FACEBOOK: UNA POLÍTICA DE DATOS QUE GOBIERNA LA INTIMIDAD. ESTUDIO DEL CASO COLOMBIANO

POR:

ANGIE YULIETH VARGAS TAPIERO

C.C.: 1117548626

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE POLITÓLOGA

ASESOR:

FRANCIS MARGOT CORRALES ACOSTA

C.C.: 43164359

SOCIÓLOGA MAGISTER EN CIENCIAS POLÍTICAS

PROGRAMA DE CIENCIA POLÍTICA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

UNIVERSIDAD DE ANTIOQUIA

MEDELLÍN

2019

Facebook: Una política de datos que gobierna la intimidad. Estudio del caso colombiano*[1]

Angie Yulieth Vargas Tapiero: Estudiante de Ciencia Política de la Universidad de Antioquia, Medellín.

Resumen

Este estudio da cuenta del análisis del tratamiento de datos personales en RSV a partir del caso de Facebook enfocado en las afectaciones a la intimidad del ciudadano y cómo estas interpelan la posición del Estado colombiano. Lo anterior se logra en un abordaje en principio conceptual y teórico sobre el Estado y la intimidad, luego se adentra en el caso desde un análisis documental de la política de datos de la RSV con observaciones constantes desde secciones anteriores para finalmente en un análisis jurídico concentrarse en el caso colombiano y cómo esto constituye una problemática, demostrándose la permisividad del Estado en acciones de relegación o delegación en su obligación de garantizar la intimidad. Se encuentra relevante en este escrito el análisis selecto sobre los avances jurídicos e institucionales del Estado Colombiano según la intimidad como concepto que exige la discusión pública y política sobre su reglamentación. Se aspira al aporte en planteamientos analíticos para la continuación de investigaciones en el campo académico y político, como objeto que merecer ser pensado para construir institucionalidad desde las garantías de una ciudadanía en línea.

Palabras claves: Redes sociales virtuales; Facebook; Intimidad; Estado; regulación; datos personales.

Abstract

This study highlights the analysis of the processing of personal data at virtual social networks (VSN) focused on the case of Facebook regarding the affectations on the citizen's intimacy and how they relate with the position of the Colombian State. The above is achieved first through a conceptual and theoretical approach of the State and intimacy, then the analysis is

*Este artículo es producto de la investigación de trabajo de tesis, *Tratamiento de Datos Personales en internet: un trato sobre el Estado y el ciudadano*, para optar por el título de politóloga de la Universidad de Antioquia.

deepened through a documentary analysis of VSN's data policy with constant observations based on previous sections to finally centered on the Colombian case in a legal framework and how this constitutes a problematic situation, demostrating State's permissiveness in relegating or outsourcing its obligation to guarantee intimacy. The selective analysis of the legal and institutional development of Colombian State according to intimacy as a concept that requires a public and political discussion about its regulation is relevant in this paper. The aim of this work is to contribute analyzed approaches for the continuation of research in the academic and political field, as an object that deserves to be thought to build institutionality from the guarantees of an online citizenship.

Key words: Virtual social networks; Facebook; Intimacy; State; regulation; personal data.

Introducción

Debido al tratamiento de datos personales en plataformas en línea como son las redes sociales virtuales (RSV) han emergido acciones diferenciadas de los Estados a nivel global según su postura de interés. Las pretensiones regulatorias y garantistas de la Unión Europea (UE) marcan la pauta jurídica global con su extensa y especializada RGPD[2] y, sus antecedentes[3], o las mercantiles pero también regulatorias de EEUU que está trabajando en mejorar el control al tratamiento de datos personales precaviendo perjuicios en el mercado, obviando además los intereses del mercado global. Colombia, es el tercer tipo de Estado que emerge sin el avance jurídico de la UE y sin la capacidad y el interés en el mercado de los EEUU, pero buscando mediar entre ambas posturas, este tercer Estado es el de la mayoría de los estados a nivel global.

En términos investigativos el fenómeno consiste en el tratamiento de datos personales en internet a partir de las regulaciones diferenciadas que tienen los Estados en el marco de la globalización. Son varios los aspectos que tienen relación desde la Ciencia Política, se destacan: los efectos sobre las subjetividades ciudadanas en internet influenciadas por

[2] Reglamento General para la Protección de Datos: "relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (RGPD UE 2016/679).
[3] Veáse: Umbrella Agreement, Privacy Shield, caso Schrems y derecho al olvido.

relaciones entre usuario y red, la determinación de las relaciones colectivas que tienen lugar en el espacio virtual diseñado por las plataformas, y la relación de poder entre las plataformas y los Estados.

No obstante, es preciso concentrar esfuerzos en lo que se halla fundamental, el lugar de la intimidad en el tratamiento de datos y las regulaciones relacionadas, como principio del fenómeno debido al tipo de información tratada y los efectos sobre el sujeto. El concepto es lo suficientemente amplio para ser abordado desde diferentes ámbitos y disciplinas, sin embargo en esta ocasión es planteado desde la estatalidad, por tanto el objetivo es analizar rol del Estado colombiano como regulador garante del derecho a la intimidad del ciudadano respecto al tratamiento de datos personales de la red social virtual (de en adelante RSV) con más usuarios a nivel global, con un historial en casos legales relacionados, Facebook. Por ende, son dos los actores determinantes en la relación analizada, el Estado colombiano como garante de derechos, y Facebook como responsable del tratamiento a través del cual se ven los intereses del mercado virtual global, el ciudadano es el actor impactado por esta relación.

A pesar de lo dicho, se registra en la Ciencia Política una ausencia de análisis pertinente, si bien existen investigaciones concernientes a internet y la globalidad virtual en relación con el Estado, suele ser una lectura maniquea de la mutua exclusión per se de ambos actores, por sus lógicas propias (La territorialidad vs. La virtualidad, por ejemplo, Público vs. Privado); también se registran trabajos sobre el ejercicio ciudadano en línea entre personas, pero en estos no se revisa las relaciones entre los diferentes actores de la virtualidad que son las plataformas, el Estado y los ciudadanos. Desde otras disciplinas como el derecho la aproximación entre estos actores es meramente expositiva de la regulación actual.

Es pertinente este análisis en la disciplina, pues desde una lectura de las afectaciones sobre la intimidad de los ciudadanos y su relación con la institucionalidad del caso, proporciona críticas sobre el estado de las cosas, y cómo al Estado Colombiano le corresponden unas acciones puntuales para la mejor construcción de la institucionalidad según el enfoque presentado.

Entonces, la perspectiva de esta investigación es neoinstitucionalista tomando como referente a Mann, pues encuentra que es conveniente la interacción entre ambos actores y espacios concretos, Facebook como actor simbólico de internet y el Estado, dada la arena institucional

que este constituye, enfoque desde el que se demuestra la vinculación política del Estado colombiano con el tratamiento de datos personales en protección a la intimidad, como una de las actividades de la sociedad donde es necesaria la penetración regulatoria del Estado.

En consecuencia, las observaciones críticas que propone este artículo están dirigidas al aporte en la discusión pública y política sobre la regulación de la intimidad desde el tratamiento de datos personales para el caso colombiano, y se proyecta que sea insumo para futuras investigaciones académicas e institucionales.

La metodología de esta investigación fue cualitativa, un análisis de caso a partir de técnicas documentales y complementarias. Se recurrió como fuentes a la política de tratamiento de datos de Facebook y los documentos normativos nacionales, a los reportes periodísticos y noticiosos de eventos conexos, también a documentos de investigaciones académicas relacionadas con el campo de este caso. Además, se utilizó la técnica de observación sobre el funcionamiento la RSV y plataformas ligadas. Finalmente, se complementa con tres entrevistas realizadas, dos iniciales a una funcionaria de la SIC y una a un investigador asistente del Parlamento Europeo perteneciente a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, la última fue hecha en el cierre de la investigación a un funcionario especializado de la Delegatura de Protección de Datos Personales de la SIC.

