Análisis comparativo aspectos de la política de datos de Facebook versus cumplimiento regulatorio sobre los datos personales[1]δ.

Analysis of aspects of Facebook's data policy versus regulatory compliance about personal data.

Marisol Martínez Arenas[1]*
Santiago Grajales [2]**

Resumen

El uso frecuente de redes sociales en la actualidad ha ocasionado que plataformas como Facebook, se conviertan en un medio indispensable de comunicación entre las personas, por esta razón se analiza la forma mediante la cual estas plataformas recopilan la información y secuencialmente se identifica el uso y tratamiento de estos datos personales, teniendo en cuenta ambas premisas se investiga las normativas internacionales que regulan el actuar de las redes sociales, que al ser comparadas con situaciones polémicas en cuanto a tratamiento de información en las que se ha visto inmersa Facebook permite determinar el cumplimiento normativo de esta red social, todo esto a través del análisis de una recopilación bibliográfica que abre el horizonte de conocimiento en cuanto al funcionamiento de la plataforma, este análisis también ayudó a determinar que en las políticas de datos de Facebook las formas de recopilación y uso de información van orientadas a beneficiar al usuario, pero los antecedentes dieron a conocer que el mayor beneficio lo obtiene la compañía, se determina entonces que el papel que juega el usuario y sus datos personales en este escenario va más enfocado a ser el producto representativo de un servicio que se ofrece de forma gratuita.

Palabras clave: Redes sociales, Facebook, privacidad, protección de datos, normas internacionales, usuarios, información.

Abstract

The frequent use of social networks today has caused that platforms such as Facebook become an indispensable means of communication between people, for this reason the way in which these platforms collect information is analyzed and treatment and use of these personal data, taking into account the premises, the international norms that regulate the act of social networks were investigated, that when compared to controversial situations regarding the treatment of information in which Facebook has been immersed, it allows determining the regulatory compliance of this social network, all this through the analysis of a bibliographic compilation that opens the horizon of knowledge regarding the operation of the platform, this analysis also helped to determine that in Facebook's data policies the forms of information collection and use are aimed at benefit the user, but the background revealed that the greatest benefit is obtained by the company, it is determined then that the role played by the user and their personal data in this scenario is more focused on being the representative product of a service that is offered for free.

Keywords: Social networks, Facebook, privacy, data protection, international standards, users, information.

[1δ] Este artículo es el resultado de Análisis comparativo aspectos de la política de datos de Facebook versus cumplimiento regulatorio sobre los datos personales

[2*]Profesional en criminalística. marisolmarar7@gmail.com
[3**]Administrador de sistemas informáticos. Auditor de Tecnología. CFA Cooperativa Financiera. sgrajalesa.sg@gmail.com

Introducción

A lo largo de la historia el hombre ha tenido la necesidad de comunicarse, y para satisfacer esta necesidad ha creado múltiples medios, desde los pictogramas en la prehistoria pasando por el telegrama, el teléfono y llegando a dar origen a los teléfonos inteligentes, que permiten a los seres humanos llevar la computadora permanentemente en sus bolsillos. Otro factor que facilitó las comunicaciones fueron las redes sociales que constituyen un medio fácil, eficiente y económico a la hora de comunicarse.

El uso de las redes sociales ha presentado un incremento exponencial en los últimos años, esto según el estudio realizado por la prestigiosa agencia de marketing y comunicación online 2.0 We are Social y la compañía creadora de la plataforma para la gestión de redes sociales Hootsuite, que indica que, al mes de enero de 2020, la cantidad de usuarios en redes sociales como: Facebook, Instagram, y WhatsApp presento el siguiente comportamiento:

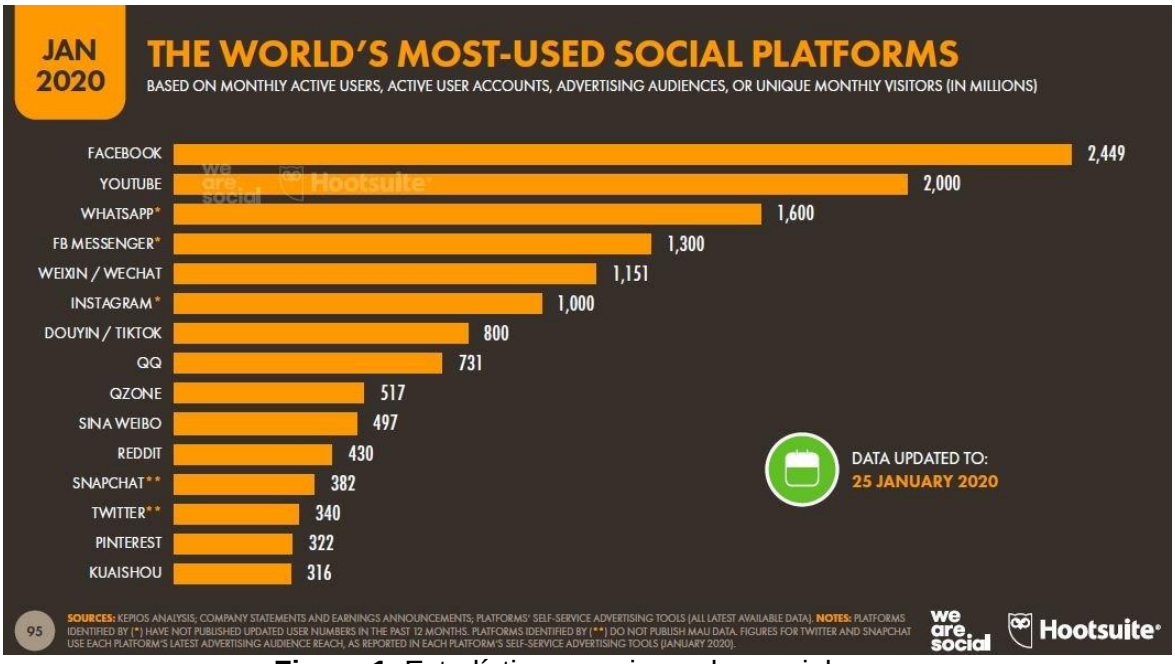

Figura 1. Estadística usuarios redes sociales
Fuente: Digital 2020 Global Digital Overview (KEMP, 2020)

Y es que la necesidad de interconexión, de comunicar acontecimientos de la vida cotidiana, conocer personas en otras latitudes, estar informados y hacer negocios, ha motivado a miles a crear perfiles en redes sociales, pero más allá de estas motivaciones es la necesidad de adquirir una identidad digital y expresar sus emociones a través de diversas opciones que dichas redes ponen a su disposición a un solo clic.

Para poder construir esta identidad digital, el usuario de manera voluntaria debe aceptar los términos y condiciones de un contrato on-line o contratos denominados click-wrap los cuales según (Vaca Cedeño & Ibarra Segovia, 2019) se destacan por una forma especial de manifestar el consentimiento: a través del clic del aceptante, para esto al momento del registro se deben suministrar datos como: nombre, apellido, numero de celular, correo electrónico, fecha de nacimiento y sexo, para posteriormente clicar la palabra “Registrarte” y con ello aceptar las condiciones, políticas de datos y cookies que tenga definido el proveedor de dicha red social.

Surge entonces una de las primeras preguntas que motivó esta revisión bibliográfica, ¿dónde va a parar esta información?, pues la respuesta es casi obvia, estos grandes volúmenes de información reposan en los servidores propiedad de la compañía responsable de la red social, para el caso de este estudio nos centraremos en Facebook.

