CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C.

IMPLICACIONES DEL *MICROTARGETING* POLÍTICO DE FACEBOOK EN LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES DE LOS USUARIOS: ANÁLISIS EN ESTADOS UNIDOS DE AMÉRICA Y MÉXICO

TESINA

QUE PARA OBTENER EL TITULO DE

LICENCIADA EN DERECHO

PRESENTA

VICTORIA VALENTINA SMITH NIEVES

DIRECTORA DE LA TESINA: DRA. MARÍA MERCEDES ALBORNOZ

CIUDAD DE MÉXICO 2020

AGRADECIMIENTOS

A mi familia, ustedes son lo más importante y valioso en mi vida. A mi mamá, porque fuiste quien construyó para nosotros, un hogar, con todo el trabajo que ello implica, siempre pusiste nuestro bienestar y cuidado por encima de todo, nunca voy a poder agradecerte lo suficiente. A mi papá, porque has sido el mejor profesor que he tenido, desde los juegos de matemáticas de pequeña o, explicarme economía, hasta enseñarme la importancia de la humildad y la bondad, agradezco inmensamente poder tenerte a mi lado en el cierre de esta etapa. Les amo a los dos, esta tesina y mi carrera en el CIDE es tanto un logro mío como es de ustedes.

A mis hermanxs. A Carolina, porque no sólo has sido mi hermana, has sido mi mejor amiga, mi única amiga en algunos momentos, siempre has sido y serás mi compañera de vida. A Ricardo, por ser un ejemplo a seguir, y por siempre preocuparte por mí y cuidarme, especialmente el último año, no pude tener un mejor hermano mayor. Les amo.

A mi mejor amiga, Valeria, porque has estado a mi lado en los momentos más importantes y en los más difíciles, eres la mejor persona que he tenido la oportunidad de conocer y me inspiras a ser mejor persona cada día. Tu amistad ha sido como una isla en medio de un océano tormentoso, un pequeño lugar seguro

ante cualquier evento desafortunado. También a Paola, por todas esas noches largas de estudio, por recordarme mis capacidades cuando a mí se me olvida cómo verlas, y porque los últimos años han sido complejos y llenos de obstáculos, y cuando sentía que estaba a punto de caer has estado ahí para ayudar a sostenerme, no puedo imaginar mi carrera en el CIDE sin tu amistad.

A mis compañeros de generación, estoy muy agradecida de haber compartido mi carrera con ustedes, un grupo en el que predominó el apoyo, la comprensión y el compañerismo. Significó mucho para mi encontrar en ustedes un lugar de acompañamiento, convivencia y amistad, cosas que considero fueron cruciales para sobrellevar cuatro años tan demandantes. Conocer personas brillantes y comprometidas con contribuir para construir una mejor sociedad es lo más valioso que me llevo del CIDE.

Agradezco a mis profesorxs por todo el conocimiento transmitido. Agradezco a la Dra Lucero Ibarra por ser un excelente ejemplo de una profesora que brinda apoyo a todxs sus alumnxs por igual. Su comprensión y apoyo en los últimos semestres de mi carrera fueron muy importantes para mí.

Finalmente, a mi directora, la Dra. María Mercedes Albornoz por su guía y acompañamiento en esta tesina. Le agradezco

mucho a usted y al Dr. Gustavo Fondevila por su apoyo y comprensión en este proceso de conclusión de la carrera.

Introducción

En la actualidad, el internet es una parte importante para el funcionamiento de una sociedad globalizada. Millones de personas de diversas partes del mundo son usuarias de plataformas digitales. Estas plataformas tienen una variedad de funciones para las personas, como compras en línea, herramientas de búsqueda o redes sociales como Facebook o Twitter. Con la presencia de este tipo de plataformas, sus usuarios se encuentran con riesgos que no existían previamente.

El avance en las tecnologías de información y comunicación, y la globalización, han conformado una sociedad en la que las plataformas de redes sociales tienen un lugar importante en la interacción social y la vida cotidiana. Para una significativa porción de la población mundial, Facebook, Instagram y WhatsApp, forman parte del día a día. Los usuarios disfrutan de tener un espacio para comunicarse, compartir opiniones o imágenes con otros usuarios, de forma gratuita y sencilla.

El éxito de las plataformas de redes sociales tiene como factor dependiente la cantidad de usuarios, ya que entre más grande sea la red de usuarios que se ofrezca, más atractivo será para

nuevos usuarios unirse.[1] Para el campo de la publicidad y promoción de otros bienes y servicios, el éxito de las plataformas de redes sociales significó un espacio con cada vez más personas participando activamente. De esta forma, las redes sociales encontraron su actividad comercial en la publicidad.

Facebook fue una de las primeras redes sociales en tener éxito en este ámbito. Creada en el 2004 por Mark Zuckerberg, en el 2020 cuenta con 1.800 millones de usuarios activos y es propietaria de otras dos de las redes sociales con mayor número de usuarios en el mundo: Instagram y WhatsApp.[2] En el período de abril-junio del 2020 Facebook obtuvo 18.321 millones de dólares de ingresos por publicidad.[3] Así, hoy en día los usuarios de Facebook u otras de las redes que son parte de la empresa, no son ajenos a la presencia de publicidad de bienes y servicios.

Los bienes y servicios que contratan publicidad en redes sociales son muy variados y, sin embargo, los últimos años, los

[1] ACC. Digital Platforms Inquiry: Final Report. Junio 2019.
[2] Juan Mejía, "Estadísticas de redes sociales 2020: usuarios de facebook, instagram, youtube, linkedin, twitter, tiktok y otros", Marketing digital y transformación digital, 26 de febrero de 2020. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/
[3] Expansión. 2020. "Facebook aumenta sus ingresos un 11% en el segundo trimestre", 30 de julio.

usuarios han notado cómo la publicidad que aparece en sus cuentas se ha vuelto más personal. Preocupaciones sobre cómo, un día después de que se tuvo una conversación con amigos sobre comprar una guitarra, aparece publicidad de guitarras en Facebook. Incluso, teorías sobre cómo las compañías de redes sociales monitorean a sus usuarios por medio de las cámaras o audios de sus dispositivos tomaron popularidad.

El avance y la creciente efectividad de la especialización y adecuación de la publicidad digital a las preferencias de cada usuario se pueden adjudicar, en gran parte, al acceso que tienen las redes sociales a la información personal de millones de personas. Facebook, la red social con mayor número de usuarios activos puede considerarse como una de las bases de datos personales más grandes del mundo. Así, la dominancia de Facebook en el mercado de publicidad digital se debe a la posibilidad y efectividad de una actividad conocida como *microtargeting*.[4]

El *microtargeting* es una técnica publicitaria que implica encontrar, analizar y procesar información sobre las preferencias de los individuos, así como sus hábitos de consumo. El propósito es que, con la información obtenida, los

[4] ACC. Digital Platforms Inquiry: Final Report. Junio 2019.

individuos puedan ser segmentados y puedan recibir mensajes especialmente diseñados de acuerdo con su perfil, preferencias, situación económica e, incluso, su personalidad. La ventaja competitiva de las redes sociales para los anunciantes es, entonces, la información personal de sus usuarios.

En consecuencia, el fenómeno del *microtargeting* como medio de publicidad digital en redes sociales como Facebook tiene implicaciones importantes en la protección de la privacidad y los datos personales de los individuos. La discusión de las implicaciones jurídicas de la publicidad digital tiene distintas aproximaciones, entre las cuales se encuentra el enfoque en publicidad digital política.

El debate sobre los efectos y posibles riesgos de la publicidad digital política tuvo un auge en 2018, después de que se hiciera público que la firma Cambridge Analytica había utilizado información personal de usuarios de Facebook, sin conocimiento de ellos, para segmentar y personalizar publicidad de ciertos partidos y campañas, como las de Trump y el Brexit, ambas en 2016. A raíz del caso de Cambridge Analytica, fueron expuestas potenciales vulneraciones y los riesgos que el *microtargeting* político puede representar no sólo para la privacidad de los individuos, sino también para funcionamiento de una sociedad democrática.

A partir de lo sucedido en 2018 y en atención a las próximas elecciones presidenciales, en Estados Unidos, se desarrolla una discusión sobre la necesidad de regular la actividad de Facebook con respecto a su servicio de publicidad digital política. Sin embargo, no hay un consenso en cuanto a cómo y desde qué perspectiva se debe dar dicha regulación.

La presente tesina afirma que es necesario adaptar la legislación, de forma que se regule el *microtargeting* político que efectúa Facebook, ya que este representa una vulneración al derecho a la privacidad. Así, se analizarán las herramientas legales vigentes en Estados Unidos (California) y México y explicará por qué estas no han sido efectivas para garantizar la privacidad de los usuarios de redes sociales frente al *microtargeting* político. Asimismo, esta tesina sostiene que, para prevenir o disminuir los riegos que el *microtargeting* político representa en distintos ámbitos, primero debe ser regulado en materia de protección de datos personales. Para este propósito, la tesina estará dividida en cuatro capítulos. El primero tendrá como objeto explicar la materia de privacidad y datos personales en Estados Unidos y en México, sus conceptos principales, así como también explorar lo que significa el microtargeting político en redes sociales. El segundo capítulo se dedicará a la explicación y análisis de la nueva legislación de California de privacidad de los

consumidores. El tercero por su parte será para analizar el marco normativo mexicano en materia de datos personales y su aplicación a plataformas como Facebook. Finalmente en el cuarto capítulo se analizará el tema de la necesidad de regulación especial para Facebook y para el microtargeting en concreto.

Capítulo I: Derecho a la protección de datos personales, redes sociales y *microtargeting* político

Este primer capítulo tiene como objetivo explicar los principales elementos conceptuales que serán abordados en el presente trabajo. En primer lugar, será expuesto el marco conceptual especializado en materia de protección de datos personales: A) Los conceptos de datos personales y privacidad; B) Los sujetos; C) El tratamiento y la transferencia de datos personales; D) Los principios más relevantes. Posteriormente, se explicará el concepto de red social y su importancia. Finalmente, en este capítulo se explicará el *microtargeting* político, los principales conceptos en este tema, su relevancia, el papel de Facebook en esta actividad y el caso de Cambridge Analytica.

1. El derecho a la protección de datos personales

A. Concepto de datos personales y de privacidad

Los conceptos de derecho a la privacidad y derechos de protección de datos personales tienen similitudes en el objeto de su protección. La privacidad y la protección de datos personales son conceptos ampliamente relacionados. Sin embargo, tienen diferencias que impiden poder considerarlos como el mismo derecho. Algunos autores argumentan que los derechos de protección de datos personales son una subespecie del derecho de privacidad. De tal forma, que es necesario

plantear las diferencias entre ambos para poder entender el concepto de cada uno de estos derechos. Es importante destacar que la conceptualización, tanto del derecho a la privacidad como de la protección de datos personales, puede variar, puesto que depende de la interpretación legislativa y judicial que le den los distintos Estados.

En Estados Unidos, la primera referencia a un derecho de privacidad fue hecha en 1879 por el juez Thomas Cooley, quien se refirió al "derecho a ser dejado en paz" como una materia de seguridad personal.[5] El término de derecho a ser dejado en paz fue utilizado posteriormente en un artículo publicado por Samuel Warren y Louis Brandeis en 1890.[6] En este artículo, los autores toman en consideración el fenómenos de publicaciones y fotografías en revistas y periódicos como un ejemplo de que el derecho tiene que adaptarse a nuevas invenciones y los avances que tiene la sociedad para poder realmente proteger al individuo.[7] Este artículo constituyó una

[5] Reilly, Robert, "Conceptual foundations of privacy: Looking Backward Before Stepping Forward", *The Richmond Journal of Law and Technology* vol 6., 2da ed (1999). https://core.ac.uk/download/pdf/232774445.pdf
[6] Samuel Warren y Louis Brandeis, The Right to Privacy, *Harvard Law Review*, vol IV (1890), 193-220.
[7] Samuel Warren y Louis Brandeis, The Right to Privacy, *Harvard Law Review*, vol IV (1890), 193-220.

contribución significativa al desarrollo del derecho a la privacidad en Estados Unidos.[8]

El derecho a la privacidad fue reconocido como constitucional en el caso *Griswold vs Connecticut*, resuelto en 1965 por la Suprema Corte de Estados Unidos.[9]En este caso se estableció que el derecho a la privacidad deriva de las siguientes enmiendas: *Primera enmienda* sobre la libertad de expresión, *Tercera enmienda* sobre la prohibición a los soldados de irrumpir en una casa en tiempos de paz sin consentimiento del propietario, *Quinta enmienda*, *Novena Enmienda* y *Décimo cuarta Enmienda.*[10]

En Estados Unidos, la protección de datos personales no es reconocida como un derecho separado del derecho a la privacidad. Las actas emitidas en cada estado con respecto al manejo de datos personales se encuentran bajo la denominación de "actas de privacidad del consumidor".

---

[8] Colin Bennett, ***Regulating privacy: data protection and public policy in Europe and the United States***, (Cornell University Press, 1992), 68-69.
[9] U.S. Supreme Court. *Griswold vs Connecticut*, 381 US 479 (1965).
[10] En este caso Estelle Griswold, la directora ejecutiva de Planned Parenthood Conneticut y Dr Lee Buxton fueron declarados culpables de proporcionar anticonceptivos ilegales. Griswold y Buxton apelan ante la Corte Suprema que la ley de Connecticut viola la Constitución de los Estados Unidos por su décimo cuarta enmienda. La Corte Suprema, en una decisión 7-2 escrita por el juez William O. Douglas, dictaminó que la ley violaba el derecho a la privacidad conyugal. **U.S. Supreme Court.** *Griswold vs Connecticut*, 381 US 479 (1965).

El derecho de protección de datos personales como un derecho individual, surgió en Alemania en 1983. El Tribunal constitucional de este país estableció que: "el libre desarrollo de la personalidad presupone la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales".[11]

En México, el derecho a la privacidad está contemplado en el artículo 16 Constitucional. Esto fue establecido por la Suprema Corte de Justicia de la Nación (SCJN) en el amparo en revisión 134/2008 en el que afirma que este derecho está implícito en el artículo 16 constitucional.[12] En esta resolución la SCJN define al derecho de privacidad como:

> La garantía de seguridad jurídica a no ser molestado en su persona, familia, papeles o posesiones, si no en virtud de mandamiento escrito. (…) un reconocimiento del derecho a la persona que tiene su idea originaria en el respeto a la vida privada. Incluye todas las

[11] Diego García Ricci, "Artículo 16 constitucional. Derecho a la privacidad" Instituto de Investigaciones Jurídicas UNAM, 2013. (Fecha de consulta: 5 de diciembre del 2019)

[12] Amparo en revisión 134/2008. Sentencia del 30 de abril del 2008. México.

> intromisiones y molestias que por cualquier medio puedan realizarse en el ámbito de la vida privada.[13]

El reconocimiento constitucional del derecho de protección de datos personales en México es relativamente reciente. Fue desarrollado con base en los postulados de la doctrina europea y los esquemas de autorregulación y sectorización del sistema anglosajón.[14] Tuvo lugar en 2009, cuando se reformó el artículo 16 constitucional y se introdujo el derecho a la protección de datos personales.[15] Asimismo, este derecho había sido incorporado en la Ley Federal de Acceso a la

[13] Amparo en revisión 134/2008. Sentencia del 30 de abril del 2008. México.