Por último, el recorrido analítico consiste en primer lugar definir el Estado como infraestructura institucional penetrante en el ejercicio ciudadano y del mercado, para luego demostrar que la intimidad es igualmente convocante de la intervención regulatoria del Estado en función de la protección a la dignidad y del desenvolvimiento libre del mismo ciudadano. Para entender la aplicabilidad de ambas propuestas teóricas en el caso, se explica el funcionamiento de Facebook desde sus políticas y su relación con las propuestas de Estado e intimidad. Redondeando se hace una valoración del caso colombiano como está dado y se resaltan las problemáticas alrededor, centrando la atención en la autoridad nacional para la protección de datos, la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio. Finalmente se concluyen con reflexiones construidas.

1. El Estado: una infraestructura de poder sobre otros poderes

Según Michael Mann el Estado es en principio una organización socioespacial, dicha organización tiene unas fuentes, tipos y funciones. Además puede ser vista como un actor: las elites estatales; y en tanto, es posible imputarles intereses desde la teoría de la acción racional (Mann, 1991). Entre las fuentes del poder del Estado está el poder político, derivado de la necesidad social de regulación, funciona como red y puede atrapar a otros poderes y a las poblaciones en su diagrama de organización (Mann, 1991).

El poder que ejerce el Estado puede ser de dos tipos, infraestructural o despótico, en la actualidad los regímenes altamente coercitivos, impositivos y poco negociadores, cuyo recurso frecuente sea la violencia son poco comunes y han ido en decadencia, el tipo de poder predominante en los estados actuales es el infraestructural, consiste en la capacidad de penetrar la sociedad civil a través de acciones coordinadas centralmente, es esto la clave de la adaptación del Estado al modelo democrático predominante, dado que se ocupa en tal proporción de la vida de los ciudadanos desde la regulación que aquellos no pueden negarse a su cumplimiento pues tendrían repercusiones sobre toda su vida regulada.

Seguidamente, por las múltiples funciones del Estado el autor hace referencia a cuatro, el mantenimiento del orden interior, la defensa/agresión militar, el mantenimiento de las infraestructuras de comunicación, y la redistribución económica; de las anteriores es conveniente denotar la definición que de la primera hace, puesto que asume al Estado como un interventor de las relaciones socioespaciales donde hay desigualdad, y donde puedan haber usurpaciones arbitrarias (Mann, 1991, p. 64), razones que suelen justificar las regulaciones del mercado. En una aplicación al caso, Saltor sostiene en relación al almacenamiento de datos:

> Surgen así nuevas asimetrías en las relaciones entre los ciudadanos y los poderes públicos y privados. La acumulación de grandes cantidades de información que afectan a la intimidad de las personas, ha generado un nuevo tipo de dominio, desconocido hasta no hace mucho tiempo (Saltor, 2013. p. 37).

En conjunto, el Estado en Mann es uno que tiende a intervenir a través de su infraestructura penetrante, y donde el poder político reconoce su facultad de acción sobre otros poderes, el del mercado, por ejemplo. Esto resulta coherente con la función del mantenimiento del orden interior, ya que el Estado tiene un rol de limitar o regular relaciones cuando haya desigualdad,

y por supuesto sea problemático, sin que esto signifique la extinción de poderes y actividades privadas. Asumiendo el tratamiento de datos la evolución tecnológica como necesidad, incluso en este caso cabe su moldeamiento por el Estado: "Más aún, las redes de poder no sólo satisfacen necesidades humanas sino que también las moldean" (Márquez, 2016, p.21).

La regulación del tratamiento de datos personales en Internet en el caso europeo y también en el estadounidense tiene lugar en respuesta a escándalos por el abuso en el tratamiento de la información personal, arbitrariedades. La intervención del Estado se justifica en lo fundamental de proteger la privacidad e intimidad, que en el marco colombiano es mejor llamado habeas data e intimidad, también el cercano caso del habeas data financiera valida en analogía esta hipótesis[4].

2. Intimidad: una posibilidad de decisión acerca de lo público y lo privado.

La intimidad como concepto refiere a varias interpretaciones históricas. En un inicio desde una perspectiva filosófica de antigüedad griega, cuando era clara la pretendida distinción entre lo público y lo privado, ubicando la intimidad dentro de esto último, en relación a lo íntimo, lo oculto, las emociones y los sentimientos, la intimidad hacía referencia "a una persona en sus relaciones consigo misma" (Sánchez, 2016, p. 70); es decir, una interpretación negativa en tanto significa la negación de acción, la exclusión de injerencia sobre lo íntimo, dado su nexo fundamental con la constitución del yo, de la identidad, sustancia del sujeto libre de intromisiones (Celis, 2006; Guerrero, 2009). Más adelante, en medio del apogeo de los medios de información, esto es, de terceros haciendo público lo que antes se consideraba reservado, Warren y Sabiers a finales del siglo XIX iniciaron el trayecto histórico para hacer de la intimidad una concepción positiva en el derecho, es decir, un fundamento de acción del ciudadano en un estado de derecho, de esta manera el concepto supera el binarismo de las esferas pública y privada, y se ubica ahora como principio de acción del sujeto para la

[4] La SIC ha impuesto multas que superan los 21 mil millones de pesos en sus funciones de inspección, vigilancia y control del régimen de protección de datos personales, que empezó a regir en 2010, incluye la ley 1581 de 2012 y 1266 de 2008, el 80% de las sanciones están relacionadas con violaciones a esta última, la ley del habeas data financiero.

separación categórica de sus esferas, derivando en derechos mucho más específicos como la autodeterminación de la información (Sánchez, 2016; Saltor, 2013).

De lo anterior es importante resaltar que a pesar de que la intimidad como concepto escapa de ser enmarcada en el binarismo público-privado, se mantiene por condición en una relación estrecha con la identidad del sujeto en tanto determinante para lo que este decide compartir o reservar, en efecto, lo íntimo que es lo propio del sujeto mantiene esta condición –el individuo no pierde pertenencia sobre lo propio- sin importar que esto sea hecho público o se mantenga en desconocimiento de la sociedad, también más allá de la condición pública o privada. Es precisamente la constante relación con el mundo exterior y las emociones lo que hace que lo íntimo sea tan influenciable como la persona misma. (Yepes, 1997).

En el marco de internet, donde lo que circula es información codificada en datos, lo relativo a una persona y su intimidad, es tratado como dato. Lo íntimo, lo más propio del sujeto es encasillado en la categoría de datos sensibles, los cuales se reconocen:

> como los datos que afectan a lo más propio de la persona, podríamos decir a su intimidad. Son todos aquellos que identifican o permiten la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, de salud, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias puede llegar a constituir una amenaza para el individuo. (Pfeiffer, 2008, p. 25).

Es preciso apuntar que la intimidad en internet se traduce en dos asuntos. El primero es la posibilidad de decidir ocultar o publicar información y, el segundo consiste en la identificabilidad del sujeto desde datos sensibles que circulan en línea. Según Sánchez (2016), los datos son sensibles para el sujeto, según Sánchez por lo que significan en la construcción de su identidad, pues dan cuenta de lo íntimo y, sostiene el autor, es sobre esto que se forjan decisiones propias, desde donde también se garantiza el desenvolvimiento de la personalidad y la conducta del sujeto.

Una demostración de esta teoría sobre la intimidad es el *profiling*, técnica usada en el tratamiento de datos con la que es creado un perfil de la persona a partir del cruce o la manipulación de datos primarios obtenidos (interacciones, actividad en internet, publicación

de contenido, características del dispositivo). Perfil que consiste en buena medida en datos sensibles construidos, cuya utilidad es el direccionamiento de la conducta en internet de la persona.

A estas nuevas prácticas obedece un cambio de paradigma que define el derecho a la intimidad, -antes referido al derecho a mantener oculto-, como el "derecho activo sobre el flujo de la información personal" (Celis, 2006, p. 76). Significa la posibilidad por derecho de decidir sobre lo que se oculta y lo que se comparte, derivando en esta medida en un control sobre el uso que otros hagan de la información personal (Macavilca, 2017). Se acepta que la información personal concerniente a la intimidad de la persona puede ser tratada por otros, pero también que ese tratamiento, el cual es un uso de la información, puede ser limitado por el derecho a la intimidad mismo, la información continúa perteneciendo al sujeto, lo que otorga derechos a éste.