Hasta este momento se puede percibir que la tecnología y sobre todo las redes sociales han facilitado nuestras vidas al permitirnos estas interconectados de manera continua y al alcance de nuestras manos a través de Internet, además el usuario tiene un parte de tranquilidad por el hecho de que Facebook cuenta con una serie de políticas, que harían pensar que la información se encuentra protegida de manera adecuada, entonces surge un segundo interrogante, ¿Cuál es el tratamiento que da Facebook a la información que recopila de sus usuarios?, y tal como ellos lo describen en sus políticas de datos la respuesta sería: usamos la información que tenemos para proporcionar nuestros productos, así como para personalizar las funciones y el contenido (incluidos la sección de noticias, el feed de Instagram, Instagram Stories y los anuncios) y hacerte sugerencias (como grupos o eventos que pueden interesarte o temas que quizás quieras seguir) tanto dentro como fuera de nuestros productos (Política de datos, 2018).

En este punto se comienza a generar incertidumbre debido a la controversia en la que se ha visto envuelta la compañía, por la supuesta intervención en asuntos diplomáticos de naciones como: Estados Unidos y Reino unido, específicamente en una vulneración de datos muy nombrada en los últimos años, como es el caso de Cambridge Analytica en donde esta firma de análisis de datos que trabajó con el equipo electoral de Donald Trump y la campaña ganadora del Brexit recolectó millones de perfiles de votantes estadounidenses en Facebook , en una de las mayores violaciones de datos del gigante tecnológico, y los utilizó para crear un poderoso programa de software para predecir e influir en las elecciones en la urna (Graham-Harrison & Cadwalladr, 2018).

Se convierte entonces en un menester del equipo de trabajo, cuestionar el cumplimiento de Facebook con relación a normas internacionales aplicables a redes sociales que buscan salvaguardar la privacidad de la información, y para lograr este objetivo se van a explorar aquellas leyes que han sido definidas a nivel mundial para regular el ámbito de las redes sociales, posteriormente se evalúan los antecedentes que tiene la red social en cuanto a conflictos que apunten a la vulneración de datos, para rematar con el análisis de las formas mediante las cuales se recopila la información y el tratamiento que se le da a la misma cuando ya se encuentra en poder de Facebook.

De esta manera, se va a explorar cómo la literatura se ha pronunciado con respecto a este tema y sobre todo intentar mostrar desde el conocimiento que las personas deben crear conciencia y responsabilidad para el uso de este tipo de medios, que ya están inmersos en la vida cotidiana y pueden llegar a ser el foco de vulneración de la intimidad del individuo, causándole diversidad de conflictos a nivel social, personal, profesional, político, entre otros.

En la primera sección de este artículo, se encontrará un análisis de la forma mediante la cual se recopilan los datos en esta red social, posteriormente se procede a describir el uso y tratamiento dado a esta información y se realiza un comparativo del reglamento que rige actualmente la operación de Facebook en Europa, versus los antecedentes de incumplimiento de esta compañía en el tratamiento de datos personales, con el propósito de generar conclusiones basadas en las etapas analizadas anteriormente que brindan una luz sobre la realidad en el manejo de datos por parte de Facebook.

Metodología

En la siguiente revisión bibliográfica se busca cuestionar el cumplimiento de la red social Facebook, con respecto a las regulaciones para la protección de datos personales definidas a nivel internacional, se exploran las formas mediante las cuales Facebook recopila la información personal de los usuarios, con el propósito de mostrar al lector lo expuesto que se encuentra con el simple hecho de registrarse en este medio y se analiza el uso y tratamiento de esta información por parte de la red social y cuál es el provecho que la misma saca de esta.

Posteriormente, se identifica aquella regulación con mayor impacto a nivel mundial y que aplique a la operación de las redes sociales, sus antecedentes y características relevantes, con el propósito de desarrollar un comparativo entre aquellas acciones en las cuales la red social Facebook se ha visto implicada en controversias relacionadas con el manejo erróneo de información personal versus aquellos lineamientos que han sido incumplidos o quebrantados por su actuar.

Marco Referencial

En esta sección podrá encontrar la definición de una serie de conceptos utilizados en el desarrollo del artículo, con el propósito de brindar mayor claridad y entendimiento al lector al momento de realizar la lectura de la revisión bibliográfica.

