov.co/sites/default/files/boletin-juridico/Resolucion%202389%20de%2028%20de%20enero%20de%202022%20%28Google%20LLC%29.pdf

Superintendencia de Sociedades. (1999). *Responsabilidad de Matrices o Controlantes.* (Oficio No. 125-1063). https://www.supersociedades.gov.co/documents/107391/159040/OFICIO+Responsabilidad+Matrices.pdf/6aa872c8-ba06-434a-75b4-622e050e3b4b?t=1670905298838&download=true

Superintendencia de Sociedades. (2010). *Guía Práctica Régimen de Matrices y Subordinadas. https://www.supersociedades.gov.co/documents/20122/1229078/Guia-Practica-Regimen-Matrices-y-Subordinadas.pdf/6c4a9d36-224c-e72e-8bb5-eec20d380f4a?t=1654295200749*

Superintendencia de Sociedades. (2022). Circular Externa No. 100-000008. *Por la cual se reestructura y actualiza la Circular Básica Jurídica de la Superintendencia de Sociedades.* D.O. No. 52.093. https://incp.org.co/wp-content/uploads/2022/08/Circular-100-000008-de-2022.pdf

Superintendencia de Sociedades. (2024). *Inversión Extranjera.* (Oficio No. 220-034451). https://www.supersociedades.gov.co/documents/107391/159040/OFICIO+220-034451+DE+27+DE+FEBRERO+DE+2024.pdf/a464ee8c-8e50-198e-2856-89eea275e4ac?version=1.1&t=1710868753743

Teitelbaum, A. (2012). *Empresa Transnacional.* Observatorio de Multinacionales en América Latina. https://omal.info/spip.php?article4802.

Tribunal Administrativo de Cundinamarca. Sección Primera, Subsección C. Proceso con No. de radicado No. 25000234100020220044400. *Declarar la Nulidad de la Resolución No. 53593 de 03 de septiembre de 2020, la Resolución No. 14010 del 16 de marzo de 2021 y la Resolución No. 60478 del 21 de septiembre de 2021.* Abril 04 de 2022.