Sánchez (2016) sugiere como un derecho derivado la autodeterminación informativa, "facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida tanto en registros públicos como privados, especialmente, aunque no exclusivamente, en aquellos almacenados en medios informáticos" (p.79). Entre tanto, Macavilca (2017) presenta así la libertad informática: "la facultad de controlar la identidad personal informática a través del consentimiento para preservar, acceder, o rectificar datos informativos referidos a la vida privada de las personas" (p. 181). La intimidad como lo decidido sobre sí mismo, se transforma en el control sobre lo decidido a través de otros derechos derivados.

Macavilca (2017) continúa su disertación señalando que, en el contexto de globalidad virtual, donde el sujeto también se construye desde las redes de información, como es el caso de las redes sociales virtuales donde deposita datos que le conciernen, el derecho a la intimidad se convierte en la posibilidad de controlar la identidad informática a través del consentimiento dado en estas redes.

Por otra parte, Celis (2006) se refiere acerca del control de lo publicado, señalando que el derecho a la intimidad implica también un derecho a oponerse al tratamiento de datos personales, puesto que significa en principio el derecho a la disposición de la información

personal ya preservarla de potenciales agresiones, en coherencia con lo expuesto por Sánchez (2016), que lo señala como decidir la finalidad y uso de la información personal.

Es así como la intimidad se reconoce como objeto de protección por parte del Estado en diferentes países, no solo por lo que en principio significa para la dignidad humana sino también por sus riesgosos usos posibles. Se señala, por ejemplo, la identificabilidad de las personas a través de escasos datos o informaciones personales mediante herramientas informáticas lo que puede ser origen o causa de acciones discriminatorias, es decir, potenciales agresiones (Sánchez, 2016) para un sujeto que se encuentra indefenso, dada la veracidad de la información y lo sensible a la persona (Celis, 2006); o, en cualquier caso, de abuso de la información contra lo que la persona estime una expectativa razonable de intimidad (Guerrero, 2009).

Es pertinente retomar a Macavilca, quien se concentra en las condiciones actuales de Internet, sostiene que el derecho a la intimidad significa la posibilidad de mantener el anonimato en las comunicaciones y por tanto controlar la identidad informática. En el caso de Facebook, el derecho a la intimidad se reduce a lo que el contrato diseñado por la RSV específica, imponiendo de manera unilateral una concepción inmodificable por el usuario del derecho a la intimidad, un contrato por adhesión (Sotelo, 2012) como se verá más adelante, desde la cual se imposibilita para sus usuarios y no usuarios el anonimato.

Frente a esto, es indispensable las categorías resaltadas por Sánchez (2016) de conocimiento y consentimiento pues significa que, más allá de llenar casillas para continuar con el registro en una red social, es importante que el usuario conozca las consecuencias para su intimidad y que comprenda la relevancia de lo que permite. Incluso, es fundamental que los contratos para el tratamiento de datos personales den lugar a un control de la información personal por parte del usuario que es también ciudadano, que los contratos conciban el derecho a la intimidad como un límite propio de la dignidad humana sobre el tratamiento de datos personales en redes sociales virtuales, en otras palabras, que no sea solamente la conveniencia de la RSV lo que defina la intimidad (el control sobre la información) para cada usuario sino que estos tengan per sé unos atributos propios de ciudadanos que les permitan limitar los contratos del tratamiento de datos personales, atributos que por supuesto no existen sin un marco legal de garantía ni protección estatal.

3. Tres puntos de análisis para acercarse a la red social virtual

Facebook es observada desde tres puntos problematizados: el primero, el consentimiento en el proceso de registro; el segundo, la indexación según el diseño del algoritmo y sus consecuencias; el tercero y último, la regulación.

Para registrarse en Facebook basta con unos datos: nombre, apellido, correo electrónico, fecha de nacimiento, y explicitar si se es hombre o mujer. Al llenar estos datos, lo siguiente es una casilla para marcar: "Al hacer clic en registrarte, aceptas nuestras condiciones, política de datos y la política de cookies. Es posible que te enviamos notificaciones por SMS que puedes desactivar cuando quieras" (Facebook). Los primeros datos recolectados por Facebook parecen poco significantes, apenas necesarios y son insuficientes. También es necesario hacer clic en aceptar las políticas antes enunciadas, tras haber autenticado el correo y entonces es posible hacer uso de los servicios de la red social virtual.

Del proceso de registro es pertinente identificar el consentimiento dado en un contrato por adhesión (Sotelo, 2012). El contenido de este es por completo definido por la plataforma y el usuario acepta meramente sin posibilidad de objetar o negarse a alguna de sus cláusulas, a pesar de la sensibilidad de algunas de ellas.

Desde el funcionamiento, estar activo en Facebook es crear, observar o compartir contenido de interés personal, pues son usuarios registrados los que navegan en la plataforma. El contenido visto en Facebook, en su feednews son publicaciones de perfiles seguidos y algunas sugeridas por la misma plataforma, ambas tienen un método de selección basado en las interacciones analizadas del usuario. Existe una selección de publicaciones (ya que no se ve todo lo publicado por los perfiles seguidos) y un orden en la exhibición de esa misma selección (no se ven las publicaciones en orden cronológico sino de relevancia) basado en lo que Facebook calcula puede interesar al usuario.

Sobre la indexación hay dos cuestionamientos. El primero de ellos es cómo son leídos los datos que le dan pistas a Facebook sobre cada usuario, y el segundo, las consecuencias o mejor dicho, la particularización del contenido, fragmentando la realidad en la feednews de cada usuario.

La pretensión de ampliar el consumo de contenido como de cualquier servicio es lo esperado de una empresa, lo cuestionado del funcionamiento es el mecanismo para ello. Siguiendo las políticas de datos y de condiciones del servicio de la RSV se reporta la obtención o recopilación de datos personales y su análisis por parte de Facebook, cuyo resultado son gustos o intereses probabilísticamente encontrados. El primer aspecto problematizador en el funcionamiento de la RSV es cómo son leídos los datos personales, y cuál es el interés priorizado a la hora de sugerir contenido, es decir, en qué consiste el diseño del algoritmo que indexa.

Lo segundo en la indexación del contenido son sus consecuencias en tres estancias: la primera, la lectura dirigida que los usuarios hacen de su realidad virtual, de esto hace parte no sólo la selección de lo mostrado sino también la prohibición de lo que Facebook estima no se debe hacer público, afectando en principio la forma de informarse; la segunda, el direccionamiento de la decisiones y acciones en la red, pues el sujeto está informado por un contenido limitado; la tercera, la fragmentación de la sociedad dadas las realidades paralelas para los usuarios, según Magnani leyendo a Castells, (Magnani, 2017).

Por último, la regulación de Facebook que se reduce a la plataforma misma o la falta de claridad sobre la regulación. Según la RSV la regulación que le atañen son las políticas dadas por ella misma en el contrato por adhesión y el marco jurídico que limita a éste, -de un estado de Estados Unidos con mínimas posibilidades de acceso para los usuarios de otras partes del mundo, como Colombia-, (Políticas de tratamiento de datos, Facebook) reduciendo la regulación a la que tiene acceso el usuario a la plataforma misma. Para el caso de las regulaciones de conducta delictiva, Facebook asegura enmarcarse dentro de las legislaciones internacionales. Hasta este punto se cuestiona el vacío de límites externos en la relación usuario-red que redunda en la falta de garantías para el usuario (Márquez, 2015).