Seguridad de la Información: La seguridad de la información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a las organizaciones asegurar la confidencialidad, integridad y disponibilidad de su sistema de información (Mifsud, 2012), y aplica no solamente para organizaciones, también para personas que disponen de información que pueda ser vulnerada (Iván et al., 2015)

Web beacons: Los Web Beacons son una herramienta integral en la web hoy en día. En su forma más simple, los Web Beacons son pequeñas cadenas de código que proporcionan un método para entregar una imagen gráfica en una página web o en un mensaje de correo electrónico con el fin de transferir datos (Software, 2018)

RGPD: El RGPD establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales. Se aplican tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE (Comisión GDPR, 2020)

Comisión Federal de Comercio (siglas en ingles FTC): La única agencia federal que tiene jurisdicción tanto en el ámbito de la protección del consumidor como en el terreno de la competencia en amplios sectores de la economía. La FTC trabaja a favor de un cumplimiento de la ley vigoroso y efectivo; promueve el interés de los consumidores compartiendo su experiencia y conocimientos con las cámaras legislativas federales y con las legislaturas estatales, y con agencias gubernamentales de EE. UU (FTC, 2020).

Cookies: Pequeña cantidad de información que se almacena en un dispositivo (ya sea ordenador, tableta o Smartphone) con el fin de identificar al navegador mientras interacciona con los sitios web (Cookies, 2018).

Píxeles de seguimiento: también llamado píxel de conversión, tracking pixel, pixel tag o simplemente píxel de rastreo es una diminuta imagen de 1x1 pixel (base por altura) transparente, por

lo normal en formato GIF, que se inserta dentro del código fuente de un sitio web con el fin de medir una actividad concreta (Team, 2019).

API´s: Igual que una interfaz de usuario permite la interacción y comunicación entre un software y una persona, una API (acrónimo de Application Programming Interface) facilita la relación entre dos aplicaciones para el intercambio de mensajes o datos. Un conjunto de funciones y procedimientos que ofrece una biblioteca para que otro software la utilice como capa de abstracción, un espacio de acceso e intercambio de información adicional en la parte superior. Así una se sirve de la información de la otra sin dejar de ser independientes (BBVA, 2016).

NASDAQ; Acrónimo de National Association of Securities Dealers Automated Quotation y es la bolsa de valores electrónica automatizada más grande de Estados Unidos (Vu, 2019).

SDK: Acrónimo de "Software Development Kit" (Kit de desarrollo de software). El SDK reúne un grupo de herramientas que permiten la programación de aplicaciones móviles (INTERNET, 2019).

DPC: Comisionado es el encargado de asegurar el respeto por el derecho individual a la privacidad, y hacer cumplir las obligaciones impuestas por la Ley de Protección de Datos irlandesa (Technology, 2018).

TJCE: Tribunal de Justicia de la Unión Europea (TJUE) interpreta la legislación de la UE para garantizar que se aplique de la misma manera en todos los países miembros y resuelve los litigios entre los gobiernos nacionales y las instituciones europea**s** (Tribunal de Justicia de la Unión Europea (TJUE), 2020)**.**

¿Cómo Facebook recopila información personal de sus usuarios?

Para responder a este interrogante la primera fuente de consulta obviamente son las políticas de datos que expone la propia red social en su sitio web, aquí llama la atención el encabezado del documento que indica: "a fin de proporcionarte los Productos de Facebook debemos tratar información sobre ti. El tipo de información que recopilamos depende de la forma en la que usas nuestros productos." (Política de datos, 2018) y vaya que el último planteamiento es bastante cierto, ya que, dependiendo del uso que tenga el individuo de la red social, los sitios web donde realice registro a través de Facebook o simplemente dando un "me gusta" da pie para que la compañía obtenga información, se profundizará más adelante en este aspecto.

Volviendo con las políticas de datos Facebook, es sorprendente observar la forma en que esta red social justifica por qué recopila cierto tipo de información y llama la atención el hecho de que según ellos todo se hace para el "beneficio de sus usuarios" con el propósito de facilitar su interacción y comunicación a través de los productos de la red social.