[14] Olivia Mendoza, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Scielo, junio 2016, scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267 (Fecha de consulta: 4 de diciembre del 2019).

[15] El 1 de junio de 2009, se publicó en el DOF el Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, a efecto de incluir el derecho a la protección de datos personales, consiste en garantizar los derechos de acceso, rectificación, cancelación y oposición a los titulares de los datos personales, en los términos que fije la ley, la cual establecerá los principios que rijan el tratamiento de los datos, así como los supuestos de excepción a dichos principios, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger derechos de terceros.https://www.dof.gob.mx/nota_detalle.php?codigo=5484681&fecha=30/05/2017

Información Pública Gubernamental de 2002, abrogada en 2006.[16]

Posteriormente, en el 2010 entró en vigor la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, LFPDPPP).[17] Esta ley define "dato personal" como cualquier información concerniente a una persona física identificada o identificable (artículo 3). Posteriormente, en 2017 fue publicada en el diario oficial de la federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sin embargo, debido a que esta ley no es aplicable para entidades privadas, la presente tesina no se enfocará en el contenido de esta ley.[18]

En este apartado fueron planteados los orígenes y fundamentos del derecho privacidad y del derecho protección de datos personales en la Unión Europea, Estados Unidos y México. Es entonces relevante, para identificar los conceptos de

[16] Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública. DOF 09-05-2016

[17] *Ley Federal de protección de datos personales en posesión de particulares*, Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010.

[18] *Ley General de protección de datos personales en posesión de sujetos obligados*. Cámara de Diputados H. Congreso de la Unión. DOF 26-01-2017.

privacidad y protección de datos, destacar el aspecto en común entre estas tres regiones y los aspectos que los diferencian.

Es posible afirmar que, en las tres legislaciones mencionadas, el concepto de privacidad es, en general, más amplio que el de protección de datos. La privacidad puede referirse a aspectos de espacios físicos, a privacidad informacional, privacidad en la propiedad privada, entre otros. Es en la parte informacional en la que la privacidad coincide con la protección de datos personales. La protección de datos se encarga de salvaguardar todos los aspectos de la vida que pueden ser reducidos a términos informacionales. Sin embargo, en todas las legislaciones analizadas el derecho de privacidad es usado para proteger al individuo de interferencias a su vida privada. En cambio, en la protección de datos personales no es necesaria una interferencia como tal.

La diferencia principal entre Estados Unidos y la Unión Europea y México, es que en el primero el derecho de protección de datos personales no está explícitamente considerado como derecho. La regulación sobre protección de datos personales se encuentra dentro de lo establecido sobre derechos de privacidad. Por tanto, en Estados Unidos podría afirmarse que la protección de datos personales es una subespecie del derecho a la privacidad, aunque, doctrinalmente, los conceptos sean distinguibles. En cambio,

tanto en la Unión Europea como en México, el derecho a la privacidad y el derecho a la protección de datos personales son derechos individuales distintos que, en ocasiones, tienen el mismo objeto de protección.

B. Sujetos: el responsable del tratamiento

En el Reglamento General de la Protección de Datos de la Unión Europea (en adelante GDPR), fue hecho en 2016 y entró en vigor en mayo del 2018.[19] En este se define al responsable del tratamiento (*controller*) como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento."[20]

En el caso de México, en la LFPDPPP, el artículo 1º establece que son responsables del tratamiento los particulares que sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales. El mencionado artículo expone dos excepciones: las sociedades de información crediticia en los supuestos de la *Ley para regular las Sociedades de Información Crediticia* y los particulares que almacenen datos para uso personal sin fines comerciales.[21]

Es importante plantear la distinción entre responsable y el encargado del tratamiento. El responsable decide sobre el manejo de los datos personales, establece las finalidades del

[19] *Reglamento General de Protección de Datos Personales*. Consejo de la Unión Europea. Directiva 95/46/EC.
[20] *Reglamento General de Protección de Datos Personales.* Consejo de la Unión Europea. Directiva 95/46/EC. Artículo 4 (7).
[21] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 1.

tratamiento o el uso que se le dará a los datos personales, entre otras cosas. Mientras que el encargado es la persona física o moral, ajena a la organización del responsable, que trata los datos personales a nombre y por cuenta del responsable.[22]

C. El tratamiento y la transferencia de datos personales

La LFPDPPP define el tratamiento como "la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales."[23] Posteriormente define a la transferencia como "la comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento."[24]

Es necesario destacar el concepto de tratamiento intensivo. La Ley Federal, en el artículo 3º, establece que el tratamiento intensivo se presenta en tres situaciones: 1) cuando existen riesgos inherentes a los datos, 2) cuando sean datos personales

[22] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 1.
[23] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 3.
[24] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 3.

sensibles, y 3) cuando se efectúen transferencias de datos personales.[25]

> Los riesgos inherentes a los datos a tratar se entienden como: el valor potencial cuantitativo o cualitativo que pudieran tener estos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares involucrados; el volumen personal de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.[26]

Por otro lado, los datos personales sensibles son definidos como aquellos que se refieren a la esfera íntima del individuo o puedan dar lugar a cierto tipo de discriminación, por ejemplo, origen étnico, preferencia sexual, opiniones políticas, entre otros.[27]

---

[25] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 75.

[26] *Lineamientos Generales de Protección de Datos Personales para el Sector Público.* INAI. ACT -PUB/19/12/2017.10.

[27] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 3, fracción VI.

El concepto de tratamiento intensivo es relevante debido a que sería aplicable a las transferencias realizadas entre Facebook y entes interesados en utilizar los datos obtenidos para el *microtargeting* político.

2. *Redes Sociales*

A) Concepto e importancia

En primer lugar, es relevante distinguir dos percepciones que pueden derivarse de la denominación de "red social". Una red social puede conceptualizarse de forma sociológica, como una "serie compleja de interrelaciones dentro de un sistema social."[28] Dicha percepción no será el enfoque de este texto. La segunda percepción, útil para el tema que se está tratando en la presente tesina, es la de red social virtual.

Entonces, una red social virtual puede definirse como una herramienta digital, que facilita la construcción de un perfil público o semipúblico a una persona dentro de un sistema delimitado. El objeto de una red social es que la persona pueda construir una conexión con otros usuarios con los que

[28] Félix Requena, El concepto de red social, **Revista española de investigaciones sociológicas,** nº 48, pg 137-152.

comparta aspectos en común, así como también poder observar conexiones externas entre otros usuarios.[29]

B) Facebook y su papel en materia de datos personales

Facebook ha sido la red social con mayor relevancia desde su creación en 2004. A pesar del incremento en la relevancia de otras redes sociales como Tik Tok o Twitter, en el 2020 Facebook se posiciona como la red social más utilizada a nivel mundial, con WhatsApp e Instagram, de la que también es propietario, en tercer y sexto lugar respectivamente.[30]

La plataforma ha evolucionado con los nuevos avances tecnológicos. Entre los desarrollos más importantes de Facebook, se encuentran los algoritmos que utilizados para el manejo de la información de los perfiles de sus usuarios. El algoritmo actual es un algoritmo complejo que permite fácilmente la organización y aparición de publicaciones en el

[29] Boyd, d. m., & Ellison, N. B, Social network sites: Definition, history, and scholarship, ***Journal of Computer-Mediated Communication***, article 11 (2007).

[30] Juan Mejía, "Estadísticas de redes sociales 2020: usuarios de facebook, instagram, youtube, linkedin, twitter, tiktok y otros", Marketing digital y transformación digital, 26 de febrero de 2020. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/

news feed de forma personalizada, utilizando los datos de sus perfiles, previos me gusta, lista de amigos, entre otros datos.

Con sus millones de usuarios, Facebook puede ser una de las bases de datos más grandes en el mundo. Por consiguiente, Facebook también puede considerarse como uno de los mayores factores de riesgo para la protección de los datos personales. Sin embargo, la regulación de los datos personales de Facebook, en general, es realizada por parte de Facebook. Es decir, que la política sobre datos personales en Facebook tiene como base principal la autorregulación.[31]

3. *Microtargeting político*

A) Concepto y relevancia

En el ámbito de comunicación política, la persuasión mediante el estudio de mercado, la recopilación y análisis de datos para que posteriormente sean utilizados en estrategias de promoción en medios, es una práctica común. Estas prácticas están especialmente presentes en las campañas políticas. Entre las estrategias para una campaña política, se encuentra el targeting, el cual consiste en la división de los votantes en segmentos, de acuerdo con ciertas características comunes, para después diseñar contenido personalizado para cada

[31] Sophie Boerman, "Political *Microtargeting*: Relationship Between Personalized Advertising on Facebook and Voters' Responses", Cyberpsychology, Behavior, and Social Networking, junio 2016.

segmento.[32] El targeting y la segmentación del electorado son técnicas de comunicación y persuasión anteriores al *microtargeting* digital, la minería de datos. El uso de dichas técnicas para la comunicación personalizada ha permitido a los actores políticos relacionarse de manera eficiente con potenciales votantes con los que, de otra forma, hubiera sido más difícil y costoso relacionarse.[33]

Aunque las campañas políticas hayan utilizado actividades como targeting y *microtargeting* comúnmente en el pasado, con los constantes avances tecnológicos, las implicaciones y consecuencias del *microtargeting* son distintas. En vista de nuevas tecnologías y plataformas que constituyen una parte significativa de la vida cotidiana, como las redes sociales, la cantidad de información que puede obtenerse de los datos digitales es considerablemente mayor. De esta forma, también son mayores los riesgos, que actividades como el *microtargeting* político, implican para la privacidad de las personas que son objeto de las mismas. Sin embargo, por su

[32] International Institute for Democracy and Electoral Assistance, "Digital *Microtargeting*", Political Party Innovation Primer 1 (2018).
[33] International Institute for Democracy and Electoral Assistance, "Digital *Microtargeting*", Political Party Innovation Primer 1 (2018).

novedad, las consecuencias del *microtargeting* digital, específicamente, el político, han sido poco estudiadas.[34]

El *microtargeting* es una técnica que implica encontrar y analizar información sobre las preferencias de los individuos, así como sus hábitos de consumo. Con esto, posteriormente, los individuos pueden ser segmentados y reciben mensajes diseñados de acuerdo con su perfil y características.[35] Información del individuo como tipos de restaurantes que frecuenta, género de lectura preferido, preferencia en películas, opiniones sobre artistas, entre otros, puede producir resultados significativamente más precisos e incrementar la efectividad del *microtargeting*.[36] El *microtargeting* político se entiende cuando se hace uso de estas técnicas para la comunicación persuasiva política. De esta forma, la importancia que puede tener para la actividad de *microtargeting*, una plataforma como Facebook, con acceso a

[34] Entre los estudios más importantes sobre *microtargeting* digital se encuentra: *Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies*. Murray, Gregg. Journal of Political Marketing, Julio 2010; *Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?*'. Bennett, C. J. International Data Privacy Law, 6/4 (November 2016).

[35] *Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses.* Boerman, Sophie. Cyberpsychology, Behavior, and Social Networking. Junio 2016.

[36] *Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies*. Murray, Gregg. Journal of Political Marketing, Julio 2010.

este tipo de información sobre millones de usuarios, resulta clara.

Ahora bien, existen varios medios que el *microtargeting* político puede utilizar para hacer llegar los mensajes a los individuos que sean su objetivo. Uno de estos, es por medio del internet, redes sociales, correos, etc. Esto constituye el *microtargeting* digital. En el *microtargeting* digital, se analizan conjuntos de datos específicos, y por la cantidad de datos disponibles, se puede lograr una comprensión detallada del comportamiento, las opiniones y los sentimientos de los individuos. De forma que, el grupo de individuos que haya sido analizado será blanco de anuncios políticos en línea, que responderán a sus opiniones y preocupaciones individuales. Estos mensajes en línea solo pueden ser vistos por aquellos votantes en los grupos objetivo.[37]

Otro concepto importante es el de minería de datos. La minería de datos es una técnica utilizada para el *microtargeting*, que consiste en "un proceso de análisis inductivo de datos para encontrar patrones interesantes y relaciones previamente desconocidas".[38] En el marketing comercial, es una técnica

[37] International Institute for Democracy and Electoral Assistance, "Digital Microtargeting", Political Party Innovation Primer 1 (2018).
[38] Gregg Murray, Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies, ***Journal of Political Marketing*** (2010).

muy utilizada para realizar segmentación de mercados. Sin embargo, la minería de datos también puede ser útil para el *microtargeting* con fines políticos. Uno de los posibles resultados de la minería de datos para campañas políticas puede ser convencer a la población indecisa de votar, a hacerlo o a no hacerlo.[39]

Entonces, la minería de datos es una metodología de análisis de datos que emplea algoritmos especializados para extraer información de conjuntos de datos extensos.[40] A partir de esta información, se crean reglas que establecen relaciones entre dos variables distintas. Las reglas son derivadas de un árbol de decisión y pueden predecir el comportamiento futuro de nuevos datos y clasificar segmentos de un mercado.[41]

La segmentación, que ha sido mencionada repetidas veces para conceptualizar el *microtargeting* político, significa dividir, en este caso, al electorado, en bloques más pequeños y usar diferentes métodos de campaña para cada segmento. Cada regla obtenida por la minería de datos representa un segmento

[39] Gregg Murray, Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies, ***Journal of Political Marketing*** (2010).
[40] Bennett, C. J, Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?, ***International Data Privacy Law***, 6/4 (2016): 261–275.
[41] Gregg Murray, Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies, ***Journal of Political Marketing*** (2010).

conformado por individuos con características similares. De esta forma, los mensajes serán personalizados de acuerdo con las características, preferencias, opiniones específicas de cada segmento.[42]

La relevancia del *microtargeting* político en la actualidad se debe, principalmente, al impacto que este puede tener en la toma de decisiones de cualquier individuo que sea objeto de dicha actividad, especialmente en cuestiones electorales. Si bien el *microtargeting* político no es una práctica nueva, éste adquiere especial importancia debido a los avances tecnológicos y la creciente influencia de las redes sociales. Las redes sociales aumentan considerablemente la cantidad de información disponible sobre los individuos y, a diferencia de los otros medios, normalmente los individuos otorgan su consentimiento sin ser conscientes del alcance del tratamiento que se le puede dar a sus datos.