Empero, a pesar de lo aseverado por la RSV, la SIC a través de la resolución 1321 de 2019, asegura que todo tratamiento que se haga en Colombia está sujeto a la ley nacional y por tanto hay dos responsables en el caso del tratamiento de datos personales en Colombia por parte de Facebook: Facebook inc. y Facebook Colombia. Lo cual es confirmado por la conducta de Facebook que responde los llamados de la institucionalidad colombiana a través

de las respuestas registradas en la misma resolución, aunque esto parezca contradictorio con lo anunciado en sus políticas internas.

En otras palabras, el usuario tiene unas obligaciones innegables para con Facebook una vez accede a su uso, pues Facebook mismo establece mecanismos para el obligatorio cumplimiento como la eliminación de contenido o la suspensión de cuentas cuando se viola las normas de convivencia, no obstante, ¿cuáles son las obligaciones de Facebook para con sus usuarios?, ¿quién vigila o controla su cumplimiento? Esto es resuelto no satisfactoriamente más adelante principalmente desde la ley 1581 y la Delegatura de Protección de Datos Personales.

En suma, el registro es abordado desde del consentimiento, es decir, cuáles son las condiciones para que éste sea aceptable ética y políticamente más allá de lo legalmente válido cuando existe una completa sumisión del usuario dado el tipo de contrato. Y, este es relevante porque es a través del consentimiento del usuario que se recurre a ciertas prácticas bajo la premisa de la autorización dada. La indexación es de interés ya que los datos personales son recopilados y cruzados, cuyos resultados son más datos personales y en algunos casos sensibles, pues son los datos los que dan cuenta de la intimidad del usuario; en cambio, las consecuencias o afectaciones a pesar de estar relacionadas con el desarrollo de la conducta con base a la intimidad y la constitución de la identidad, excede la discusión política al respecto y exige unas perspectivas y análisis específicos desde ámbitos filosóficos, sociológicos y antropológicos. La regulación por su parte establece los límites y garantías para los actores que son partes y afectados en este proceso desde el registro, la indexación y sus consecuencias, en este caso mostrado.

Desde la superficie este asunto convoca a una discusión acerca del poder privado (Facebook) sobre la privacidad o intimidad de los usuarios que significa el tratamiento de datos personales. Para ahondar es necesario detenerse en la política de datos como se hará a continuación.

- **Políticas internas como evidencia**

En concreto, lo expreso en la política de datos de Facebook es la recolección y el uso de la información, correspondientes a las gráficas 1 2.

RECOLECCIÓN DE DATOS (cómo se obtienen los datos)		
Según quien los proporciona	**Cómo se proporciona**	**Datos**
Usuario	El usuario (directamente)	Ubicaciones de fotos, fechas de creación de archivos, contenido.
	Redes y conexiones	Páginas, cuentas, hashtags usados y grupos con los que el usuario está conectado y la interacción, también las personas con las que más se comunica el usuario, o los grupos de los que hace parte el usuario.
	Uso	Usos de los Productos, contenido visto o con el que se interactúa, (like o reacciones, comentarios, por ejemplo), funciones utilizadas y acciones del usuario, interacciones del usuario con cuentas y personas, y hora, frecuencia y duración de las actividades con las actividades.
	Actividad de otros usuarios	Comentarios e interacciones de otros usuarios con el contenido del usuario y mensajes, entre otros.
	Transacciones	Información de pago y de tarjeta más otros detalles.
Información del dispositivo	Atributos	Del software y hardware del equipo: modelo, nombres de aplicaciones y archivos, almacenamiento disponible, comportamientos, operaciones, señales, plugins, cookies, configuración del dispositivo e identificadores (único, los del dispositivo y de aplicaciones en específico).
	Operaciones	
	Identificadores	
A través de socios		A través de plugins sociales (Botón de megusta, por ejemplo), inicio de sesión con Facebook, API y SDK, o el pixel de Facebook, se conoce actividades realizadas por el usuario fuera de Facebook, datos sobre el dispositivo utilizado, sitios web visitados, compras hechas, anuncios vistos, uso de servicio.

Gráfica 1. Tabla de resumen sobre la recolección de datos personales. **Fuente**: Elaboración propia, basada en la Política de datos de Facebook.

Las primeras observaciones son sobre la recolección. Dentro de lo que el usuario proporciona es importante resaltar la diferencia que se hace en el mismo contrato entre lo que se proporciona explícita o directamente y lo que Facebook obtiene a través del usuario, dando lugar a cuestionar qué tanto puede conocer el usuario de lo que se recoge sobre él. Luego, en redes y conexiones, la diferencia no explicada entre los grupos con los que el usuario está

conectado y a los que pertenece es síntoma de una falta precisión constante dentro del contrato. Finalmente, y aún más importante, a través de socios se obtiene información con la siguiente condición: "ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella" (Facebook), esto último es de suma gravedad porque implica que el contrato de la RSV también aplica para personas que no se hayan registrado, y que por tanto no hayan hecho clic en aceptar las políticas y condiciones, esto es una tercerización del consentimiento de los no usuarios, consentimiento que no es posible rastrear en su autorización puesto que se desconoce la forma exacta de contrato en cada servicio socio de Facebook.

No obstante, todos los datos recolectados no son relevantes en sí mismos, sino por su utilidad, y esto depende de que conformen una unidad de sentido en relación con el usuario al que pertenecen, o sea que significan al ser cruzados o conectados con otros datos en el proceso de perfilación o profiling. Se trata de la creación de un perfil del usuario con sus gustos, intereses, personalidad, a partir del análisis de los datos recolectados creando nuevos datos personales, en buena medida sensibles (preferencias sexuales, políticas, condición económica, etc.), con el fin de direccionar los contenidos visibles para el usuario, dígase, direccionar la conducta de navegación incluso más allá de la plataforma. Es importante denunciar que no se hace explícito el tratamiento de datos sensibles dentro de las políticas de datos de la RSV, es decir, no se reconoce la categoría legal y ética de los datos tratados.

Según las políticas este es el fin de los datos:

USO (Cómo se usa la información)			
Qué se usa	**Quién usa**	**Qué entrega Facebook**	**Para qué se usa**
Proporcionamos, personalizamos y mejoramos nuestros Productos	A vendedores y proveedores de servicio y Anunciantes	Análisis, informes de medición, estadísticas y observaciones.	Proporcionar los Productos a partir de la personalización de funciones y contenido para la uniformación de la experiencia en todos los Productos de Facebook, para hacer más relevante el contenido visto. En el caso de los anuncio para seleccionar y personalizar anuncios, ofertas y otro contenido publicitario que te
Información de los dispositivos y Productos de Facebook			
Información relacionada con la ubicación			

Reconocimiento facial Anuncios y otro contenido publicitario Ofrecemos mediciones, análisis y otros servicios empresariales			mostramos. Las mediciones y análisis son usadas para ayudar a los socios a medir la eficacia y la distribución de sus anuncios y servicios, para hacerles conocer qué personas usan sus servicios y cómo interactúan con sus sitios web, aplicaciones y servicios.
Información y contenido	socios investigadores y académicos	Información y contenido	Investigaciones que permitan profundizar los conocimientos y la innovación que den soporte a nuestro negocio o nuestra misión

Gráfica 2. Tabla de resumen sobre la el uso de datos personales. **Fuente:** Elaboración propia, basada en la Política de datos de Facebook.

Sobre el uso es necesario hacer explícita la ambigüedad constante en términos como personalizar o la relevancia del contenido, cuando no se explica en qué consisten, o los criterios tenidos en cuenta para ello, igualmente, el enunciado interés de dirigir el contenido para su mayor consumo deja en claro únicamente el objetivo determinante, el cual guía acciones de mercado desconocidas por el usuario que incumben su información personal y afectan su comportamiento en los servicios de internet de los que Facebook sea socio.

La información obtenida por Facebook acerca de sus usuarios afecta el derecho a la intimidad de los mismos en dos sentidos, tanto por la decisión de publicar u ocultar información como por la identificabilidad del usuario. En el primer sentido, es clara la relación sobre la autorización dada y sobre si esta es explícita previa e informada, como ya se ha demostrado con las observaciones el cumplimiento del criterio de explicitud no es verosímil, y también se cuestiona lo accesible al entendimiento que sea la información dada, son tres los acuerdos que acepta el usuario con un clic[5]. La identificabilidad, por su parte, tiene relación con los datos sensibles que permiten la perfilación y el reconocimiento del usuario a través de sus prácticas.