Para entrar en detalle, según las políticas de datos de Facebook (Política de datos, 2018), estos obtienen información de 3 fuentes, que son: lo que el propio usuario y otras personas hacen y proporcionan (Política de datos, 2018), información de los dispositivos e información de los socios, a continuación, se expone el tipo de información que se encuentra vinculado a cada una de estas fuentes:

Información que el usuario y otras personas crean y proveen

- **Proporcionada por el propio usuario:** se colecciona información del contenido que se crea o se comparte, mensajes enviados o comunicaciones con otros usuarios, metadatos

(ubicación y fecha de creación de un archivo) e información que se captura en la aplicación de Facebook a través de la cámara de los dispositivos.

En esta categoría también se incluye información que la red social denominada “Datos con protecciones especiales” relacionados con creencias religiosas, ideologías políticas, intereses, aspectos de salud del usuario, origen étnico y racial, y se les categoriza de protección especial porque se deben salvaguardar conforme a las leyes de cada país (Política de datos, 2018).

- **Redes y conexiones:** de esta fuente se obtiene información relacionada con personas, paginas, cuentas, hashtags y aquellos grupos a los que pertenezca e interactúe el usuario, llama la atención aquí, que, si este mismo decide sincronizar información desde su dispositivo móvil, la red social también podría acceder a sus contactos, historial de llamadas y mensajes de texto (Política de datos, 2018).

- **Uso del usuario:** la recopilación que se realiza en este aspecto es interesante, aquí la red social puede conocer el tipo de contenido que ve y publica el usuario, las acciones que lleva a cabo en la red, hora, frecuencia y duración de las actividades que realiza y qué uso le da el mismo a la cámara proporcionada por Facebook (Política de datos, 2018).

- **Transacciones financieras o compras a través de Facebook:** se colecciona información sobre pagos que se realicen a través de los productos de la red social (juegos, donaciones, entre otros) en donde se obtienen datos del número de la tarjeta débito o crédito, información sobre la cuenta y autenticación y detalles de facturación (Política de datos, 2018).

- **Información que proporcionen otros usuarios sobre usted:** esta fuente no depende directamente del usuario propietario de la cuenta, debido a que, la información que aquí se recolecta está relacionada con el contenido, comunicaciones e información que otras personas proporcionan sobre usted (etiquetas y comentarios en fotos, si sus amigos sincronizan su libreta de contactos, entre otros) (Política de datos, 2018).

Datos de los dispositivos de conexión

Cuando en la política de datos de Facebook se mencionan “dispositivos de conexión” hace referencia a computadoras, teléfonos, televisores y cualquier dispositivo que se pueda usar para conectarse a la red, con respecto a esto la compañía colecciona datos como:

- **Propiedades del dispositivo:** sistema operativo, versión de software y hardware, espacio de almacenamiento, tipos de aplicaciones, archivos y plugins.

- **Operaciones:** recolecta información sobre las acciones ejecutadas en los dispositivos, por ejemplo, en los móviles ejecutar una aplicación en segundo plano, en los computadores los movimientos del mouse, entre otros.

- **Señal:** información sobre conexiones bluetooth y puntos de conexión a redes wifi.

- **Datos de configuración:** opciones activas en los dispositivos, un ejemplo claro ubicación a través GPS, cámara, entre otros.

- **Conexiones y redes:** número de teléfono celular, dirección IP e información de otros dispositivos que se encuentren conectados a su red.

- **Información de las cookies:** en este punto la red social puede recolectar información sobre el seguimiento a la navegación en Internet del usuario, es decir, los sitios que visita, la publicidad que visualiza, entre otros.