B) Cambridge Analytica como ejemplo de algunos de los riesgos del *microtargeting* político en Facebook

En 2013, investigadores del Centro Psicométrico de la Universidad de Cambridge analizaron los resultados de

[42] Bennett, C. J, Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?, ***International Data Privacy Law***, 6/4 (2016): 261–275.

voluntarios que tomaron un test de personalidad en Facebook para crear un perfil psicológico denominado OCEAN, por sus siglas en inglés que representan: "openness, conscientiousness, extraversion, agreeableness, and neuroticism". Esta investigación estableció una clara relación entre la actividad de los usuarios en Facebook y este perfil de personalidad. [43] Después de esto, se presentó un segundo proyecto de investigación por Global Science Research en cooperación con Cambridge Analytica, para identificar los parámetros necesarios para desarrollar los perfiles OCEAN utilizando un test de personalidad en una plataforma de Amazon (Amazon's Mechanical Turk platform and Qualtries). El test requería que los usuarios concedieran acceso a los datos de sus contactos en Facebook incluso aunque estos no hubieran consentido el test. Cambridge Analytica utilizó este análisis OCEAN, junto con otros datos privados y públicos, para desarrollar un *microtargeting* a los individuos más propensos a poder ser influenciados en su comportamiento político.[44]

En el año 2018, se reveló que la empresa de origen inglés Cambridge Analytica había utilizado los datos de los usuarios de Facebook para la creación de perfiles psicológicos,

[43] Christopher Wylie, "Mindf*ck: Cambridge Analytica and the Plot to Break America", London : Profile Books, 2019.
[44] *Ibid*

microtargeting y, por tanto, había influido, de algún modo en procesos electorales en Estados Unidos. [45] La Comisión Federal de Comercio de Estados Unidos comenzó a investigar a Facebook en marzo ese año, cuando fue revelado que utilizaban un test de personalidad para recolectar datos de los usuarios y posteriormente venderlos a Cambridge Analytica. Con las investigaciones a Cambridge Analytica se confirmó que habían utilizado técnicas ilícitas de extracción de datos no sólo para las elecciones de Estados Unidos, sino también para otros casos, como el Brexit y algunas elecciones en Sudamérica.[46]

Las investigaciones del caso Cambridge Analytica han continuado durante 2019. En julio de 2019, la Comisión Federal de Comercio de Estados Unidos acusó formalmente a Facebook de haber compartido de manera inapropiada los datos de 87 millones de usuarios con Cambridge Analytica. Así, la comisión ordenó a la red social a pagar una multa de 5.000 millones de dólares como sanción por las malas

[45] Carole Cadwalladr, "50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, The Cambridge Analytica Files, 17 de marzo de 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[46] *Ibid*

prácticas en el manejo de la seguridad de los datos de los usuarios.

A partir del caso de Cambridge Analytica, se visibilizó la interferencia que puede tener un sujeto interesado -por ejemplo, una consultora- en el proceso de toma de decisiones políticas de cualquier individuo, a través del uso de los datos personales que ese individuo sube voluntariamente a en redes sociales. Asimismo, se demostró la facilidad con la que se pudieron realizar transferencias de datos personales sin que los usuarios fueran conscientes del uso que se les daba a sus datos.

El desarrollo tecnológico ha permitido recabar, almacenar y procesar grandes cúmulos de información en tiempo real, lo cual, le ha dado un valor agregado a la información. Esto debe servir para discutir sobre la necesidad de realizar cambios tanto en políticas corporativas dentro de empresas como Facebook, así como cambios a nivel legislativo en materia de protección de datos personales y derechos de privacidad.

Asimismo, debe considerarse la relevancia que dichas transferencias pueden tener en las próximas elecciones presidenciales de Estados Unidos e, incluso, en elecciones de países como México. Por tanto, es de suma importancia que los ciudadanos cuenten con herramientas efectivas para contrarrestar violaciones a sus datos.

Capítulo II: Marco normativo vigente en California sobre protección de datos personales

En el 2018, *The Guardian* reveló información sobre sobre actividades ilícitas de la firma Cambridge Analytica, específicamente en las elecciones estadounidenses del 2016, al recabar información de los perfiles de Facebook de miles de usuarios sin que estos dieran su consentimiento o estuvieran al tanto de la recopilación de estos datos. Una de las discusiones que despertó el escándalo de Cambridge Analytica fue sobre la política de privacidad de Facebook y, consecuentemente, sobre la falta de legislación sobre protección de los datos personales en Estados Unidos.[47] Así, un desarrollador de bienes raíces interesado en este tema encabezó una iniciativa de una nueva legislación en materia de privacidad para California en la boleta estatal.[48] Si los votantes la hubiesen aprobado, la iniciativa habría sido excepcionalmente difícil de modificar y hubiera podido tener consecuencias

[47] Carole Cadwalladr, "50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, The Cambridge Analytica Files, 17 de marzo de 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[48] California Privacy Consumer Act (CCPA): Background on the CCPA & the Rulemaking Process. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa.

problemáticas. Sin embargo, esta iniciativa tuvo una respuesta fuerte de los opositores.[49]

Después de la certificación de la boleta, el desarrollador ofreció a la legislatura de California que, si aprobaban una ley sustancialmente similar a la iniciativa, él retiraría la iniciativa de la votación. Este acuerdo fue atractivo para todas las partes. Tanto el desarrollador como los oponentes ahorrarían gastos con este acuerdo y la legislatura tendría la posibilidad de arreglar la ley y modificarla con el tiempo.[50] Consecuentemente, la legislatura de California presentó, modificó y promulgó la **AB 375** o Ley de Privacidad del

[49] La iniciativa de boleta es un proceso que le permite a los ciudadanos de California presentar propuestas de ley y reformas sin contar con el apoyo del gobernador o de la Legislatura. El proceso sigue el siguiente orden: Primero, se escribe el texto de la propuesta; se envía el borrador de la iniciativa al Fiscal General para obtener el título oficial y el resumen; las medidas activas se convierten en iniciativas, mientras que las medidas inactivas son propuestas retiradas o fallidas; se circulan peticiones de iniciativa para recolectar suficientes firmas de los votantes registrados; las firmas se entregan a funcionarios electorales del condado para su verificación; la iniciativa será calificada para la boleta electoral o será reprobada por el Secretario de Estado, después de las verificaciones y las fechas límite; los votantes de California aprobarán o rechazarán la iniciativa de votación calificada.
State of California Department of Justice, "Ballot Iniciatives", https://oag.ca.gov/initiatives.

[50] California Privacy Consumer Act (CCPA): Background on the CCPA & the Rulemaking Process. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa.

Consumidor de California (en adelante CCPA por sus siglas en inglés).[51]

La CCPA fue firmada el 28 de junio de 2018 por el gobernador Brown, y entró en vigor el 1 de enero del 2020.[52] Esta ley tiene como objetivo que los consumidores tengan un mayor control sobre su información personal que es manejada y comercializada por empresas privadas.

Este capítulo tiene como objetivo analizar los aspectos principales de la CCPA y si esta es una legislación efectiva para regular las actividades minería de datos y *microtargeting* político en Facebook, de forma que se proteja a los usuarios de potenciales vulneraciones a su privacidad. Por tanto, el presente capítulo pretende afirmar que la CCPA no representa un mecanismo efectivo para proteger a los usuarios de Facebook frente a actividades como el *profiling* y el *microtargeting político*, las cuales, sin la debida regulación, pueden ser violatorias de los derechos de privacidad e incluso de otros derechos humanos, como el derecho a la autonomía y la libertad de decisión.

[51] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.100 Civil Code, 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.
[52] State of California Department of Justice. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

En esta tesina se seleccionó la legislación de California por sobre otras legislaciones estatales de EE.UU., principalmente por las siguientes razones:

a) La CCPA es la primera legislación estatal en Estados Unidos en la que se incorporan derechos del consumidor sobre sus datos personales similares a los que se encuentran en el GDPR. Esto es especialmente relevante, ya que el GDPR es considerado el instrumento más avanzado en materia de protección de datos personales.

b) Después del caso Cambridge Analytica, algunos estados, tales como Virginia, Massachussets y California, presentaron iniciativas para actualizar sus leyes sobre protección de datos personales. Sin embargo, California es el primer estado que firmó y aprobó una ley en la que se incorporen derechos del consumidor para otorgarle mayor control sobre su información personal. De esta forma, la CCPA representa la regulación más estricta de los Estados Unidos sobre protección de privacidad e información personal.

c) Con la entrada en vigor de esta ley en California, varias compañías que tienen responsabilidad de cumplimiento han anunciado que aplicarán las disposiciones de esta ley para todos sus consumidores en Estados Unidos. Por tanto, en algunos casos, las obligaciones adquiridas por esta ley serán

cumplidas incluso con respecto a usuarios residentes fuera de California.

1. Marco Normativo previo a la entrada en vigor de la CCPA

Como ya fue mencionado, la materia de datos personales en Estados Unidos se maneja como una subespecie del derecho a la privacidad. Por tanto, no existe una ley federal de privacidad. Asimismo, la mayor parte de las legislaciones estatales dejaban un espacio amplio a la autorregulación por parte de las empresas de redes sociales. Previo al caso de Cambridge Analytica, California no era la excepción a esta situación. La legislación de protección de datos personales en California derivaba del derecho a la privacidad establecido en el artículo 1 sección 1 de la Constitución de dicho Estado, el cual estipula lo siguiente:

> Todas las personas son por naturaleza libres e independientes y tienen derechos inalienables. Entre estos están disfrutar y defender la vida y la libertad, adquirir, poseer y proteger la propiedad, y buscar y obtener seguridad, felicidad y privacidad.[53]

[53] Sec. 1 added Nov. 5, 1974, by Proposition 7. Resolution Chapter 90, 1974.

Las leyes de California en materia de privacidad, derivadas del artículo previamente mencionado, se pueden clasificar en: leyes sobre privacidad en general, privacidad en línea, política de información sobre salud, y leyes sobre robo de identidad. Para el tema de datos personales en redes sociales son aplicables las contenidas en las de privacidad en general y en las de privacidad en línea. Dentro de la clasificación de privacidad en general se encuentran normas como la de números de cuentas bancarias en la sección 4100 del Código Financiero de California[54] o la Ley de Privacidad de las Comunicaciones Electrónicas de California, contenida en la sección 1546 del Código Penal. En esta última se requiere que las entidades gubernamentales obtengan una orden de registro para poder acceder a datos almacenados en un dispositivo electrónico o datos de un proveedor de servicios en línea.[55]

En la categoría de privacidad en línea se encuentran cuatro normas: la ley de protección de la privacidad en línea del 2003, información personal recopilada en internet, funcionarios públicos, y para expedientes de alumnos. De estas cuatro, la ley aplicable, previo al caso de Cambridge Analytica, para

[54] Section 4100, California Financial Code, Consultado el 27 de febrero de 2020 http://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml.

[55] Section 1546, Penal Code of California, California Electronic Communications Privacy Act, 1986.

redes sociales como Facebook, era la ley de protección de la privacidad en línea del 2013. Esta ley establecía que los sitios web comerciales o servicios en línea que recopilaran o trataran información personal de los consumidores, tendrían que publicar una política de privacidad en su sitio y cumplir con ella. La política de privacidad tenía que contener las categorías de información de identificación personal recopilada y las categorías de información de terceros con quienes el sitio compartiera la información.[56] De tal forma, que la regulación para el tratamiento de los datos personales en redes sociales dependía de lo que cada negocio estipulara en su política de privacidad y la ley no preveía ningún tipo de derecho del consumidor sobre su información. Entonces, la legislación tenía como base principal de protección al consumidor los dos elementos siguientes: una política de privacidad que cumpliera con los requerimientos mínimos de la ley y el consentimiento del consumidor a dicha política. Tampoco existía una norma que facultara a alguna autoridad de California para resolver sobre controversias en la materia, por lo que cualquier controversia relacionada a la protección de datos personales en

[56] The Verge, No one is ready for California's Consumer Privacy act, The Verge, 2019, https://www.theverge.com/2019/12/31/21039228/california-ccpa-facebook-microsoft-gdpr-privacy-law-consumer-data-regulation (Fecha de consulta: 27 de febrero 2020).

redes sociales sería competencia de la Comisión Federal de Comercio.

Por tanto, antes de la CCPA, California sí contaba con una legislación extensa sobre la privacidad de sus ciudadanos. Sin embargo, en materia de datos personales en línea, específicamente, los recopilados y tratados por redes sociales, la legislación californiana no difería de la laxitud y falta de precisión que caracterizaban, en general, a la protección de datos personales estadounidense en el orden estatal.

2. La CCPA y su contenido

Con la entrada en vigor de la CCPA, California cambia su regulación para la protección de la privacidad de los consumidores, adoptando una legislación rígida que se asimila a la europea. La CCPA representa la legislación con mayor protección a los consumidores de redes sociales en Estados Unidos. Consecuentemente, también representa un posible modelo para legislaciones en esta materia que están siendo discutidas en otros Estados. Esto se debe, principalmente, a cuatro factores: les otorga derechos a los consumidores sobre los datos que serán manejados por las empresas privadas, confiere a los consumidores la posibilidad de presentar acciones privadas en ciertos casos, faculta al Procurador

General de California para establecer regulación en la materia y atender los casos de controversias que se presenten y establece la obligación de que las empresas ofrezcan a los consumidores la opción *"Do not sell my information"*.[57]

En esta sección se analizará el contenido de la CCPA que se considera más relevante para el tema y objeto de la presente tesina.

A. Ámbito subjetivo de aplicación

De acuerdo con el objeto de la CCPA, los sujetos de la ley pueden clasificarse en dos categorías: los sujetos obligados y los sujetos de protección. Los sujetos de protección de la CCPA son las personas físicas residentes del Estado de California.[58] Por su parte, los sujetos obligados por la CCPA son las empresas[59] de carácter privado que operen en California. Esta ley no obliga a entidades gubernamentales o sin fines lucrativos. Una entidad que califica como empresa en términos de la CCPA, es cualquier empresa, corporación,

[57] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.100 Civil Code, 2018 (pp. 35) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

[58] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 (g) Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

[59] Se utilizará el término empresa como equivalente del término "business" utilizado en el texto original de la CCPA

asociación u otra entidad legal que opera para el beneficio financiero de sus accionistas o propietarios, que recopila o en nombre de la cual se recopila información personal de los consumidores, y que determina los propósitos y medios del procesamiento de dicha información.[60] Asimismo, para que la empresa se encuentre obligada por la CCPA, debe cumplir tres requisitos:

> 1) tener $ 25M + en ingresos anuales, u
>
> 2) obtener más del 50% de sus ingresos de la venta de datos del consumidor, o
>
> 3) comprar, recibir anualmente para fines comerciales del negocio, vender o compartir acciones para fines comerciales, solos o en combinación, la información personal de 50,000 o más consumidores, hogares o dispositivos.[61]

B. Ámbito territorial de aplicación

En el contenido de la CCPA no hay un apartado específico para definir su aplicación o alcance territorial. Sin embargo, con

[60] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 (c) Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

[61] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 Civil Code, 2018 (pp. 10) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

base en varios apartados, se puede entender que la CCPA es aplicable si por lo menos uno de los siguientes tres factores se encuentra o se lleva a cabo en el territorio del Estado de California: el establecimiento o lugar de operación de la empresa, la residencia del titular de la información y el lugar donde se realiza la conducta comercial.

En primer lugar, una empresa puede estar dentro del ámbito de aplicación territorial de la CCPA por medio de dos formas. De forma directa, cuando se encuentra establecida en California.[62] Por otro lado, una entidad que no se encuentre establecida en California puede estar obligada por la CCPA cuando controle o sea controlada por una empresa que esté establecida en California, cumpla con los requisitos mencionados previamente y comparta marca con dicha empresa.[63]

En segundo lugar, la CCPA es aplicable a cualquier empresa que recopile información personal de una persona física que resida en California. Por último, la actividad comercial, o la

[62] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 (c) Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.
[63] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 (c)(2) Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

recopilación de la información se debe llevar a cabo dentro de California.