[5] Condiciones, Políticas de datos y Políticas de cookies.

Se demuestra a este punto que el tratamiento de datos personales es un tratamiento de la intimidad, tanto por los datos insumos como por la fabricación de perfiles y el posterior direccionamiento de la conducta virtual. Anótese que la intimidad como derecho positivo reside entre lo que se pública y lo que no, y que como concepto filosófico refiere también a determinación de la identidad que implica el desenvolvimiento de la personalidad según Sánchez (2016). Véase que incluso lo que el usuario decide no publicar, con lo que interactúa pero no quiere compartir, es también objeto de lectura, análisis, observación, y convertido en estadísticas e informes que son posteriormente vendidos a empresas relacionadas con Facebook.

Frente a los posibles usos de esta información se encuentra el trabajo de Michal Kosinski, David Stillwell, y Thore Graepel (2013) quienes a través de un análisis basado en los datos de los perfiles en Facebook, un listado de sus likes e información de encuesta, demostraron lo predictible de la información personal de los usuarios. Para lograr su cometido, los investigadores distinguen entre los datos registrados por los usuarios y la información predecible, es así como para su estudio trabajan con 58,466 voluntarios por medio de una plataforma virtual. Dentro de la información de usuarios descubierta se encuentran la orientación sexual, origen étnico, posición política, religión, personalidad, inteligencia, satisfacción con la vida, uso de sustancias, entre otros.

Teniendo en cuenta lo anterior, los investigadores concluyen que la información obtenida depende de la data recolectada, señalando que, de tener otro tipo de registros más variados, así mismo sería la información predicha, haciendo referencia a registros como historiales de búsqueda, de visitas a otros sitios web, como sucede con los registros de los que dispone Facebook. En esta orden, señalan que la información obtenida puede ser usada para proveer servicios o productos, como es el caso de servicios de venta que adopten su funcionamiento al perfil del usuario, ofreciendo los productos según el estado de ánimo conveniente del usuario (Kosinski, Stillwell & Graepel, 2013). Entre los riesgos negativos que concluyen los investigadores se encuentra el uso de la información personal perfilada sin el consentimiento individual o la notificación al usuario, aseverando:

> "Commercial companies, governmental institutions, or even one's Facebook friends could use software to infer attributes such as intelligence, sexual orientation, or

> political views that an individual may not have intended to share" (Kosinski, et al., 2013, p. 4).

Lo sucedido en la investigación anterior funciona de manera similar a Facebook según su propia política de datos, salvo que en este caso es mucha más la data recolectada y mucho más amplia variedad de información predecible y mayor su asertividad, por tanto mayor es el peligro de un tratamiento no por completo consentido. El supuesto de identificabilidad se confirma cuando las sugerencias de contenido dentro y fuera de Facebook (contenido sugerido en el feed news de la RSV así como avisos publicitarios en las sitios web de las empresas socias) demuestran ser el resultado de la inferencia, o sea, de la predicción de los posibles gustos e intereses de los usuarios y no usuarios que visitan los sitios web socios por Facebook para sus análisis, estadísticas, informes y observaciones.

En continuidad, predecir según la información personal significa la persuasión manipuladora de lo íntimo sobre la capacidad deliberativa del usuario, capacidad que reside en la intimidad según Sánchez (2016). Se confirma entonces que la intimidad significa más allá de lo dado como público o privado, siendo también las bases de la conducta del sujeto, evidente en estas prácticas de internet. Esto es bien sabido dada la inteligencia artificial y otras herramientas tecnológicas usadas por Facebook y empresas para garantizar una prestación eficiente de sus servicios y una venta de sus productos.

En consideración de lo que se estima consiste el tratamiento de datos personales, Sotelo (2012) rescata los siguientes riesgos en un tratamiento inadecuado de datos según el GECTI (Universidad de los Andes):

> "la publicación de datos que por su naturaleza pertenecen a la esfera íntima de la persona; publicación de información errónea, inadecuada, incompleta, desactualizada o parcializada; manipulación o cruce de los datos almacenados que permiten crear perfiles virtuales" (p. 241).

Desde Cambridge Analytica (CA en adelante) se demuestra que los peligros pueden ir mucho más allá de lo estimado por Sotelo, se le relaciona con la elección de Trump y otras. En este caso se encuentra la utilización indebida de datos personales de 50 millones de usuarios de Facebook a nivel mundial, datos obtenidos a través de la aplicación *thisyourdigitallife*,

desarrollada por Dr. Aleksandr Kogan. Con estos datos se crearon perfiles psicográficos de los usuarios, con los que CA influenció de manera confiable a estos en función de manipular su comportamiento electoral y de mercado con las llamadas "noticias falsas" en varias plataformas socias de Facebook y en esta misma (Resolución 1321).

CA ocupa la agenda pública mundial en este orden, el 11 de diciembre de 2015 con el artículo de The Guardian sobre CA en la campaña de Cruz inicia el historial en medios de esta empresa de publicidad y sus polémicas, continúan algunos reportajes, la mayoría en medios anglosajones sobre la elección de Trump, el Brexit, Kenia y México. Pero, es el 17 de marzo de 2018 donde explota, sale a la luz las denuncias y evidencias de CA en el poder global, The Guardian, The New York y The Observer publican en sus portales artículos relacionados con testimonios y cifras. En Colombia la ola de esta noticia internacional inicia con dos medios reportando el 19 de marzo, pero es el martes 20 de marzo que se ubica en toda la agenda nacional. Seguidamente, en el espacio local evoluciona el escándalo por la aplicación Pig.gi y la especulación sobre su uso en campañas nacionales y locales[6].

La intimidad en el tratamiento de datos personales de Facebook le incumbe al Estado porque hay un ejercicio de poder privado que puede ser arbitrario contra el ciudadano-usuario en diferentes instancias del tratamiento, como lo demuestra la siguiente lectura de política de datos. En suma: 1. La autorización en el contrato por adhesión donde el usuario tiene nulas posibilidades de negociación. 2. El consentimiento no solo es falto de negociación sino que está sujeto al consumo de un servicio de uso mayoritario en el país, 68% de los colombianos están en Facebook, condicionando materialmente la libertad de decisión. 3. La capacidad tecnológica de Facebook para recopilar información en otras plataformas sin un consentimiento explícito del usuario. 4. La capacidad de influencia sobre el comportamiento del usuario en la red dado el diseño de algoritmos que indexa y sugiere contenido. 5. La

[6] Estos datos corresponden a un rastreo investigativo sobre el caso de Cambridge Analytica en medios globales, se encuentra que existe un descubrimiento periodísitico y la reproducción del escándalo noticioso en medios de diferentes países. Se registran: 16 noticias de seguimiento previo al escándalo global en medios extranjeros y nacionales, entre diciembre de 2015 y febrero de 2018; dos publicaciones del descubrimiento periodístico el 17 de marzo de 2018; en Colombia se encuentras 21 publicaciones relacionadas al caso entre 19 de marzo y 4 de abril de 2018. Se anexa la matriz evidencia del rastreo.

ausencia de recursos y mecanismos legales para que el usuario pueda demandar otras condiciones.

4. Un marco legal poco especializado y evasivo con sus obligaciones fundamentales

El marco legal colombiano es abordado primero desde una exposición descriptiva; luego desde observaciones críticas de otros documentos legales y propios de la investigación, finalmente desde una perspectiva en relación al caso, al cumplimiento y suficiencia de la norma en relación a Facebook. Lo anterior se consigue concentrándose en la ley 1581 y la figura de autoridad sobre el caso que es la Delegatura de Protección de Datos Personales de la SIC.