El manejo de cookies por parte de Facebook llama la atención, por el hecho de que aunque una persona no tenga una cuenta registrada en Facebook, no quiere decir que la red social no pueda acceder a cierta parte de su información, debido a que las fuentes de datos disponibles no se limitan a Facebook, y el análisis puede aplicarse fácilmente a otros puntos de preferencia personal (Isaak & Hanna, 2018) aquí es donde juega un papel importante el manejo de cookies, por el hecho de que cada sitio web con el logotipo de Facebook está vinculado a Facebook, lo que permite el seguimiento de los no miembros, así como de los miembros (Isaak & Hanna, 2018), ya que, estos sitios web trabajan con cookies vinculadas con otra herramienta denominada baliza web (web beacons) que juntas constituyen un poderoso medio para realizar seguimiento o rastreo a la navegación de las personas y así brindar a la compañía información que posteriormente negociará con las empresas interesadas en la creación de publicidad dirigida para sus clientes potenciales.

Hay que tener en cuenta que en la política de datos de Facebook específicamente en la sección de "información de los socios" que se menciona posteriormente, se describe lo siguiente: "Estos socios nos brindan información sobre las actividades que realizas fuera de Facebook, incluidos datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que haces, los anuncios que ves y la manera en la que usas sus servicios, ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella." (Política de datos, 2018), ahora bien esto es informado a las personas que registran un perfil en Facebook, la pregunta es ¿cómo se le notifica a las personas que no tienen cuenta registrada en la red social?, actualmente las páginas web indican sobre el manejo de cookies, sin embargo, para la persona sigue siendo transparente el manejo que se le da a la información que se recolecta sobre él, se puede ver lo rentable que resulta para Facebook recolectar este tipo de información sin importar obtenerla de personas a las que ni siquiera les interesa contar con un perfil en la red social, siendo un atentado directo hacia la privacidad de su información.

Otro método de recopilación de información utilizado por la red social, se encuentra al alcance de sus manos y actualmente se ha convertido en una herramienta indispensable en su vida cotidiana, en este momento estará pensando en su dispositivo móvil y esto apenas es un elemento del mecanismo, lo realmente importante para esta compañía es conocer un dato tan básico como su número de teléfono que hoy en día se ha convertido prácticamente en una huella digital adicional de las personas, porque constituye un número e identificador único.

Si bien Facebook ha dejado claro para las personas que se registran en su red social, a través de las políticas de datos que se recopila su número de celular, al mismo tiempo esto no lo tienen claro las personas que no han registrado un perfil activo en Facebook, tal y como lo indica The New York Times en un artículo publicado en abril de 2019: aunque hay personas que se han mantenido fuera de Facebook y otras redes sociales, su número de teléfono está casi seguro en las listas de contactos de muchas otras personas en sus teléfonos. Si se usan Facebook (o Instagram o WhatsApp), que han sido impulsados a subir sus contactos para ayudar a encontrar a sus "amigos", que muchas personas lo hacen (Tufekci, 2019), hasta este punto se puede decir que Facebook ha sido "transparente" porque lo descrito actualmente se encuentra incluido en sus políticas de datos, sin embargo, aparece un concepto que la red social no ha dejado claro en dichas políticas y tiene que ver con los "perfiles sombra" donde entra en juego su número de teléfono que al ser cargado por otra persona al subir su lista de contactos a Facebook proporciona el dato de su número celular y una vez que su número aparece en algunas cargas, Facebook puede ubicarlo en una red social, lo que lo ayuda a inferir cosas sobre usted, ya que tendemos a parecernos a las personas en nuestro conjunto social. (Facebook incluso mantiene perfiles de "sombra" de no usuarios y despliega "píxeles de seguimiento" situados en toda la web, no solo en Facebook, que transmiten información sobre su comportamiento a la empresa) (Tufekci, 2019).

¿Entonces esta actividad porque no se menciona en las políticas de datos?, obviamente porque constituye un abuso a la privacidad de las personas, sobre todo por el hecho de que son personas que no han tenido interés en registrarse en la red social y sin embargo se recolecta información sobre ellas, lo que constituye una acción intrusiva en su vida personal y le da a la compañía y sus empresas socias la potestad de conocer cosas sobre usted a través de modelos estadísticos de inferencia computacional, que brindan la posibilidad de conocer aspectos de su personalidad que están en el ámbito de su intimidad y que usted no ha hecho ni quiere hacer público.