C. Derechos del consumidor

Como ya fue mencionado, uno de los principales aspectos de la CCPA es que concede derechos a los consumidores, similares a los del GDPR.[64] La CCPA reconoce, esencialmente, los siguientes derechos a sus consumidores: el derecho a saber, derecho de supresión, derecho a elegir que sus datos no sean vendidos y derecho a no discriminación.

El derecho a saber o derecho de acceso consiste en que los consumidores puedan estar informados acerca de las prácticas que las empresas realizan con sus datos. Al respecto, la CCPA establece que el consumidor tendrá derecho a solicitar que una empresa que recopile su información personal le revele las categorías y piezas específicas de información, así como los propósitos para recopilar dicha información.[65] El consumidor debe ejercer su derecho a saber por medio de una "solicitud verificable del consumidor". Si la solicitud del consumidor no está debidamente autenticada, el negocio no enviará la información solicitada.[66] Esto se adopta como medio de

[64] California Privacy Consumer Act (CCPA): Background on the CCPA & the Rulemaking Process. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa.

[65] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.100 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

[66] Se considera que una solicitud está debidamente autenticada cuando la empresa puede verificar que quién la realiza es en efecto el consumidor del

protección contra la obtención ilegal de información personal de un tercero. Al mismo tiempo, la empresa que recopila información personal del consumidor tiene la obligación de informar a los consumidores, antes o al momento de la recopilación, sobre las categorías y propósitos de la recopilación.[67]

Es importante destacar que estas normas acerca del derecho a saber son aplicables a cualquier empresa que recopile información personal de los consumidores, independientemente de si vende o no tal información. La CCPA contiene también una sección específica para el derecho a saber en caso de que la empresa venda la información personal que recopila de sus consumidores. En dicha sección, la ley dispone que el consumidor tiene derecho a solicitar, de una empresa que vende su información personal o que la divulgue con fines comerciales: las categorías de información

---

que se está recolectando la información. Sección 1798.140, inciso (y), CCPA.

Se considera una solicitud verificable del consumidor la que se realiza desde una cuenta, protegida por contraseña, mantenida por el consumidor con la empresa, mientras el consumidor está conectado a la cuenta. Asimismo, un consumidor que no mantiene una cuenta con la empresa puede hacer la solicitud de información siempre que la empresa pueda autenticar la identidad del consumidor. Sección 1798.185, inciso (a), párrafo (7), CCPA.

[67] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.100 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

personal que recopiló; las categorías de información que vendió o divulgó con propósito comercial; las categorías de terceros a quiénes vendió la información.[68] Para esto, también se requiere de una solicitud verificable del consumidor.

Por último, otro aspecto relevante del derecho a saber contenido en la CCPA, es que su ejercicio se encuentra limitado a un máximo de dos solicitudes por cada consumidor en un período de 12 meses. Asimismo, la empresa no está obligada a retener información personal recopilada sólo para una transacción si ésta no es vendida o si no se considera como información personal.

Por otro lado, el derecho de supresión obliga a la empresa a eliminar cualquier información personal que haya recolectado sobre cualquier consumidor que, por medio de una solicitud verificable, requiera hacer uso de este derecho.[69] Toda empresa que recolecte información personal de sus consumidores está obligada a cumplir con este derecho, incluso si no vende los datos. Al recibir la solicitud verificable

[68] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.115 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.
[69] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.105 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

del consumidor la empresa debe eliminar la información personal de sus registros y ordenar a cualquier proveedor de servicios que elimine la información de sus registros.[70] Adicionalmente, la CCPA contempla algunas excepciones en las que la empresa no estará obligada a eliminar la información del consumidor.[71]

El derecho de portabilidad existe en relación con el derecho de acceso y consiste en la obligación de la empresa de proporcionar la información personal correspondiente a la solicitud del consumidor, en un formato fácilmente utilizable

[70] *Ibid*

[71] La empresa no está obligada a eliminar la información del usuario si es necesario que se la mantenga para: 1) completar la transacción para la cual se recopiló; cumplir con los términos de una garantía escrita o retiro de producto realizado de acuerdo con la ley federal, proporcionar un bien o servicio solicitado por el consumidor o ejecutar un contrato entre la empresa y el consumidor; 2) detectar incidentes de seguridad, protegerse contra actividades maliciosas, engañosas, fraudulentas o ilegales; o enjuiciar a los responsables de esa actividad; 3) depurar para identificar y reparar errores que perjudiquen la funcionalidad prevista existente; 4) ejercer la libertad de expresión, garantizar el derecho de otro consumidor a ejercer el derecho a la libertad de expresión de ese consumidor o ejercer otro derecho previsto por la ley; 5) cumplir con la Ley de Privacidad de Comunicaciones Electrónicas de California; 6) participar en investigaciones científicas, históricas o estadísticas públicas (…) cuando es probable que la eliminación de la información por parte de la empresa haga imposible o perjudique seriamente su logro cuando el consumidor de su consentimiento; 7) permitir únicamente usos internos que estén razonablemente alineados con las expectativas del consumidor en función de la relación del consumidor con la empresa; 8) cumplir con una obligación legal; 9) utilizar de otra manera la información personal del consumidor, internamente, de manera legal que sea compatible con el contexto en el que el consumidor proporcionó la información.

para permitir que el consumidor transmita la información de una entidad a otra entidad sin obstáculos.[72]

Finalmente, el derecho a la no discriminación consiste en la obligación de la empresa de no dar un trato distinto a los consumidores que hayan ejercido alguno de los otros derechos contenidos en la CCPA. En la sección del derecho a la no discriminación se enlistan algunas de las actitudes que se consideran como discriminatorias, como negarle el servicio, cobrar diferentes precios por bienes o servicios, entre otras.[73]

D. El derecho a optar por que no se venda la información (*right to opt-out*)

Otro derecho que confiere la CCPA a los consumidores, es el específico para las empresas que recolectan y venden esa información personal. Así, la ley determina que el consumidor tiene de derecho a ordenar a la empresa que no venda su

[72] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.110 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.
[73] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.125 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

información personal a terceros. En la CCPA se hace referencia a este derecho como *the right to opt-out.*[74]

Asimismo, la CCPA impone a las empresas que vendan información, la obligación de notificar al consumidor que su información puede ser objeto de venta a terceros y la de hacerle saber que tiene la opción de no consentir a esta venta, en cualquier momento.[75] A partir del momento en el que el consumidor decida utilizar la opción de *opt-out*, la empresa estará impedida de vender su información personal a menos que posteriormente el consumidor le dé autorización expresa de que lo haga.[76]

En el mismo sentido, las empresas tienen la obligación proveer al consumidor de un link claro y visible de "No vender mi información personal", que lo dirija a una página en la que pueda ejercer su derecho. De la misma manera, junto con el link, la empresa debe ofrecer una explicación del derecho del consumidor a optar porque no vendan su información. Esto se

[74] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.115 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.
[75] *Ibid*
[76] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.135 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

puede hacer por distintos medios; por ejemplo, se puede incluir en su aviso de privacidad.[77]

3. Análisis de la CCPA con respecto al microtargeting político en Facebook

En esta sección del capítulo, la presente tesina pretende analizar si las obligaciones contenidas en la CCPA son aplicables a Facebook y, en su caso, si sirven para regular el *microtargeting* político y para limitar las potenciales vulneraciones que esta actividad puede tener a la privacidad de los usuarios.

A. Facebook como sujeto obligado de la CCPA

Para esto, primeramente, se debe determinar si Facebook califica como sujeto obligado por la CCPA. Facebook es, en efecto, una entidad que recolecta y almacena información personal de sus consumidores, y que tiene operación en el estado de California. Como ya se explicó en el apartado anterior, para calificar como empresa bajo la CCPA, las entidades deben cumplir con por lo menos uno de tres requisitos. En este caso, Facebook, indiscutiblemente, cumple con el primero, puesto que en sus reportes anuales se muestra

[77] *Ibid*

que recibe más de veinticinco millones de dólares de ingresos anuales.[78]

En cuanto a los otros dos requisitos, pueden existir dudas de si Facebook cumple con los supuestos que plantean. Estas dudas tienen como base la determinación de la actividad comercial de Facebook. Uno de los supuestos exige que el 50% de los ingresos de la empresa provengan de la venta de información personal de los consumidores. El segundo establece que la empresa compre, reciba o comparta por propósitos comerciales la información personal de 50,000 consumidores o más.[79]

La discusión acerca de si Facebook vende o no vende los datos de sus usuarios a terceros será abordada más adelante en el presente capítulo. Por lo pronto, se considera que, independientemente de la definición que se dé a la actividad comercial de Facebook, esta plataforma sí califica como empresa para la CCPA, ya que cumple con la definición de empresa estipulada en la ley y con el requisito de ingresos anuales.

[78] Expansión. 2020. "Facebook aumenta sus ingresos un 11% en el segundo trimestre", 30 de julio.
[79] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.115 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

B. Aplicación territorial

Ya fue explicado que la aplicación territorial de la CCPA depende de tres factores: establecimiento o lugar de operación, residencia del titular de los datos y lugar de la conducta comercial. Así, en primer lugar, Facebook debe tener establecimiento y/o lugar de operación en California. De esta forma todas las operaciones de Facebook en California deben cumplir con la normatividad de la CCPA. Sin embargo, también serían alcanzadas por esta ley las operaciones realizadas por Facebook, fuera de California. En efecto, puede que la CCPA sea uno de los marcos normativos vigentes más relevantes para Facebook en el ámbito internacional.

Por otro lado, la aplicación y alcance territorial de la CCPA es importante para determinar qué usuarios pueden ejercer los derechos que confiere dicha ley. De acuerdo con la CCPA, el usuario de Facebook se considera como consumidor si reside en el estado de California. Así, sólo los usuarios que sean residentes californianos podrían exigir el cumplimiento de los derechos contenidos en la CCPA.

La delimitación del lugar de la conducta comercial es la que resulta más complicada, debido a la naturaleza extraterritorial de la actividad de las redes sociales. Asimismo, podría haber problemas para determinar la aplicación si mientras un

residente californiano se encuentra fuera del estado se recolecta y transfiere su información personal.

En este sentido, la CCPA es aplicable a las actividades de Facebook siempre que alguno de los tres factores ya mencionados se pueda establecer en California. Se ha hablado de la posibilidad de que Facebook adapte su política de privacidad a las estipulaciones de la CCPA para todos los estados de EE.UU. Sin embargo, esto sería una decisión privada de Facebook.

C. Los derechos del consumidor para los usuarios de Facebook

¿La CCPA representa un cambio de regulación para Facebook? Como ya se había mencionado previamente, la legislación federal y estatal en EE.UU. dejaba la actividad de Facebook principalmente librada a su autorregulación. Esto indicaría que una ley como la CCPA, considerada la legislación más estricta hasta el momento en EE.UU. en la materia, representaría un cambio importante para la política de privacidad y manejo de datos de Facebook. Sin embargo, se tiene que considerar que Facebook ya había adecuado su política general para que cumpliera con las exigencias del GDPR. En consecuencia, hay quienes consideran que es probable que Facebook no tenga que realizar cambios significativos en su política, puesto que ya cumplía con el

GDPR, y con los puntos en común que aquél tiene con la CCPA.[80]

En virtud del derecho de acceso, los usuarios de California podrían pedirle a Facebook las categorías de información sobre ellos mismos que han sido recolectadas y con qué propósitos. La diferencia entre el derecho de acceso en el GDPR y en la CCPA se da realmente en los procesos de solicitud y plazos, los cuales hacen al derecho contenido en la CCPA un poco más limitado.[81]

En general, los derechos contenidos en la CCPA funcionan de manera muy similar a los del GDPR, pero de una forma más limitada. Esto pasa con los derechos de no discriminación, portabilidad y supresión.[82] En cuanto al derecho de supresión, la CCPA da a los usuarios de Facebook el derecho a que se elimine su información y, por tanto, ya no pueda ser almacenada o procesada. Sin embargo, la CCPA incluye varios supuestos en los que Facebook podría rehusarse a hacer cumplir esta solicitud.[83] Asimismo, estos derechos implican

[80] Antonio García, "Why California's Privacy Law Won't Hurt Facebook or Google", 2018. https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/. Consultado el 28 de mayo del 2020.
[81] Laura Jehl, "CCPA & GDPR Comparison Chart", Baker Law, 2018. https://bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf
[82] *Ibid*
[83] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.115 (d) Civil Code, 2018

una limitación al manejo, procesamiento y transferencia de información personal en Facebook, sólo en tanto los usuarios exijan activamente su cumplimiento. En consideración de que al crear una cuenta se debe aceptar la política de privacidad de Facebook, si un usuario no realiza la solicitud verificable del consumidor como está requerida en la CCPA, el tratamiento de su información seguirá esencialmente sujeto a la autorregulación de Facebook.

La CCPA sí incluye una sección sobre requerimientos mínimos que debe tener la política de privacidad, entre los que se encuentra informar al usuario sobre las categorías de información y el propósito de recolección. Esto Facebook ya lo incluye en su aviso; sin embargo, más adelante en esta tesina se abordará por qué esto no es eficiente para limitar las acciones de Facebook sobre la información personal de sus usuarios.

Ahora bien, ¿cómo repercuten los derechos del consumidor de la CCPA en el *microtargeting* político? Ya que se aclaró que Facebook es sujeto obligado por la CCPA, el contenido de esta ley regula todas las actividades que realice Facebook con la información personal de sus usuarios, incluyendo así el *microtargeting* comercial y el *microtargeting* político.

---

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

Sin embargo, la presente tesina afirma que el *microtargeting* político se encuentra regulado por la CCPA únicamente en cuanto al ejercicio de los derechos que se le confieren al usuario de Facebook. En este sentido, con el derecho de acceso y portabilidad, el usuario debería recibir información que indicará las categorías de información que Facebook ha recolectado junto con la lista de anunciantes que han hecho uso de targeting con su cuenta.

Podría parecer que el derecho de supresión funcionaría para limitar que la información personal del usuario se destine a minería de datos y posteriormente a *microtargeting* político, sin embargo, como ya fue mencionado, este derecho tiene muchas limitantes. Asimismo, es necesario plantear que todos estos derechos del usuario de Facebook, conferidos por la CCPA, pueden funcionar para regular de cierta forma el *microtargeting* político, sólo en la proporción del entendimiento del usuario sobre este tema. No hay realmente una regulación directa del *microtargeting* político en Facebook, sino un aumento del control del usuario de Facebook sobre lo que Facebook realiza con su información, considerando también que dicho control es más limitado que el que confiere el GDPR a los usuarios europeos.[84]

[84] Laura Jehl, "CCPA & GDPR Comparison Chart", Baker Law, 2018. https://bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf

De esta forma, la presente tesina afirma que, aunque la CCPA implica un avance en la legislación estadounidense al otorgar a los usuarios de California un mayor control sobre su información personal, ésta no implica una limitación importante para Facebook ni una regulación del *microtargeting* político realizado en esta plataforma.