En primer lugar la intimidad como concepto tiene antecedentes jurídicos propios en Colombia, mas la regulación pertinente para el caso concreto de este análisis, Facebook, corresponde mejor a la categoría de datos personales dentro de la cual interfieren otros derechos como el habeas data. La relación con la intimidad se da sustancialmente sobre los datos sensibles, pero como se ha demostrado los datos personales ordinarios son útiles para la técnica de profiling solo por la construcción de datos sensibles. A continuación se aborda la legislación pertinente al tratamiento de datos personales en Colombia seguida de las críticas respectivas.

La apertura conceptual al respecto la presenta Monsalve (2017), quien observa la diferencia entre datos personales e información traída de la sentencia T414 DE 2012, “dato es aquel elemento que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella”, e información es “más que los datos concernientes a un individuo que lo identifican o lo hacen identificable, aquellos datos que tienen un efecto directo en su vida privada, con capacidad de determinar su existencia y libertad de tomar decisiones” (T414, 2012). Además de múltiples sentencias de la Corte Constitucional también es un antecedente jurídico fundamental la ley 1266 de 2008, el Habeas data financiero, precedente en la protección de datos personales.

Respecto a los datos personales en su amplitud para uso más allá del sistema financiero, la legislación colombiana está enmarcada en la ley 1581 de 2012, cuyo objeto es “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las

informaciones que se hayan recogido sobre ellas en bases de datos o archivos" (ley 1581, 2012). El ámbito de aplicación es el "tratamiento de datos personales efectuados en el territorio colombiano o cuando la legislación sea aplicable en virtud de normas o convenios vigentes" (ley 1581, 2012), aplica incluso a "proveedores de servicios de redes sociales digitales, aunque su sede principal no se encuentra en el territorio colombiano, o parte del tratamiento se efectúe fuera del mismo" (Resolución 1321, 2019).

Según la ley 1581, los tres actores en el tratamiento son: titular, responsable y encargado. Para el caso de Facebook, se resaltan los siguientes principios de la misma legislación: de libertad, entendida para este caso como el consentimiento previo, expreso e informado (ley 1581, 2012); de veracidad o calidad de la información, entendido como que esta debe ser "veraz, completa, exacta, actualizada, comprobable y comprensible" (ley 1581, 2012); de transparencia, "obtener información acerca de la existencia de los datos que conciernen al usuario" (ley 1581, 2012); finalmente, también el principio de seguridad, sustancialmente definido como evitar la adulteración y el acceso no autorizado de la información.

Así mismo se interpreta tácitamente una clasificación por regulación de tres datos personales entre, público, privado o sensible, de la cual cabe destacar que los datos sensibles se definen como "aquellos que afectan la intimidad del titular o cuyo uso indebido pueda generar discriminación" (1581 de 2012). De otro lado, se reconoce como derechos de los titulares: conocer, actualizar y rectificar, así como revocar la autorización cuando el tratamiento no respete la ley o lo acordado; derechos sustentados en los principios de transparencia y veracidad, y reglamentados en el decreto 1377, donde también figuran como procedimientos para el adecuado tratamiento de datos personales.

- **Observaciones a la norma**

No obstante, el statuquo de la protección de datos personales es más que la ley estatutaria y el decreto reglamentario, por tanto se presentan las siguientes observaciones. En primer lugar, la sentencia C748 que consiste en la exequibilidad de ley 1581 registra el salvamento de voto de algunos magistrados que cuestionan la definición de los actores, pues según los magistrados que disienten, se parte de un supuesto contraevidente, ya que los datos son más que acopiados y tratados (responsable y encargados), son también recopilados y usados (no existe figura legal para quienes realizan estas acciones). Cuya consecuencia consiste en que

la fuente (aplicaciones socias que recogen información para Facebook, por ejemplo) y los usuarios (campañas políticas, empresas) carecen de un catálogo propio de obligaciones jurídicas que puedan ser verificadas y exigibles judicialmente. Crítica con la que coincide Monsalve (2017) resaltando la importancia de los usuarios en el tratamiento de la información, quienes son terceros autorizados para consultarla, obsérvese que quienes pagan un tratamiento específico son los usuarios de la información y por tanto de ellos debería poder derivarse una responsabilidad ética y legal del uso y la creación de información personal construida a partir del análisis de datos.

En segundo lugar, la transferencia de la información se encuentra sujeta al principio de seguridad según la legislación vigente, frente al caso de CA la SIC representada por la Dirección de Investigación de Protección de Datos Personales de la misma entidad emite la resolución 1321 de 2019 donde desde un enfoque preventivo se busca el mejoramiento de las condiciones de seguridad de la plataforma.

Luego, aunque existe unos clasificación según el tipo de dato personal (público, privado o sensible), esta también convoca a la crítica hecha en el salvamento de voto de la sentencia C748, en donde se manifiesta "ausencia de una tipología que permita niveles diferenciados de protección", pues la calidad de datos personales que antes eran diferenciados en la jurisprudencia entre semiprivados, privados, es una pérdida de matices normativa sobre la intimidad (sentencias C748, Ley 1581).

Finalmente, la última observación crítica sobre la ley 1581 es la autoridad competente de su implementación, la Delegatura de Protección de Datos personales de la Superintendencia de Industria y Comercio, entidad creada para el exclusivo cumplimiento de la normativa, dígase según un funcionario de la Delegatura en entrevista, "para la investigación y sanción de casos específicos sobre la normativa".

Desde el salvamento de voto antes referenciado, hay "inexistencia de una autoridad de control pertinente" (Sentencia C748). Se cuestiona la independencia de la entidad dado los innumerables procesos de administración de datos personales que tienen lugar al interior de la rama ejecutiva, se alega entonces que esta constituye juez y parte sobre la vigencia de principios y facultades de los usuarios; además, teniendo en cuenta que los organismos de control son importantes actores en el tratamiento de datos (registros juridiciales,

investigaciones de fiscalía, contraloría, etc.), es preocupante que una entidad de la rama ejecutiva vigile desde el tratamiento de los datos a organismos de control. Crítica compartida con Sotelo (2012), quien acentúa en la improbable parcialidad teniendo en cuenta la cantidad de datos tratados por entidades estatales.

Sin embargo esto último es respondido en entrevista por el funcionario de la Delegatura (2019) que asegura, según la misma legislación 1581 y el decreto 1377, en caso de entidades públicas es la encargada de investigar y sancionar la Procuraduría General de la Nación.

Aún con esta corrección a la crítica, es preocupante la limitación que tiene la Delegatura frente a la evolución de los fenómenos relacionados con su campo, su mera función investigativa y sancionatoria sobre lo dado en la norma, hace imposible que se pronuncie sobre fenómenos que evolucionan como el profiling o el uso de técnicas muy específicas no contempladas por la legislación vigente, esto sin ahondar en la dependencia que tiene al ejecutivo, como no sucede con agencias análogas como la española de protección de datos, con funciones más amplias que se complementan sumadas a una independencia organizativa. En consecuencia, en Colombia los organismos con la facultad de investigar públicamente los fenómenos relacionados a la protección de datos personales y de proponer nuevos mecanismos y formas de protección al usuario son el Congreso de la República, el Gobierno Nacional a través de sus ministerios y la Corte Constitucional, los dos primeros actores políticos cuya voluntad depende de la agenda electoral y que no han demostrado hasta ahora interés en una estructura integral de protección de datos personales hacia el usuario más allá de las problemáticas de seguridad y del buen nombre, discusiones necesarias pero insuficientes para todo lo que implica el tratamiento de datos personales.

- **Observación en relación a Facebook**

En este apartado se cierra con los hallazgos de Facebook en el caso colombiano, su cumplimiento a la regulación nacional y su relación con otros actores.