D. Ineficacia de la CCPA para regular la venta de información como parte de la actividad comercial de Facebook

Esta tesina sostiene que el *microtargeting* político en Facebook implica una venta de datos a los anunciantes. Por tanto, una forma indirecta de regular el *microtargeting* político, sería limitar y regular la venta de información de los usuarios de Facebook. De esta manera, por medio del derecho de acceso, el usuario podría saber qué información se está vendiendo, y cuándo la venta es a agentes políticos, así como también podría optar por que su información no sea vendida para tales fines.

En este sentido, la CCPA otorga un derecho que no se encuentra contemplado como tal en el GDPR, que es el derecho de optar porque la información personal no sea objeto de venta. Este derecho podría funcionar para limitar la

transferencia de información personal de los usuarios de California a sujetos o entidades con fines políticos. Sin embargo, existe discusión sobre si este derecho, considerado como uno de los aspectos más importantes de la CCPA, es aplicable con respecto a Facebook. Esto se debe a que Facebook declara que su actividad comercial sólo incluye la venta de publicidad, no de información o datos personales. Asimismo, no hay consenso sobre si, la información que pueden procesar los anunciantes, puede calificarse como venta de información personal, ya que es información anonimizada.

Por estas razones, la presente tesina considera que la falta de acuerdo en cuanto a la definición de la actividad comercial de Facebook es una de las principales muestras de la ineficacia de la legislación para proteger al usuario contra las potenciales vulneraciones que el *microtargeting* político produce en su privacidad y sus datos personales. La CCPA no contempla una definición de la actividad comercial que se adapte a la práctica real de las plataformas de redes sociales en el mercado digital. En consecuencia, esto ha servido a Facebook como excusa para evadir la aplicación de medidas de regulación más estrictas en cuanto a cómo maneja los datos personales de sus usuarios y, por tanto, le ha dado la posibilidad de evadir medidas que podrían funcionar para regular o limitar el

microtargeting político que se lleva a cabo dentro de la plataforma.

Esta tesina afirma que, si bien Facebook no vende directamente datos personales identificables a usuarios específicos, esto no significa que la actividad comercial de Facebook no deba ser regulada de la misma forma que cualquier negocio que forme parte del mercado digital de datos. Para entender mejor por qué Facebook podría evadir el cumplimiento de las secciones de la CCPA dirigidas a la venta de datos, se analizarán los dos argumentos principales que plantea Facebook sobre su actividad comercial: a) las empresas no pagan un precio por obtener el código con la información sobre usuarios de Facebook, pagan por la publicidad puesta en dicha plataforma utilizando listas de segmentos demográficos específicos; b) la información sobre usuarios a la que tienen acceso las empresas que pagan por publicidad en Facebook es anónima, es decir, no se otorgan datos de una persona o personas físicas identificas.

En primer lugar, es necesario plantear la definición de venta de información personal. La CCPA define la venta como cualquier acción de vender, alquilar, liberar, divulgar, difundir, poner a disposición, transferir o comunicar oralmente, por escrito, o por medios electrónicos o de otro tipo, la

información personal de los consumidores a otra empresa o un tercero a cambio de una consideración monetaria o valiosa.[85]

Asimismo, la CCPA contempla supuestos específicos en los que no se considera que una empresa vende información, entre los que se encuentra el supuesto en el que la empresa utiliza o comparte con un proveedor de servicios información personal de un consumidor que es necesaria para realizar un propósito comercial. Para que la empresa califique en este supuesto, tendría que cumplir con dos condiciones: haber notificado que esa información se utiliza o comparte en sus términos y condiciones; el proveedor de servicios, en este caso, no debe recopilar, vender ni usar la información personal del consumidor, excepto cuando sea necesario para realizar el propósito comercial.[86]

Además, es necesario entender el funcionamiento básico del proceso de intercambio de información entre Facebook y los posibles anunciantes ya sea políticos o puramente comerciales. Facebook utiliza un rastreador píxel, el cual se presenta como

[85] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.140 (t) (1) Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

[86] Legislative Counsel of California, Assembly Bill No. 375, Sec. 1798.135 Civil Code, 2018 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018.

una herramienta ofrecida a los anunciantes que paguen su servicio publicitario.[87] El píxel de Facebook es el código que permite a esta plataforma recolectar datos que sirvan para mejorar la efectividad de los anuncios y para poder realizar el "*targeting*" a ciertos grupos demográficos de usuarios.

Asimismo, el píxel de Facebook es utilizado por los anunciantes como un fragmento del código, que el anunciante coloca en su sitio web de forma que tenga acceso a información de los usuarios con la que se pueden construir herramientas para efectivizar el *microtargeting*.Del intercambio de información que se realiza entre los anunciantes y Facebook por medio de este código, se garantiza la capacidad de "entregar anuncios a las personas con más probabilidades de realizar determinadas acciones".[88]

Entonces, Facebook afirma que debido a cómo funciona su píxel, y a que es mediante este código, aparentemente gratuito, que los anunciantes tienen acceso a la información de sus usuarios, la venta de datos no se encuentra dentro de su actividad comercial. En cambio, sostiene que el producto que

[87] Sara Morrison, "Facebook is gearing up for a battle with California's new data privacy law", Vox, 17 de diciembre de 2019. https://www.vox.com/recode/2019/12/17/21024366/facebook-ccpa-pixel-web-tracker

[88] S. C. Matza, M. Kosinski, "Psychological targeting as an effective approach to digital mass persuasion", Columbia University, 2017.

vende es la publicidad dirigida a sectores demográficos específicos (*targeting*/*microtargeting*), mientras que el código de píxel es sólo una herramienta para la realización de su objetivo comercial.

Sin embargo, esta forma de ver la actividad comercial de Facebook no considera que el píxel de Facebook sí amplía el alcance de su mercado por fuera de sólo un mercado publicitario. La información que obtienen los anunciantes por medio del píxel de Facebook les otorga la posibilidad de construir su propia base de datos utilizando esta información y así realizar un *microtargeting* más efectivo tanto dentro como fuera de Facebook.[89] La ventaja comparativa de realizar la publicidad dentro de Facebook viene justamente de la amplia base de datos que Facebook tiene de sus usuarios y que para utilizar dicha información los anunciantes deben pagar los servicios de publicidad dentro de la plataforma.

La recolección de los datos de los usuarios de Facebook representa una barrera en la entrada al mercado de publicidad a otros competidores con una red menor de usuarios. De esta forma, Facebook tiene un poder sustancial en un mercado publicitario en el que el objetivo sea dirigirse a sectores

[89] Michael Kosinsky. Facebook sells personal data. https://www.nytimes.com/2018/12/12/opinion/facebook-data-privacy-advertising.html.

demográficos específicos. El poder sustancial en el mercado le da a su vez mayor capacidad de recolectar datos e información personal de los usuarios.[90] Cuanto mayor sea la red de usuarios de una plataforma digital, tendrá más capacidad de recolección de datos, lo que a su vez aumenta significativamente la efectividad de tecnologías para la comunicación persuasiva, como lo es el *microtargeting* político. El mercado de *microtargeting* publicitario en Facebook depende directamente del funcionamiento de este código, puesto que sin él no habría razón para que los anunciantes compraran el servicio de Facebook, en primer lugar.

Ahora bien, otro cuestionamiento sobre la efectividad en la aplicación de la legislación existente para proteger la privacidad de los usuarios es que el píxel de Facebook funciona de forma que la información que se da a los anunciantes es anónima. Es decir que los anunciantes reciben información sin que ésta contenga datos de personas físicas identificadas. Los anunciantes no reciben nombres, perfiles ni correos electrónicos específicos. Si bien pueden conocer información de preferencias de los usuarios en cuanto a sus

[90] ACCC. Regulation for Digital Platforms. Final Report 2019.

anuncios, no sabrán de qué usuarios específicos proviene dicha información.

De esta forma, surge la duda de si realmente existe una vulneración a la privacidad y los datos personales de los usuarios de Facebook. La presente tesina sostiene que sí existe una vulneración importante a los datos personales y a la privacidad de los usuarios, ya que la información que provee el código píxel es el factor esencial para que, con minería de datos, tanto Facebook como anunciantes externos realicen predicciones acertadas sobre características de la vida íntima y puedan revelar aspectos que se consideran dentro del espectro de información o datos personales sensibles. Al respecto, ya se han realizado investigaciones que comprueban que, con acceso a información sin ser identificable a personas en específico, se puede obtener información personal sensible de los usuarios de plataformas digitales que posteriormente es utilizada con fines de comunicación persuasiva del comportamiento.[91]

Con lo anterior, y en consideración del antecedente de Cambridge Analytica, es evidente que el *microtargeting* representa una herramienta relevante para actores interesados en persuadir efectivamente el comportamiento de los

[91] Uno de los estudios sobre la efectividad de la persuasión utilizando información recolectada sobre usuarios en plataformas digitales es el siguiente: S. C. Matza, M. Kosinski, "Psychological targeting as an effective approach to digital mass persuasion", Columbia University, 2017.

individuos de forma que se beneficien sus propios intereses políticos. La legislación permite que la actividad comercial publicitaria de Facebook se lleve a cabo de tal forma que los intereses de persuadir del anunciante se encuentran por encima de los potenciales daños que éstos puedan causar a los usuarios.

Esto es, en parte, consecuencia de la falta de adaptabilidad de la CCPA a la práctica de las plataformas digitales de redes sociales y a las técnicas publicitarias que evolucionan de forma continua. De esta forma, las previsiones sobre venta de datos en la CCPA no se adecúan de manera efectiva al funcionamiento de la actividad comercial de Facebook y, en consecuencia, a las implicaciones que tiene la venta de información de usuarios con el propósito de realizar publicidad mediante el *microtargeting* político.

La iniciativa de la CCPA se presentó en el contexto de lo sucedido con Cambridge Analytica. Sin embargo, al analizar la CCPA y el contexto actual de las redes sociales como Facebook, es posible concluir que esta ley no es un mecanismo suficiente ni totalmente efectivo para regular el uso de datos personales por parte de Facebook y redes sociales similares. Además, la CCPA, a pesar de otorgar derechos al consumidor, no clasifica como una regulación directa de actividades realizadas por redes sociales relacionadas con el manejo de

datos que tienen la potencialidad de vulnerar la privacidad del usuario. Asimismo, no contiene regulación especial ni para el *microtargeting* político ni para la creación de perfiles utilizando los datos.[92] La CCPA se limita, principalmente, a la regulación de las transacciones comerciales simples de información personal y a que el consumidor tenga conciencia u control sobre dichas transacciones. Así, a pesar de que la CCPA significa un considerable avance en materia de privacidad y protección de datos personales en Estados Unidos, un panorama futuro debe incluir legislación de protección de datos personales más especializada en la regulación de plataformas digitales.

[92] En la legislación europea sí se regula la creación de perfiles, en el artículo 22 del GDPR, que estipula el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente.

Capítulo III: Marco normativo vigente en México sobre protección de datos personales

1. Evolución del derecho mexicano en materia de protección de datos personales

El derecho de protección de datos personales, originalmente, se deriva del derecho a la privacidad. Sin embargo, con el constante desarrollo de nuevas tecnologías y el avance del internet en el mundo globalizado, el derecho de protección de datos personales ha evolucionado de tal forma que, hoy en día, México lo reconoce como un derecho fundamental y autónomo. En esta sección, se realizará una explicación general de la evolución del derecho de protección de datos personales en México.

La primera presencia de la protección de datos personales en México se deriva de un instrumento internacional, la Declaración Universal de los Derechos Humanos, del 10 de diciembre de 1948.[93] En el artículo 17 establece que nadie será objeto de injerencias arbitrarias en su vida privada. No obstante, en el orden interno, fue recién en 1990 cuando se creó la Comisión Nacional de Derechos Humanos. Además, la

[93] ONU: Asamblea General, Declaración Universal de Derechos Humanos, 10 Diciembre 1948. 217 A (III).

importancia constitucional de los derechos fundamentales en instrumentos internacionales se deriva de las reformas de 2011.[94] Asimismo, en el ámbito internacional, en 1980 en el marco de la Organización para la Cooperación y el Desarrollo Económico se emitieron las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales", el primer instrumento supranacional que analiza a profundidad el derecho a la protección de estos datos específicamente.[95]

En cuanto a instrumentos legislativos nacionales, antes de 2002, México no contaba con previsión alguna sobre protección de datos personales en específico. Se consideraba que cualquier asunto en esta materia entraba dentro del ámbito de protección del derecho a la vida privada. En junio del 2002 entró en vigor la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que contaba con una sección dirigida a la protección de datos en posesión del sector público.[96]

---

[94] Diario Oficial de la Federación, reforma constitucional a artículos 1º, 3º, 11, 15, 18, 29, 33, 89, 97, 102 apartado B y 105, publicada el 10 de junio del 2011

[95] Instituto Federal de Acceso a la Información Pública, La protección de datos personales en México: una propuesta para deliberar, julio de 2008, http://iaipoaxaca.org.mx/biblioteca_virtual/datos_personales/5.pdf.

[96] Cámara de Diputados. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. DOF 9 de mayo del 2011.

En dicha ley fue incluido un capítulo de protección de datos personales, en el cual se establecieron los principios generales que rigen el tratamiento de datos personales en posesión de los entes públicos. Asimismo, se estableció como órgano garante al Instituto Federal de Acceso a la Información Pública.[97]

En 2007 se reformó el artículo 6 de la Constitución.[98] En materia de protección de datos personales, las fracciones II y III de dicho artículo señalan que "la información que se refiere a vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes".[99] Además, que "toda persona tendrá acceso a sus datos personales o a la rectificación de estos respectivamente."[100]

El 2009 se reformó el artículo 16 constitucional de forma que se reconoce al derecho de protección de datos personales como un derecho fundamental y autónomo.

> Art 16. (…) Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y

[97] A partir de 2015, fue sustituido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
[98] Decreto que reforma los artículos 6, 41, 85, 99, 108, 116 y 112. DOF 13 de noviembre del 2007. 3ª Reforma al artículo 6º. http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum_art.htm.
[99] Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos. Artículo 6.
[100] *Ibid*

> cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[101]

La primera ley en materia únicamente de protección de datos fue la Ley Federal de Protección de Datos Personales en posesión de los Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010.[102] Posteriormente, en 2017, entró en vigor la Ley General de Protección de Datos Personales en posesión de sujetos obligados.[103]

2. *La Ley Federal de protección de datos personales en posesión de particulares, su aplicabilidad y las herramientas para proteger los derechos del titular de los datos personales*

[101] Constitución Política de los Estados Unidos Mexicanos. Artículo 16. 6ta Reforma. DOF 25 de junio de 2009.
[102] *Ley Federal de protección de datos personales en posesión de los particulares.* Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010.
[103] *Ley General de protección de datos personales en posesión de sujetos obligados*. Cámara de Diputados H. Congreso de la Unión. DOF 26-01-2017.

La finalidad de la LFPDPPP consiste en regular el tratamiento legítimo, controlado e informado de los datos personales del individuo, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa.[104] En esta sección, se analizarán los artículos de la esta ley que podrían ser aplicables en el caso del *microtargeting*, los derechos del titular al respecto y las herramientas que se le otorgan para el ejercicio de tales derechos.

En primer lugar, esta ley es aplicable para personas físicas y morales de carácter privado que lleven a cabo el tratamiento de datos personales.[105] De esta forma, Facebook, como persona moral de carácter privado que realiza tratamientos de datos personales, estaría dentro del ámbito protección de la ley. En este caso no existiría el problema que existe con la CCPA sobre el enfoque en comercialización de los datos y, por tanto, la cuestión sobre si Facebook realmente comercializa datos o únicamente publicidad. En cambio, la aplicación de la LFPDPPP únicamente requiere que exista tratamiento de datos, por lo que sólo es necesario que se obtengan y

[104] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 1º.
[105] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 2º.

almacenen los datos de los usuarios, lo cual es característica incuestionable de la actividad de Facebook.

Sin embargo, debido a que Facebook es una empresa trasnacional, con origen extranjero, se debe tomar en consideración el ámbito territorial de aplicación de la LFPDPPP. Con base en lo estipulado en el artículo 4 del Reglamento de la LFPDPPP, en principio, el contenido de esta ley no le sería aplicable, debido a que Facebook no está establecida en México.[106] El establecimiento se entiende como el local en donde se encuentre la administración principal del negocio. El establecimiento de Facebook se encuentra en Silicon Valley California. No obstante, en 2018, después de los eventos de Cambridge Analytica, el INAI emitió un comunicado en el que informó que iniciaría una investigación de las actividades de Facebook con respecto al tratamiento de los datos personales de sus usuarios mexicanos y si estos datos

[106] Artículo 4. El presente Reglamento será de aplicación obligatoria a todo tratamiento cuando: I. Sea efectuado en un establecimiento del responsable ubicado en territorio mexicano; II. Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano; III. El responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional, y IV. El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento (…).

habían sido tratados también por Cambridge Analytica.[107] Asimismo, el INAI comunicó que trabajaría en colaboración con autoridades británicas y estadounidenses. Parece que dicha investigación no tuvo seguimiento ya que no existía constancia del tratamiento de los datos de usuarios mexicanos. Sin embargo, incluso si hubieran tenido dicha constancia, debido al ámbito territorial de aplicación de la LFPDPPP, el INAI no hubiera podido sancionar efectivamente a Facebook.

Aunque, la LFPDPPP y, en su caso, el INAI, difícilmente sirven como mecanismos para regular la actividad de Facebook e imponer coactivamente la protección de los datos personales, el INAI sí podría procurar establecer un diálogo o colaboración con esta empresa a fin de que su política tome en cuenta los derechos de los titulares que se prevén en la legislación mexicana. Ahora bien, sería necesario cuestionar si, incluso en ese caso, la legislación mexicana sería eficiente para regular el *microtargeting* político en Facebook de forma que se prevengan o disminuyan sus posibles riesgos.

En la Ley se definen los datos personales como cualquier información concerniente a una persona física identificada o

[107] Comunicado, "EL INAI PROMOVERÁ COOPERACIÓN CON AUTORIDADES NACIONALES Y EXTRANJERAS POR CASO FACEBOOK-CAMBRIDGE ANALYTICA", INAI. 25 de marzo de 2018. http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-081-18.pdf.

identificable.[108] Asimismo, es importante identificar el concepto de datos personales sensibles.

> Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.[109]

Con este concepto, el presente trabajo afirma que algunos de los datos recopilados por Facebook, al ser utilizados para el *microtargeting* político, se configuran como datos personales sensibles. Como ya se estableció en el Capítulo I de este texto, el *microtargeting* político es una actividad que se realiza mediante la minería de datos, en este caso, que son recopilados por Facebook. Mediante la minería de datos, se segmentan grupos de individuos en consideración de características

[108] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 3 frac V.
[109] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 4 frac VI.

comunes, entre las que se encuentran origen racial o étnico, creencias filosóficas o morales, opiniones políticas, preferencias sexuales, entre otras, las cuales conforman información que aumenta significativamente la efectividad del *microtargeting* político.[110] Estas características usadas para segmentar población se obtienen fácilmente desde la actividad y los perfiles de usuarios de redes sociales como Facebook. Por tanto, los datos que recopila Facebook de sus usuarios sí pertenecen a la clasificación de datos personales sensibles, en conformidad con lo establecido en el artículo 3 fracción VI de la LFPDPPP.

Otro artículo que es relevante mencionar es el artículo 7, que establece lo siguiente:

> (…) En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados

[110] Sophie Boerman, "Political *Microtargeting*: Relationship Between Personalized Advertising on Facebook and Voters' Responses", Cyberpsychology, Behavior, and Social Networking, junio 2016.

> conforme a lo que acordaron las partes en los términos establecidos por esta Ley.[111]

En este artículo importa la precisión de lo que constituye una expectativa razonable de privacidad. Si se establece que la expectativa razonable tiene como base la confianza que deposita el usuario a Facebook, de que sus datos serán tratados conforme a lo que acordaron, en este caso en el aviso de privacidad, entonces la expectativa razonable se encuentra directamente relacionada con el consentimiento.

En el ámbito internacional, en Estados Unidos hay dos casos en los que la Corte Suprema ha establecido delimitaciones a la expectativa razonable de privacidad en comunicaciones.[112] En *Carpenter vs US*, se establece que no existe una expectativa de privacidad cuando el individuo entrega voluntariamente su información a un tercero.[113]

En México, no existen precedentes judiciales que ayuden a la interpretación del concepto. Sin embargo, el INAI relaciona el concepto de expectativa razonable con el principio de lealtad.

---

[111] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 7.

[112] United States v. Jones, 565 U.S. 400 (more) 132 S. Ct. 945; 181 L. Ed. 2d 911; 2012 U.S. LEXIS 1063; 80 U.S.L.W. 4125; Carpenter vs United States. 585 U.S., 138 S. Ct. 2206; 201 L. Ed. 2d 507.

[113] Carpenter vs United States. 585 U.S., 138 S. Ct. 2206; 201 L. Ed. 2d 507.

En sus guías sobre los principios de protección de datos personales, el INAI ubica el principio de lealtad al artículo 7 de la LFPDPPP. Define la lealtad como tratar los datos sin engaño y de la forma como lo hemos prometido o anunciado, incluso en circunstancias adversas. Su relación con la expectativa razonable tiene como base la imposibilidad del titular de controlar lo que el responsable hace con su información, el titular da su consentimiento de buena fe. Por tanto, el INAI ha definido la expectativa razonable como la confianza que el titular deposita en un tercero, respecto de que los datos personales proporcionados serán tratados conforme a lo acordado y a lo que se establece en la ley.[114]

A diferencia de Estados Unidos, en México, partiendo del artículo 7, se puede entender que, aunque el individuo entregue sus datos voluntariamente a un tercero -en este caso, Facebook- existe expectativa de privacidad en función de lo acordado por las partes. Existe expectativa de privacidad, pero esta será delimitada por lo que consienta el usuario de Facebook al aceptar el aviso de privacidad. De esta forma, tanto en México como en Estados Unidos, la expectativa razonable de privacidad, en cuanto a datos personales, tiene

[114] Guía de aplicación de protección de datos personales a la cobranzaextrajudicialinicio.ifai.org.mx/DocumentosdeInteres/Guía_Cobranza_Extrajudicial_INAI.pdf.

como base el consentimiento del titular de los datos. Sin embargo, como se argumentar más a fondo en el capítulo IV, de acuerdo con la postura defendida en la presente tesina, la expectativa razonable de privacidad no debería basarse puramente el consentimiento del individuo. Esto es así porque, aunque se considere la importancia de la autonomía de la voluntad de las partes, la recopilación de datos en redes sociales puede tener implicaciones de orden público.

En cuanto a los derechos con los que cuenta el titular de los datos, la LFPDPPP prevé los derechos ARCO (acceso, rectificación, cancelación y oposición). Estos derechos tienen similitudes a los que se otorgan al usuario en la CCPA que son los que Facebook afirma ya estar cumpliendo, especialmente, el derecho de cancelación. El titular tiene derecho a solicitar la cancelación de sus datos personales en posesión del responsable, para lo cual iniciará un período de bloqueo y posteriormente se realizará la supresión de los datos.[115]

Por último, es necesario mencionar las otras dos herramientas que la LFPDPPP otorga para su cumplimiento. Estas herramientas son dos procedimientos de derecho administrativo: la verificación, que tiene como finalidad

[115] Ley Federal de protección de datos personales en posesión de los particulares. Cámara de Diputados H. Congreso de la Unión. DOF 05-07-2010. Artículo 25.

vigilar el cumplimiento de la propia ley y de la normativa que de ésta derive, ya sea de oficio o a petición de parte, y la imposición de sanciones, por parte del INAI.

En conclusión, la legislación mexicana no contiene normas que sirvan para regular el *microtargeting* político en Facebook. En general, puede que la LFPDPPP sea deficiente en el sentido de, que faltan consideraciones especiales en cuanto a la actual forma de actividad de las plataformas digitales.

Capítulo IV: Regular a Facebook desde la protección a la privacidad y datos personales de sus usuarios; una alternativa para limitar los riesgos del *microtargeting* político

Esta tesina afirma que es necesario crear un marco normativo que regule eficientemente el *microtargeting* político en plataformas digitales como Facebook. No obstante, hasta ahora el enfoque principal de la discusión sobre la regulación de Facebook ha estado en imponer limitaciones al contenido de los anuncios políticos dentro de esta plataforma. De esta forma, los esfuerzos de promoción de regulación se enfocan en Facebook como medio de comunicación, en lugar de como empresa de tecnología, de manera tal que le sean aplicables las limitaciones que tienen otros medios de comunicación tradicionales en cuanto a publicidad política.

La presente tesina considera que sí se debe regular a Facebook (con respecto al *microtargeting*) como medio de comunicación, para disminuir el impacto de la promoción política en materia electoral. Sin embargo, propone que el primer paso debería consistir en regular específicamente al *microtargeting* político en plataformas digitales desde la materia de privacidad y protección de datos y, así, tener la posibilidad de reducir los riesgos generales que implica esta actividad en Facebook. Así, este último capítulo tiene los

siguientes propósitos: señalar los riesgos generales del *microtargeting* político en Facebook que justifican la necesidad de regulación; explicar por qué la actual forma de llevar a cabo el *microtargeting* político vulnera el derecho de privacidad; analizar por qué el enfoque actual en el consentimiento que actualmente adopta la legislación de protección de datos es ineficiente para regular el *microtargeting* político; y, por último, plantear posibles aproximaciones y propuestas para regular esta actividad desde el ámbito de privacidad y datos personales.

I. Los riesgos del microtargeting político en Facebook

Las diferencias más importantes entre el *microtargeting* simplemente comercial y el *microtargeting* político son, precisamente, las implicaciones y riesgos que cada uno tiene para los usuarios. El *microtargeting* político en Facebook necesita de pronta regulación puesto que conlleva mayores riesgos, entre los cuales se encuentra la posible manipulación del electorado.

Varios estudios han confirmado la efectividad del *microtargeting* político en redes sociales.[116] Lo importante a destacar es que esta efectividad no sería la misma si no se

[116] Entre ellos: Sophie Boerman; Gregg Murray, C. J Bennett.

tuviera acceso a los datos a los que se tienen acceso al comprar publicidad en Facebook. Así, el usuario promedio puede ser objeto de *microtargeting* político sin entender completamente lo invasivo que éste puede ser.

En primer lugar, como ya fue explicado en el inicio de esta tesina, para poder realizar el *microtargeting* político, primero se efectúa la actividad denominada minería de datos. Con esto, se utiliza la información de los usuarios de Facebook como sus "me gusta", lo que comparten, sus interacciones con sus contactos, entre otras cosas, para crear perfiles, saber cuáles son sus preferencias personales, orientación, clase socioeconómica, tendencias y opiniones en ámbitos políticos, etc.[117] Esto, por sí mismo, independientemente de la finalidad de la recolección de datos, ya genera riesgos para la privacidad del usuario.

Por otro lado, el riesgo que ha causado mayor preocupación es la capacidad del *microtargeting* de manipular decisiones políticas. Así, por ejemplo, en la campaña electoral estadounidense del 2016, se mostraron anuncios sólo a la población afroamericana en los que se recordaba que Hillary Clinton se había referido a los hombres afroamericanos como

[117] Sophie Boerman, "Political *Microtargeting*: Relationship Between Personalized Advertising on Facebook and Voters' Responses.

"súper predadores".[118] De la misma forma, una campaña política puede utilizar el *microtargeting* para inducir a cierto grupo de personas a no votar, si esto es conveniente para los intereses de quien dirige la campaña.

Asimismo, la distribución de información falsa aumenta su riesgo de desinformación con el *microtargeting*, puesto que incrementa la posibilidad de dirigirla a los segmentos que tengan más probabilidad de creer en dicha información. La efectividad de la distribución de *fake news* tiene relación con la efectividad del *microtargeting*.[119]

II. Análisis de las implicaciones del microtargeting político en la protección de la privacidad: ¿por qué la actividad actual debe considerarse como violatoria de los derechos humanos?

En los capítulos previos de la presente tesina se ha ido explicando por qué el *microtargeting* político vulnera la privacidad y la protección de información personal de los usuarios de Facebook. En esta sección se pretende sostener que, además de su impacto en esos dos ámbitos, ambos protegidos tanto en México como en EE.UU., el

[118] Frederik J. Zuiderveen, "Online Political Microtargeting: Promises and Threats for Democracy", Utrecht Law Review, vol 14 (2018). http://doi.org/10.18352/ulr.420
[119] *Ibid*

microtargeting político genera también vulneraciones de otros derechos fundamentales.

En primer lugar, hay que considerar la relación que tiene el derecho de privacidad y de protección de datos personales con otros derechos fundamentales, en este caso en concreto. Es clara la indivisibilidad existente entre el derecho de privacidad y el derecho de protección de datos personales.[120] La necesidad de regular el *microtargeting* político en Facebook se debe a la ineficacia de la legislación actual para proteger el manejo de los datos de los usuarios de Facebook cuando el *microtargeting* político tiene implicaciones en derechos fundamentales.

Es necesario tomar en cuenta que la recolección de información de usuarios de Facebook para el *microtargeting* político, convierte a esta actividad en una forma de comunicación política persuasiva de grandes grupos de personas, altamente efectiva.[121] Se pueden destacar tres

[120] La indivisibilidad de derechos se caracteriza por una fuerte interdependencia bidireccional entre dos derechos distintos. Cuando existe indivisibilidad, la vulneración de uno de los derechos, implica la vulneración del otro.

[121] Algunos estudios sobre la efectividad del *microtargeting* politico: Gregg R. Murray, Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies, ‚Journal of Political Marketing, (2010); International Institute for Democracy and Electoral Assistance, "Digital Microtargeting", Political Party Innovation Primer 1 (2018); Sophie Boerman, "Political Microtargeting: Relationship Between

factores que diferencian sustancialmente el impacto del *microtargeting* político en Facebook de cualquier otro tipo de *microtargeting*/*targeting*: a) acceso a datos personales sensibles para persuasión psicológica; b) alcance a grandes grupos de personas; c) su objeto/fin: político.

El *microtargeting* político en Facebook representa un medio efectivo de persuasión psicológica en masa. Ya se han realizado estudios que confirman que, con la tecnología actual, es posible procesar información anónima, como "me gustas", *clicks* en publicidad, entre otros, para construir perfiles psicológicos significativamente más precisos, que incluyen información como preferencias sexuales, opiniones políticas, condición social. [122] Se adaptan las formas comunicación persuasiva a los perfiles psicológicos creados con estos datos con el objeto de influenciar el comportamiento y las decisiones de las personas, de forma que se beneficien ciertos intereses políticos. Es clara entonces, la necesidad de evaluar la potencial vulneración que esta práctica tiene sobre el derecho fundamental a la autonomía.