En el tratamiento de datos de la RSV se objeta el cumplimiento del principio veracidad, pues para esto se requiere que sea posible ejercer los derechos del titular de conocer, corregir, actualizar o suprimir los datos personales en Facebook, es decir que sea el usuario quien determine la veracidad de la información, lo cual es posible solo parcialmente, cuando estos

sean publicados en un perfil, no obstante en el caso de los datos obtenidos a través del usuario más no explícitamente proporcionados por este, o los creados a partir del cruce de la información o perfilación, cuyo resultado son datos nunca explicitados por el usuario, sino construidos a partir del análisis de lo publicado e interactuado en la red, estos datos no se pueden conocer. No es posible conocer el perfil que de una persona ha construido Facebook, y por tanto es imposible corregir, actualizar o suprimirlos, datos que efectivamente conciernen al usuario pues refieren a su conducta o identidad, este es un procedimiento de exclusivo conocimiento de Facebook y cuyos resultados son compartidos a modo de observaciones con terceros usuarios de la información.

Luego, el cumplimiento de la autorización previa, expresa e informada frente al tratamiento de datos personales, en primera medida la extensa amplitud del contrato sobre el tratamiento de datos personales y la falta de explicitud sobre los datos tratados que también son sensibles dificultan que el usuario efectivamente se informe acerca del tratamiento previamente. Además, Facebook no cumple con la explicitud a ciencia cierta, por ejemplo no se conoce en qué consiste la perfilación en su plataforma, cuáles son los datos creados o fabricados. Por último, la autorización sobre datos sensibles no debe estar mediada por la adquisición de un bien o servicio, y el ciudadano debe poder no aceptar su tratamiento según la ley 1581 que reza:

> **Artículo 6.** 1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
>
> 2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.
>
> Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.

Sin embargo, la Delegatura de protección de datos personales de la SIC ya se ha pronunciado sobre el funcionamiento de Facebook. Este ha sido un acercamiento insuficiente por sus dos enfoques, uno preventivo y otro de seguridad, presentados por un funcionario de la Delegatura en entrevista.

Del primero debe decirse que es reprochable frente al grave caso que fue CA, Facebook le informa a la Dirección de la Delegatura de 146.697 casos de usuarios en Colombia afectados por la falla de seguridad, según la resolución 1321 de 2019, y la respuesta a diferencia de otros países no fue la exposición de los efectos puntuales de esta falla ni tampoco la sanción por ellos, sino optar por ordenar con un plazo de vencimiento acciones para la prevención de casos similares, esto es claramente insuficiente para sentar precedente sobre la autoridad de la institucionalidad colombiana para proteger a sus ciudadanos, pues no se busca corregir sobre los daños realizados ni tampoco conocer o descartar los perjuicios y afectaciones concretas sobre los usuarios, más allá de la cifra dada.

El enfoque de seguridad es claramente insuficiente porque asume que el único peligro en el tratamiento de datos personales es proveniente de los usuarios de la información, de su uso por externos, mas no se analiza los peligros del mismo tratamiento para la intimidad e integridad del ciudadano desde el responsable que es quien diseña el procedimiento hasta su uso. Es decir, todas las observaciones sobre la autorización, el principio de veracidad, las consecuencias de la perfilación para la conducta y el desarrollo del individuo, además de la ausencia de mecanismos para que el usuario interpele el contrato por adhesión que es el tratamiento de datos personales no busca mitigar las arbitrariedades entre el ciudadano que es usuario y la RSV, sino frente a otras plataformas, ramificando las responsabilidades en casos específicos mas no desde la estructura responsable que posibilita esas fallas por unas facultades desproporcionada sobre el usuario.

CONCLUSIONES

La falta de enfoques integrales que hagan cumplir lo establecido en la ley 1581 especialmente en RSV como Facebook, de la cual se demuestra su capacidad de fallar sistemáticamente, se concibe como una omisión del Estado colombiano, visible desde la misma agenda pública donde no se encuentra lo enunciado como problemático y no es objeto de discusión. El Estado es una estructura institucional que existe en tanto regula e interviene las actividades y relaciones de las personas, específicamente en el caso colombiano cuando se ha mostrado de manera sobre evidente la incumbencia del Estado en la protección de los datos personales en función de la de la protección a la intimidad, recuérdese todo el avance jurídico respecto a la regulación.

Visible es entonces la omisión parcial del Estado colombiano con su tenue enfoque preventivo cuando se requiere una regulación especializada en internet para la protección de datos personales en función de la intimidad, más allá de la seguridad. Se concluye que obedece a una ramificación o tercerización de las responsabilidades sobre el tratamiento de datos, pues el enfoque de seguridad asume que los peligros es por el acceso de terceros a la información mas no por las mismas facultades del responsable, Facebook. Esta usual ramificación conlleva a que la seguridad sea un enfoque sobre terceros al igual que la intimidad, en Colombia las discusiones se concentran en el respeto al honor y buen nombre, vulnerados por otros usuarios en la red social virtual, nuevamente reduciendo a terceros todo el espectro del fenómeno. Esta forma de establecimiento encuentra al responsable del tratamiento como capaz de resolver todas las problemáticas alrededor y permisivamente delega la obligación de protección a los mismos actores privados del mercado que son las redes sociales virtuales, que como Facebook han cometido constantes y graves errores en el tratamiento.

Es fundamental resaltar que si no es el Estado el que proporciona mecanismos para la garantía de la intimidad del ciudadano y otros derechos que están en vilo en internet, nadie tiene la obligación de hacerlo. La relación red social virtual- usuario es lo suficientemente desproporcionada como para que los ciudadanos no sean libres en internet, y no puedan formarse allí para ser críticos con sus democracias, el control sobre la conducta del sujeto está por mucho, en el caso colombiano, en manos de un mercado monopolizado y altamente poderoso tecnológicamente, la falta de una postura integral y completa para la protección es el abandono de esta obligación.

Por último, luego de esta investigación queda un amplio panorama para ser investigado. Incluso cuando la RSV cumpla con todos los requerimiento legales, qué tan libres o influenciados son los usuarios para el ejercicio de la ciudadanía en línea. También, cuáles son los efectos de técnicas como perfilación sobre la democracia y sus eventos electorales, inclusive los cambios en el marketing electoral que tiene la perfilación. Las afectaciones que tienen sobre el mercado una regulación más estricta y, cómo solventarlas para incentivar la investigación tecnológica. Desde el sujeto es importante analizar las afectaciones en la configuración de la identidad cuando existe y no regulación del tratamiento de datos

personales. Además si encuentra que el Estado en su poder político atrapa otros poderes, qué tanto puede atrapar a un poder tan amplio y bien construido sobre la información de los usuarios como son estas plataformas de internet entre las que se encuentran las RSV.

BIBLIOGRAFÍA

Celis, M. (2006). La protección de la intimidad de como derecho fundamental de los mexicanos. En *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales* (71-108). México: Universidad Nacional Autónoma de México.

Corte Constitucional de Colombia. (1992).Sentencia T-414/92. (Magistrado ponente Ciro Angarita Barón)

Corte constitucional (2011). Sentencia C-748/11. (Magistrado Ponente Jorge Ignacio Pretelt Chaljub; 6 de octubre de 2011).

Decreto 1377 de 2012. Ministerio de Comercio, Industria y Turismo. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. 27 de junio de 2013.

Guerrero, O. (2011). La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal. *Revista Derecho Penal y Criminología*, 32(92), pp. 55-84.

Facebook. Política de datos. En esta Política, se describe la información que tratamos para respaldar a Facebook, Instagram y Messenger, así como otros productos y funciones que ofrece Facebook (Productos de Facebook o Productos). Recuperado de https://web.facebook.com/about/privacy/update. Visitado por última vez el 20 de febrero de 2018.

Kosinski, M., Stillwell, D., y Graepel, T., (2013). Private traits and attributes are predictable from digital records of human behavior. *PNAS*, 110(15), 5802-5805.

Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera,

crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. 31 de diciembre de 2008

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012.

Macavilca, Z. (2017). El derecho a la intimidad en el contexto de las nuevas tecnologías de comunicación e información. En *El derecho a la intimidad: Nuevos y viejos debates* (181-192). Madrid: Dykinson.

Magnani, E. (2017). Big data y política. El poder de los algoritmos. *Nueva Sociedad* (269), pp. 45-55.

Mann, M. (1991). El poder autónomo del Estado: sus orígenes, mecanismos y resultados. *Zona Abierta,* (57-58), pp. 15-50.