Ahora bien, a partir del 2018 con el caso de Cambridge Analytica, se demostró cómo la persuasión mediante

---

Personalized Advertising on Facebook and Voters' Responses", Cyberpsychology, Behavior, and Social Networking, junio 2016.

[122]S. C. Matz et.al, "Psychological targeting as an effective approach to digital mass persuasion", Columbia University (2017).

microtargeting político en una red social puede influenciar la ideología política al grado de que exista una influencia considerable en las decisiones electorales de los individuos. El *microtargeting* político en Facebook no debe ser regulado únicamente por su impacto en materia de protección de datos personales, sino también por su impacto en materia electoral.

Desde antes de su éxito en plataformas de redes sociales, el *microtargeting* político se utilizaba como forma de propaganda política para elecciones y tenía el objetivo de ser persuasivo en favor de una campaña política. Con su inclusión en redes sociales, el *microtargeting* político no sólo es una forma de comunicación y propaganda política en medios normales, sino también una técnica que utiliza la información de los usuarios con el objeto de manipular sus decisiones e ideologías efectivamente, en favor de un interés o campaña política.[123] La persuasión efectiva del voto por medio de una actividad que obtiene datos personales e incluso sensibles del electorado, en consecución de un interés o partido político,

[123] Ya existen estudios que buscan confirmar la efectividad de *microtargeting* político en Facebook para interferir en las decisiones electorales de las personas, incluyendo incentivarlos a no votar como medida estratégica para incrementar las posibilidades de un partido o campaña política: Sophie Boerman, "Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses", Cyberpsychology, Behavior, and Social Networking, junio 2016; S. C. Matz et.al, "Psychological targeting as an effective approach to digital mass persuasion", Columbia University (2017).

claramente interfiere con los derechos políticos considerados esenciales para el funcionamiento de países democráticos -como Estados Unidos y México-.

En este sentido, Facebook, incluso cuando es una compañía particular, no debería tener la capacidad de autorregular actividades internas que tienen implicaciones de interés público al vulnerar el derecho a la privacidad, en su sentido de no interferencia del Estado en las decisiones privadas de los individuos. Al interferir en estas decisiones, también se vulnera la autonomía y, la parte que la autonomía tiene en los derechos políticos de los ciudadanos.

III. Menos responsabilidad para los usuarios, más responsabilidad para las plataformas digitales: ¿por qué el enfoque actual en el consentimiento del usuario es insuficiente?

Ya planteada la necesidad de regular el *microtargeting* político en Facebook, esta tesina sostiene que, ya que esta necesidad se justifica con la vulneración del derecho a la privacidad y autonomía, se debe empezar por regular dicha actividad desde la materia de datos personales. Sin embargo, en esta sección se abordará que uno de los problemas principales de las herramientas legales para proteger la privacidad y los datos personales de los usuarios de plataformas digitales es que

posiciona al consentimiento del titular como mecanismo prioritario para asegurar la protección de su información personal.

La mayor parte de los esfuerzos legislativos se concentran en aumentar el control que el usuario de las plataformas digitales tiene sobre sus datos. De esta forma, la legislación actual parece basarse en la presuposición de que aumentar el control del usuario sobre sus datos individuales representa una limitación efectiva al tratamiento, transferencias y potenciales abusos que una plataforma como Facebook puede realizar. Sin embargo, el presente apartado mantiene que dicha presuposición tiene fallas sustanciales que, consecuentemente, derivan en una ineficacia de la legislación y regulación aplicable a Facebook para proteger adecuadamente a los usuarios de potenciales vulneraciones a sus derechos.

El manejo de la información personal y la política de privacidad de Facebook dependen del consentimiento explícito de los usuarios. Este consentimiento lo manifiestan por medio de la aceptación del aviso de privacidad. Es el consentimiento de los usuarios a la política de privacidad de Facebook lo que confiere validez legal a toda la actividad que realiza con los datos que recopila.[124] El consentimiento es un

[124] Artículo 6, GDPR.

punto central en las legislaciones sobre protección de datos personales. En la CCPA el consentimiento no se encuentra definido explícitamente; sin embargo, parece funcionar de manera similar al concepto de consentimiento en el GDPR.[125] La legislación europea plantea cuatro requisitos esenciales para que se considere el consentimiento sea válido: 1) libre; 2) informado; 3) específico; 4) sin ambigüedades. En el GDPR el consentimiento está planteado como una de las formas con las que se puede realizar procesamientos de datos de forma legal.[126]

Existen varios estudios que demuestran que los usuarios de Facebook, incluso los que tienen preocupaciones sobre su privacidad, revelan cantidades significativas de información en redes sociales.[127] El problema más común en relación con el consentimiento es un fenómeno conocido como la "paradoja

[125] El consentimiento consiste en cualquier indicación libremente dada, específica, informada y sin ambigüedades de los deseos del interesado por medio de la cual, mediante una declaración o una acción afirmativa clara, acepta el procesamiento de datos personales relacionados con él o ella, puede ser una declaración oral o escrita, incluyendo de forma electrónica. Recital 32 GDPR. Conditions for consent. Revisado 25 de abril del 2020. https://gdpr.eu/Recital-32-Conditions-for-consent/.
[126] Artículo 7, GDPR.
[127] Algunos los principales estudios al respecto son: Acquisti & Gross (2006); Stutzman, Gross & Acquisti (2012); Raynes-Goldie's (2010); Boyd & Marwick (2011).

de la privacidad".[128] La paradoja de privacidad analiza dos tipos de aproximaciones para un consentimiento informado. La primera aproximación consiste en que el aviso de privacidad informe de manera extensa y detallada la política de privacidad de la empresa o servicio, y los usos y tratamientos que se les darán a los datos de los usuarios. El problema con la primera aproximación es que un aviso exhaustivo es necesariamente técnico, por lo que los usuarios tendrían dificultad para entender las implicaciones y los alcances de lo que están leyendo y, por consiguiente, de lo que están consintiendo.

Esto conduce a la segunda aproximación, la cual consiste en que el aviso de privacidad sea más general y corto, con el propósito de hacerlo más sencillo y entendible para todos los usuarios. No obstante, un aviso de privacidad general es omiso de detalles que pueden resultar ser importantes para el entendimiento de las implicaciones del consentimiento, así como también puede tender más a encuadres o *framings*[129] de la información, de la forma que sea más conveniente para la

[128] Patricia Norberg, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", The Journal of Consumer Affairs, 2007. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[129] framing consiste en que en la descripción de cualquier problema se puede poner énfasis en ciertas consideraciones lo que en consecuencia causa que los individuos se concentren en estas para construir sus opiniones. Robert Entman, "Framing: Toward Clarification of a Fractured Paradigm", Jounral of Communication, vol 43 (2007).

empresa. Esto último puede ser ejemplificado con el modo en el que Facebook presenta la información sobre los anuncios personalizados en su plataforma.

Facebook ofrece opciones en su menú para que el usuario pueda tener información sobre cómo funciona su sistema de publicidad y anuncios segmentados. Para esto, se selecciona la opción de anunciantes y negocios en la que se despliega la lista de anunciantes que "subieron una lista con tu información y la usaron para segmentar sus anuncios". Junto con la lista, Facebook incluye un cuadro de texto en el que pretende explicar cómo se suben las listas con la información del usuario a la plataforma para después segmentar los anuncios, en este cuadro se estipula lo siguiente: "Estos anunciantes publicaron un anuncio en los últimos siete días usando una lista subida a Facebook que incluye tu información, por lo general, una dirección de correo electrónico o un número de teléfono. Facebook asoció la información subida con tu perfil, sin revelar tu identidad al anunciante".[130] Asimismo, en la explicación que presenta sobre cómo se tratan los datos e información compartida con socios externos, Facebook establece que no vende datos y que impone "estrictas

[130] Esto se encuentra dentro de la configuración de privacidad a la que se tiene acceso por medio de una cuenta de Facebook.

restricciones” en cuanto a la manera en que los socios pueden usar y divulgar los datos.

La información brindada por Facebook parece ser muy clara y concisa; sin embargo, no entra en detalles sobre las supuestas restricciones que se imponen a los socios externos. Además, el encuadre de la información está hecho de manera que la impresión del usuario sobre compartir información con los socios externos para segmentar los anuncios parece una opción totalmente positiva. Si lo usuarios quisieran obtener información más detallada tendrían que invertir más tiempo e incluso llevar a cabo una investigación por fuera de la plataforma de Facebook.

Sin embargo, es ineficiente enfocarse en si los usuarios de Facebook o cualquier otra red social no leen o no entienden completamente el aviso de privacidad. Este enfoque dirige los esfuerzos de la regulación para la protección de sus derechos a la privacidad y a la protección de datos personales, únicamente al consentimiento.

La presente tesina sostiene que, si la regulación y limitaciones impuestas a Facebook dependen casi enteramente del consentimiento y control del usuario -como pasa con la regulación californiana y la mexicana-, el resultado es, necesariamente, una falta de protección debida a los derechos

de protección de datos personales y privacidad. El consentimiento individual de los usuarios no limita la acción de Facebook con respecto a sus datos e información personal. El presente texto encuentra que esto se debe principalmente a las siguientes razones: a) información asimétrica en el consentimiento; b) falta de poder de negociación; c) análisis de estrategia dominante del consumidor tendiente a consentir.

a) Primeramente, en la relación entre Facebook y el individuo la información va a ser asimétrica. Es decir que, al pactar la política de privacidad Facebook siempre contará con mayor información que el individuo que tiene que tomar la decisión de otorgar o no su consentimiento. La paradoja de privacidad explicada previamente entra en esta categoría. La realidad es que por más información que se pueda brindar en la política de privacidad, entender completamente las implicaciones de técnicas como la minería de datos, *big data*, *profiling*, *microtargeting*, entre otras, conlleva tener cierto conocimiento especializado en la materia. Asimismo, los incentivos para que el usuario consiga información externa antes de consentir son muy bajos, puesto que esto implica costos altos de tiempo. De tal forma que la decisión racional para cualquier individuo sería consentir sólo con la información brindada por la plataforma, incluso cuando sea consciente del problema de

asimetría.[131] Por tanto, en la práctica, lo esperado es que los usuarios no tengan información completa al momento de dar su consentimiento. La confianza en las plataformas digitales tiene entonces un papel importante en este caso.

b) Ahora bien, incluso en el supuesto de que existiera información completa para ambas partes (Facebook y usuario), la regulación vigente parece no tomar en consideración los factores que llevan al usuario a tomar la decisión de consentir. Facebook y, en general, las plataformas de redes sociales funcionan de tal manera que, incluso con una política de privacidad potencialmente invasiva, el usuario tiende a consentir.[132] Frente a la decisión de consentir o no consentir el aviso de privacidad de Facebook, los usuarios se encuentran en una desventaja derivada de una posición vertical en el poder de negociación. El individuo como usuario de las plataformas de redes sociales, no tiene poder de negociación en cuanto a los términos del aviso de privacidad. La idea de que cada usuario de redes sociales existentes pudiera negociar con la plataforma los términos y condiciones del aviso de privacidad

[131]Hermstrüwer, Yoan, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data", Journal of Intellectual Property, Information Technology and E-Commerce Law, 2017, https://www.jipitec.eu/issues/jipitec-8-1-2017/4529/#ftn.N1005B
[132] *Ibid*

de acuerdo con su expectativa individual de cómo se manejen sus datos sería prácticamente imposible.[133]

De esta forma, el consentimiento inicial implica que el usuario únicamente pueda elegir entre consentir todo el aviso de privacidad o no consentir en lo absoluto. Aquí es relevante considerar que, si se toma la opción de no consentir, la pérdida sería no formar parte de la red social. En cuanto a los servicios de redes sociales, Facebook tiene una clara ventaja competitiva después de sus adquisiciones estratégicas de los otros dos servicios de redes sociales de mayor presencia en México y Estados Unidos: Instagram y WhatsApp. Facebook tiene acceso no sólo a los datos de usuarios de su propia plataforma si no a los datos de estas otras dos redes sociales, y aplica una política de privacidad y protección del usuario similar, especialmente con Instagram.

El usuario que no quiera consentir a los términos de Facebook estaría renunciando a formar parte de estas tres opciones de redes sociales. La relevancia de las redes sociales en el mundo actual, y en consideración de que estos cuentan como servicios de comunicación digital, son factores determinantes para que los individuos den su consentimiento a compañías como

[133] No obstante, es importante destacar la opción de la privacidad por diseño que sugiere que cualquier herramienta tecnológica ya considere la privacidad de los usuarios desde su implementación.

Facebook, incluso aunque exista una completa desconfianza con respecto a la protección de sus datos y privacidad.

c) Finalmente, en consideración del problema de información asimétrica y de la ausencia de poder de negociación por parte del usuario, es necesario tomar en cuenta que, desde un análisis racional de toma de decisiones, la estrategia dominante del individuo es otorgar su consentimiento. La valoración del costo de aceptar el aviso de privacidad no será tan alta para una persona con una expectativa de privacidad promedio. Por el contrario, el negar el consentimiento desde el aviso de privacidad significa la exclusión de redes sociales como Facebook e Instagram. Esto, para un individuo racional, significaría un costo más alto que aceptar una política de privacidad potencialmente abusiva de sus datos personales y privacidad. Para entender por qué pasa esto es necesario destacar algunos factores que influyen en las posibles estrategias de decisión.[134]

En primer lugar, el mercado de servicios de comunicación y red social se caracteriza por presentar un efecto o externalidad

[134] El análisis económico y de teoría de juegos del comportamiento del usuario de Facebook ya se ha realizado en: Hermstrüwer, Yoan, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data", Journal of Intellectual Property, Information Technology and E-Commerce Law, 2017, https://www.jipitec.eu/issues/jipitec-8-1-2017/4529/#ftn.N1005B

de red.[135] En las externalidades de red el incremento en el valor que un consumidor le da al producto/servicio es dependiente del número de consumidores que ese servicio tenga.[136] Las redes sociales funcionan con externalidades de red de tal manera que, el individuo valora más una plataforma cuando ésta tiene un mayor número de usuarios. Por tanto, la posición de Facebook frente a posibles plataformas competidoras es claramente ventajosa, también considerando que Instagram y WhatsApp forman parte de Facebook.[137] En un caso en el que a un individuo interesado en unirse a una red social se le presente la opción de unirse a las plataformas de Facebook con menos protección a su privacidad, o unirse a una plataforma competidora con menos usuarios, pero mayor protección a su privacidad, la estrategia esperada será que elija unirse a Facebook. Así, considerando también los otros factores ya explicados de información asimétrica y nulo poder de

[135] La condición de externalidad de red en Facebook ha sido confirmada por distintas comisiones de competencia económica en diversos casos: Comisión Europea. Case No comp/m.7217 - facebook/ whatsapp; ACCC. Dominancia de mercado en plataformas Digitales. Facebook/Google.

[136] J.I López, "Externalidades de red en la economía digital: una revisión teórica", Universidad Complutense de Madrid, 2006, https://dialnet.unirioja.es/servlet/articulo?codigo=2199847

[137] Juan Mejía, "Estadísticas de redes sociales 2020: usuarios de facebook, instagram, youtube, linkedin, twitter, tiktok y otros", Marketing digital y transformación digital, 26 de febrero de 2020. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/

negociación, la estrategia dominante de una persona sería otorgar su consentimiento a Facebook, a pesar de que las actividades de este puedan resultar en vulneraciones a sus derechos de privacidad y protección de datos personales. Consecuentemente, Facebook, como oferente de servicios de comunicación y red social, no tiene incentivos de brindar una protección alta a la privacidad y datos personales cuando su mayor limitante sea el consentimiento de los usuarios.

Todo lo anterior deriva en la necesidad de cuestionar la eficacia de concentrar las legislaciones y la regulación aplicable a redes sociales como una cuestión de puro consentimiento, ya sea inicial o posterior al aviso de privacidad, que se manifiesta en los controles sobre los datos como el *opt-out* que introduce la CCPA. Mientras que es necesario asegurar que el individuo pueda tener un mayor control sobre los datos que mantiene en plataformas de redes sociales, esto no es suficiente para regular eficazmente las redes sociales de forma que se proteja a los usuarios de posibles vulneraciones a sus derechos.

Asimismo, con respecto al *microtargeting* político, hace falta que en el proceso de creación de herramientas legales para regularlo se consideren también otros factores que influyen en la decisión individual y factores del mercado que le dan a Facebook y a otras plataformas digitales un poder sustancial,

con capacidad de abusar de su tecnología y acceso significativo a datos e información personal. El *microtargeting* político es un ejemplo de una actividad realizada en Facebook, con implicaciones en derechos fundamentales de los usuarios y que, sin embargo, se encuentra esencialmente monitoreada, vigilada y limitada por el consentimiento y control del usuario.

IV. Áreas de oportunidad y propuestas para una regulación de Facebook en materia de privacidad y datos personales

En esta sección se abordarán algunas alternativas y propuestas para regular el *microtargeting* político en Facebook desde la protección de la privacidad y datos personales de las personas. En este sentido, primero se explicará por qué la presente tesina no considera la posibilidad de prohibir totalmente la realización de *microtargeting* político en redes sociales. Algunas plataformas ya funcionan sin algún tipo de publicidad política, como Twitter. Sin embargo, prohibir el *microtargeting* político en redes sociales no es la alternativa más viable ni la más eficiente.

En primer lugar, una regulación que prohíba una forma de comunicación en plataformas digitales tiene la potencialidad de vulnerar la libertad de expresión. La libertad de expresión está protegida por las constituciones de México y de EE.UU. En México, el derecho a la libertad de expresión tiene tres funciones: protección del derecho individual, función democrática y función instrumental. Este se encuentra contenido en la CPEUM, en su artículo 6° el cual establece que "la manifestación de las ideas no será objeto de ninguna

inquisición judicial o administrativa", es decir, no puede ser limitada arbitrariamente.[138]

Asimismo, el artículo 7° constitucional establece como parte del alcance del derecho, en su sentido negativo que: "es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio".[139] Por otro lado, en México también tienen protección constitucional los tratados internacionales, que establecen que "el derecho a la libertad de expresión comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección y no ser molestados arbitrariamente a causa de ello."[140]

La extensión de la protección del derecho establece las limitaciones legales en el ejercicio del derecho. La constitución establece el derecho a la libre expresión sólo podrá limitarse cuando ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público. En este sentido, sí existe la posibilidad de poder

[138] Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos. Artículo 6.
[139] Congreso de la Unión. Constitución Política de los Estados Unidos Mexicanos. Artículo 7.
[140] Declaración Universal de Derechos Humanos (Art. 19), el Pacto de derechos civiles y políticos (Art. 19), así como la Convención americana de Derechos Humanos "Pacto de San José" (Art. 13)

alegar la prohibición del *microtargeting* político en tanto atenta en contra de la vida privada de los individuos que sean usuarios de Facebook. Sin embargo, requeriría de un análisis y discusión de proporcionalidad.

En EE.UU. la libertad de expresión se encuentra protegida por la 1ra Enmienda en la que se establece que el gobierno no adoptará ley alguna que coarte la libertad de palabra.[141] Por el contexto social y político de EE.UU., así como antecedentes judiciales en cuanto a libertad de expresión, la prohibición del *microtargeting* político resulta ser una vía sumamente complicada para la regulación de Facebook.

Por otro lado, la presente tesina sostiene que, como cualquier avance tecnológico, esta actividad, con la regulación adecuada, puede también tener efectos positivos. Por ejemplo, el *microtargeting* puede servir para inducir a las personas a votar, y disminuir la cantidad de personas que se abstienen de participar en elecciones, o podría utilizarse de forma que las personas que usualmente no participan en la vida política tuvieran interés, al adecuar sus cuentas en redes sociales como

[141] Jasper, Margaret C, "The Law of Speech and the First Amendment", Oceana Publications (1999).

Facebook de tal forma que los temas que más aparezcan sean aquellos en los que realmente tengan interés.[142]

No obstante, independientemente de los efectos positivos o negativos que pueda tener el *microtargeting* político, no puede ser ignorado que la forma en la que se realiza actualmente vulnera la privacidad de los usuarios. Tampoco deben perderse de vista los riesgos de desinformación que el microtargeting político conlleva al incluir y promocionar información política falsa. De esta forma, la presente tesina afirma que las áreas de oportunidad para la regulación de Facebook se encuentran en la protección de la privacidad y que la legislación debe cambiar para que se impongan mayores límites a la capacidad de tratamiento y transferencias que tiene Facebook sobre los datos de sus usuarios.

Para este tipo de regulación, la presente tesina propone como una de las limitaciones que se deben hacer a Facebook, el limitar la segmentación del *microtargeting* político. Es decir, que se limiten las categorías que Facebook puede segmentar para mostrar anuncios específicos, a categorías que no sean tan invasivas de la información personal sensible. Segmentaciones como la mencionada previamente, en la que se mostraron

[142] Frederik J. Zuiderveen, "Online Political Microtargeting: Promises and Threats for Democracy", Utrecht Law Review, vol 14 (2018). http://doi.org/10.18352/ulr.420

anuncios específicos solamente a población afroamericana, o como la que se realiza en función de datos que podrían ser calificados como datos sensibles, incluso cuando sean anónimos, no deberían estar permitidas.

En este sentido, se propone que la segmentación se limite a categorías más generales como la edad, el género y la localización, o, por otro lado, realizar mayor investigación para definir las categorías que serían aceptables en un ámbito político. Facebook ya ha limitado su *microtargeting* en otros ámbitos distintos al político, cuando limitó a ciertos anunciantes la posibilidad de segmentar por edad, afinidad multicultural, código postal, entre otras categorías.[143]

Asimismo, esta tesina considera la limitación de categorías de información de los usuarios que puede transferir a agentes políticos, incluso aunque estos no sean identificables con cuentas específicas. De la misma forma, todas las limitaciones y regulación del manejo de información de usuarios de Facebook, en cuanto al *microtargeting* político, podría requerir la realización previa de evaluaciones de impacto en derechos humanos.

Finalmente, se considera la privacidad por diseño. La privacidad por diseño se refiere la creación de nuevas

[143] Ibid

tecnologías que ya consideren la protección de los datos personales de las personas desde el momento de su diseño.[144] Esta es una alternativa necesaria y podría ser aplicable para nuevas herramientas o actividades que surjan en plataformas digitales.

[144] Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Ontario, Canada, Privacy by Design: The 7 foundational principles. 2007.

Conclusiones

El propósito de esta tesina consistió en analizar el *microtargeting* político en Facebook como una actividad potencialmente vulneradora de la privacidad y la protección de datos personales de los usuarios de redes sociales. Después de haber estudiado la protección del derecho de privacidad y del derecho de protección de datos personales en EE.UU. y México, la presente tesina concluye que, a pesar de las diferencias normativas, el *microtargeting* político sí vulnera estos derechos en ambos países y, por tanto, es necesario regular dicha actividad. Se realizó un análisis de la legislación y regulación vigente en los dos países mencionados, para determinar si éstos regulan el *microtargeting* político eficazmente, protegiendo la privacidad e información personal de los individuos.

La presente tesina sostiene que ambas legislaciones son deficientes para regular el *microtargeting* político, pero en diferentes sentidos. En México, existe una falta de adecuación de la legislación en materia de protección de datos personales, a la actividad de las plataformas digitales. Aunque en México el *microtargeting* político no representa los mismos riesgos que en EE.UU., la legislación debe tomar lo sucedido en ese país, para prever los potenciales riesgos de dejar a plataformas como Facebook sin algún tipo de regulación.

Por su parte, EE.UU. implementó la CCPA, con la que se pretende otorgar mayor protección de la privacidad de los consumidores, al reconocerles derechos sobre su información personal. Sin embargo, la CCPA carece de especialización en el tema particular del manejo de información personal de los usuarios de Facebook. De esta forma, la legislación no considera las características de la actividad de *microtargeting* político y, por tanto, es deficiente para regular y prevenir los riesgos que esta actividad conlleva.

Del análisis realizado a lo largo de la tesina se puede concluir que esto se debe al énfasis en la autorregulación de las plataformas digitales de redes sociales. Por lo tanto, se considera que hace falta una mayor intervención del aparato legislativo y regulatorio estatal frente a las nuevas tecnologías y las nuevas externalidades en los mercados digitales. Asimismo, la hasta ahora escasa intervención legislativa presenta diversos problemas que obstaculizan una protección eficaz del usuario de Facebook y resultan inaplicables para la práctica real de la minería de datos y posterior, *microtargeting* político en Facebook. Por tanto, este texto propone que, debido a los efectos e implicaciones del *microtargeting* político y otras prácticas de Facebook con respecto a los datos personales de sus usuarios, se requiere una legislación más rígida,

actualizada y especializada para protección de datos personales y privacidad de los usuarios de redes sociales.

Una regulación eficiente para plataformas de redes sociales implica varios retos a futuro. Es importante que tanto el legislador como las instituciones regulatorias facultadas en la materia, consideren la dicotomía de los dos posibles errores regulatorios aplicados a plataformas digitales. Por un lado, el error tipo 1, ante el cual nos encontramos actualmente, se trata de la subregulación de la materia, dándole prioridad a la autorregulación, con la menor intervención estatal posible. Este error tiene como consecuencia que existan ciertos daños que no sean corregidos ni internalizados. En el caso de las transferencias de datos e información de los usuarios de Facebook, los daños los asumen los usuarios. Por otro lado, el error tipo 2 sería una sobrerregulación, un abuso de la intervención estatal en la materia. Este es el tipo de error que se debe evitar en un futuro; Sin embargo, no debe implicar que se mantenga el tipo de error 1.

Las implicaciones que tiene el *microtargeting* político en derechos fundamentales como el derecho de privacidad, hacen necesario considerarlas como una justificación para impulsar una mayor regulación en la materia. La presente tesina propone como primer paso regular la actividad desde la protección de los datos personales. Sin embargo, para lograr

una regulación eficiente, se requiere de mucha más investigación y especialización al respecto. El *microtargeting* político, así como toda actividad de análisis y minería de datos en plataformas digitales, es un tema en el que todavía hace falta continuar explorando sobre su impacto en la vida cotidiana, su importancia para el funcionamiento de la sociedad actual y, consecuentemente, sus implicaciones jurídicas.

Bibliografía

ACC. Digital Platforms Inquiry: Final Report. (Australia: Junio 2019).

Acta de la Comisión Federal de Comercio. 15 U.S.C. 41 et seq. Estados Unidos de América, 1914.

Acta de privacidad del consumidor de California AB-37. Código Civil de California sec. 1798.100. Estado de California, Estados Unidos de América, 2018.

Bennet, Colin. "Regulating privacy: data protection and public policy in Europe and the United States". *Cornell University Press* (1992), 68-69.

Bennett, C. J. "Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?". *International Data Privacy Law* vol 6/4., (November 2016). https://doi.org/10.1093/idpl/ipw021

Boerman, Sophie. "Political Microtargeting: Relationship Between Personalized Advertising on Facebook and Voters' Responses", *Cyberpsychology, Behavior, and Social Networking* 19/6 (2016): 367-372. Doi: 10.1089/cyber.2015.0652

California Privacy Consumer Act (CCPA): Background on the CCPA & the Rulemaking Process. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa.

Doug Walker, Edward L. Nowlin. “Data-Driven Precision and Selectiveness in Political Campaign Fundraising”. *Journal of Political Marketing* (2018). DOI: 10.1080/15377857.2018.1457590

Entman, Robert. “Framing: Toward Clarification of a Fractured Paradigm”. *Journal of Communication*, vol 43 (2007). https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Hermstrüwer, Yoan. “Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data.” *Journal of Intellectual Property* (2017) https://www.jipitec.eu/issues/jipitec-8-1 2017/4529/#ftn.N1005B

International Institute for Democracy and Electoral Assistance. *Digital Microtargeting, Political Party Innovation Primer 1* (2018).

Ley Federal sobre Protección de Datos Personales en posesión de particulares. Cámara de Diputados H. Congreso de la Unión. México, 5 de julio del 2010.

Ley General de protección de datos personales en posesión de sujetos obligados. Cámara de Diputados H. Congreso de la Unión. México, 26 de enero del 2017.

Lineamientos Generales de Protección de Datos Personales para el Sector Público. H. Congreso de la Unión. México, 26 de enero del 2018.

López, I. "Externalidades de red en la economía digital: una revisión teórica". *Universidad Complutense de Madrid* (2006) https://dialnet.unirioja.es/servlet/articulo?codigo=2199847

Mejía, Juan. *Estadísticas de redes sociales 2020: usuarios de facebook, instagram, youtube, linkedin, twitter, tiktok y otros.* Marketing digital y transformación digital, 26 de febrero de 2020. https://www.juancmejia.com/marketing-digital/estadisticas-de-redes-sociales-usuarios-de-facebook-instagram-linkedin-twitter-whatsapp-y-otros-infografia/

Murray, Gregg. "Microtargeting and Electorate Segmentation: Data Mining the American National Election Studies". *Journal of Political Marketing* (2010): 143-166. 10.1080/15377857.2010.497732

Norberg, Patricia. “Disclosure Intentions versus Behaviors”. *The Journal of Consumer Affairs* (2007) https://doi.org/10.1111/j.1745-6606.2006.00070.x

Reilly, Robert. “Conceptual foundations of privacy: Looking Backward Before Stepping Forward”. *The Richmond Journal of Law and Technology* vol 6., 2da ed (1999). https://core.ac.uk/download/pdf/232774445.pdf

S. C. Matz et.al. “Psychological targeting as an effective approach to digital mass persuasion”. *Columbia University* (2017).

Warren, Samuel y Brandeis, Louis. “The Right to Privacy”. *Harvard Law Review* vol IV., (1890).

Zuiderveen Borgesius, Frederik and Moeller et al. “Online Political Microtargeting: Promises and Threats for Democracy”. *Utrecht Law Review* vol. 14, no. 1. (2018) http://doi.org/10.18352/ulr.420