Márquez, F. (2016). *Grandes pensadores de la Globalización*. México: Universidad Nacional Autónoma de México.

Márquez, F. (2015). Aplicación de la Ley Estatutaria 1581 de 2012 a la red social Facebook en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* (15), p. 1-31.

Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referente europeos. *Revista Prolegómenos Derechos y Valores,* 20(39), pp. 163-195.

Pfeiffer, M. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética,* 3(1), pp. 11-36.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Saltor, C. (2013). *La protección de datos personales: estudio comparativo europa-américa con especial análisis de la situación argentina* (Tesis doctoral, Universidad Complutense de Madrid). Recuperado de: https://eprints.ucm.es/22832/.

Sánchez, A. (2016). *La protección de la intimidad y vida privada en internet: la integralidad contextual y los flujos de información en las redes sociales (2004-2014)*. Madrid: Agencia española de protección de datos.

Sotelo, D. (2012). El habeas data en las redes sociales online: responsabilidad y vigilancia. *Revista Iter ad veritatem*, (10), 231-250.

Superintendencia de Industria y Comercio. (2019). Resolución 1321.

Superintendencia de Industria y Comercio. (8 junio, 2017). Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos. [Entrada informativa]. Recuperado de http://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos

Yepes, R. (1997). *La persona y su intimidad*. Servicio de Publicaciones de la Universidad de Navarra

Facebook: Una política de datos que gobierna la intimidad. Estudio del caso colombiano

Anexo: Rastreo Periodístico a Cambridge Analytica

Fecha	Publicado por	Redactado por	Título	Link	Tipo de publicación
11.12.2015	The Guardian	Harry Davis	Ted Cruz using firm that harvested data on millions of unwitting Facebook users	https://bit.ly/2lHR0Ac	Rastreo y seguimiento periodístico en medios internacionales y nacionales del caso
15.12.2015	The New York Times	Emma Roller	Is It Ted Cruz's Party — Or Marco Rubio's?	https://nyti.ms/2GAiqCU	
15.12.2015	The Atlantic	Sasso and National Journal	Political Campaigns Are Spying on You, and There Are No Rules to Stop Them	https://bit.ly/2GxsqwK	
05.11.2016	CNN	Isa Soares	Analistas psicológicos: el arma secreta de Donald Trump para que votes por él.	https://cnn.it/2GISiHk	
23.11.2016	The Guardian	Peter Stone	Data firm in talks for role in White House messaging – and Trump business	https://bit.ly/2fS5BI7	
8.12.2016	RT	Peter Stone	Revelan cómo el Big Data y unos científicos hicieron a Trump presidente	https://bit.ly/2z6Zru0	
04.03.2017	The Guardian	Doward and Gibbs	Did Cambridge Analytica influence the Brexit vote and the US election?	https://bit.ly/2mKmSY7	
06.03.2017	The New York Times	Confessore and Hakim	Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff	https://nyti.ms/2mdl3l2	
12.04.2017	Vice	José Luis Martínez Limón	Así es como tus datos digitales podrían decidir las próximas elecciones en México	https://bit.ly/2KZPZ6B	
03.07.2017	CNN	Sam Bright	After Trump, "big data" firm Cambridge Analytica is now working in Kenya.	https://bbc.in/2IWepv9	
26.10.2017	The Guardian	Kirchgaessner	Cambridge Analytica used data from Facebook and Politico to help Trump	https://bit.ly/2iDmKsG	
27.10.2017	CNN	Marshall Cohen	Trump. Cambridge Analytica. WikiLeaks. The connections, explained	https://cnn.it/2VqsR5m	
22.11.2017	Arcadia	Dominique Lemoine Ulloa y Santiago Parga Linares	De 'like' en 'like': el 'big data' en la política colombiana las-elecciones/66820	https://bit.ly/2IVHxTq	

15.12.2017	Revista Semana Sostenible	-	¿Sirve para algo la movilización a través de redes sociales?	https://bit.ly/2ZBhFCg	
17.01.2018	El Espectador	AFP	Los Mercer, los millonarios que sostienen a la derecha en EE.UU.	https://bit.ly/2IXOAuW	
15.02.2018	Umoya ORG	-	Datos y democracia: ¿qué papel desempeñó Cambridge Analytica en las elecciones de Kenia?	https://bit.ly/2L5qwcf	
17.03.2018	The Guardian	Cadwalladr and Graham-Harrison	Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach	https://bit.ly/2plU1sM	Revelación del escándalo
17.03.2018	The New York Times	Rosenberg, Confessore and Cadwallar	How Trump Consultants Exploited the Facebook Data of Millions	https://nyti.ms/2HH74vA	
19.03.2018	La FM	-	Así operaba Cambridge Analytica, la firma aspiradora de datos y estrategia política	https://bit.ly/2GHJK3j	Reproducción en medios nacionales del escándalo
19.03.2018	Portafolio	Efe	Acción de Facebook se hunde en Wall Street	https://bit.ly/2PvLorr	
20.03.2018	Semana	BBC	5 claves para entender el escándalo de Cambridge Analytica y Facebook.	https://bit.ly/2VoEUjt	
20.03.2018	El Espectador	-	Lo que tiene que entender sobre el escándalo de Facebook	https://bit.ly/2UWmyaf	
20.03.2018	La República	González	Cambridge Analytica señaló que además de Estados Unidos operaba en Colombia	https://bit.ly/2pog5SS	
20.03.2018	Canal RCN	-	Escándalo de uso indebido de datos sacude a Facebook	https://bit.ly/2viP1b9	
20.03.2018	RCN Radio	-	La cuestionada empresa Cambridge Analytica, sí operó en Colombia	https://bit.ly/2PwcEpH	
20.03.2018	El Tiempo	Unidad Investigativa	El rastro de la atrapadatos Cambridge Analytica en Colombia	https://bit.ly/2vntHBj	
20.03.2018	Noticias Caracol	AFP Agencia	Parlamento británico convoca a Mark Zuckerberg para hablar del escándalo de Cambridge Analytica	https://bit.ly/2XKsMai	
21.03.2018	Caracol Radio	-	Facebook asegura que fue engañada tras escándalo de filtración de datos	https://bit.ly/2VmK6EL	
21.03.2018	Portafolio	-	Mark Zuckerberg rompe silencio frente a escándalo de Cambridge Analytica	https://bit.ly/2L3r42e	
21.03.2018	El Heraldo	AFP Agencia	Psicólogo que desarrolló app de Cambridge Analytica dice que era legal	https://bit.ly/2ZBsR1x	

23.03.2018	Portafolio	John Gapper	La firma Cambridge Analytica explotó escandalosamente datos de Facebook	https://bit.ly/2L3kWXy	
23.03.2018	Portafolio	John Thornhill	Los políticos y usuarios deben actuar para salvar Internet	https://bit.ly/2XMy4SB	
26.03.2018	Caracol Radio	EFE	Autoridades de EE.UU. confirman que investigan a Facebook por filtración	https://bit.ly/2GGtRtT	
27.03.2018	Caracol Radio	EFE	El cerebro de Cambridge Analytica asegura que usaron los datos de Facebook	https://bit.ly/2Pzjz1G	
28.03.2018	CNN		Escándalo de Cambridge Analytica alcanza a Colombia: ¿por qué bloquearon la 'app' Pig.gi?	https://cnn.it/2UToYXf	
28.03.2018	Caracol Radio	Reuters	Facebook dará a sus usuarios más control sobre su información personal	https://bit.ly/2ZzQ4RN	
29.03.2018	Portafolio		Pig.gi niega haber compartido datos de colombianos con Cambridge Analytica	https://bit.ly/2Vp0Efm	
11.04.2018	Zonacero	EFE	Facebook recompensará pistas sobre "abuso de datos" de aplicaciones en su red.	https://bit.ly/2UzZ0CZ	
04.04.2019	Universidad Nacional		Efecto Cambridge Analytica afectaría intención de voto en Colombia	https://bit.ly/2LcHoNY	