Información de los socios

Información suministrada a Facebook por parte de los anunciantes, desarrolladores de aplicaciones y editores que usan lo que la compañía denominada “herramientas empresariales de Facebook” que incluye API´s, botón “me gusta”, inicio de sesión con Facebook, plugins sociales, SDK, entre otros.

Esta fuente aporta información relacionada con actividades que realiza el usuario en sitios web o aplicaciones móviles fuera de la red social, compras en otros sitios, anuncios visualizados, sin discriminar si el usuario se encuentra registrado o no en la red social, por último llama la atención que también se recopila información sobre las compras que se realizan fuera de Internet, debido a que cuenta con proveedores autorizados para compartir esta información, según indican en su política de datos.

Queda la sensación de que Facebook gracias a la información suministrada por los socios, constituye un medio entrometido en la vida de sus usuarios, contrastando lo definido en la política de datos con las revelaciones hechas por el diario británico The Times quienes mediante la revisión de más de 270 páginas de documentación encontraron que Facebook obtuvo datos de múltiples socios para una controvertida herramienta de sugerencia de amigos llamada "People You May Know"(personas que quizás conozcas) (Dance, LaForgia, & Confessore, 2018), esta es una funcionalidad que aun en 2020 continúa activa y su propósito principal consiste en dar sugerencias de amigos que se pueden agregar en la red social, lo sensible de esta función es el hecho de que varios usuarios alrededor del mundo han estado en contra, por el hecho de que permite a la red social hacer un mapeo de sus relaciones interpersonales en el mundo real (Dance, LaForgia, & Confessore, 2018), teniendo en cuenta que se han reportado casos donde la herramienta recomienda conexiones amigas entre pacientes de la misma psiquiatra, familiares separados y un acosador y su víctima (Dance, LaForgia, & Confessore, 2018), lo anterior permite inferir el alto grado de conocimiento que tiene la red social sobre los usuarios, llegando a tener información de aspectos tan íntimos en la vida de una persona como el hecho de ser acosado, un tema álgido que en pocos casos se hace público a través de una red social, por lo sensible y denigrante que puede resultar para la persona afectada.

Para finalizar esta sección, se trae a colación el siguiente planteamiento “cuando algo es gratis el producto eres tú” (Plazas Porras, 2018), una premisa muy acertada en la actualidad, porque aunque el uso de Facebook tiene la sensación de ser gratuito, realmente esta compañía recibe un pago significativo de parte de los usuarios que la usan a diario, y es su información personal que hoy en día tiene un valor predominante en el mercado, es tanto el provecho que esta compañía le ha dado a este activo que el 18 de mayo del 2012 Facebook como empresa entra a la bolsa de valores de Nueva York, específicamente al mercado NASDAQ (Plazas Porras, 2018)esto a costa de la vulneración de la privacidad de la información personal de miles de millones de personas alrededor del mundo y también por la distribución exagerada de información que algunas personas tienen en esta red social, que como se pudo ver anteriormente no solo los afecta a ellos mismos, sino también a aquellas personas que si le dan relevancia a su información personal pero son expuestas por simplemente estar en la lista de contactos de algún conocido o navegar en Internet.

¿Qué tratamiento le da Facebook a la información personal de sus usuarios?

A muchos de los usuarios de Facebook les inquieta conocer sobre el tratamiento que se le da a su información, en esta sección se trata de analizar los usos dados a dicha información que se recopila a diario de los millones de perfiles que tiene Facebook, y se analiza la posible situación de que la compañía realiza tratamiento de esta información sin el consentimiento de las personas, y para beneficio propio y de su plataforma, cabe resaltar que en sus políticas se menciona el uso dado a la información pero no habla de a quién le están proporcionando dicha información y qué beneficios obtiene de compartirla a otras empresa o plataformas.

Teniendo en cuenta las políticas de datos de Facebook sobre el tratamiento de información las cuales indican que esta se usa según las elecciones y la búsqueda que cada usuario haga, con el objetivo de crear productos personalizados que sean únicos y relevantes, usan las conexiones, preferencias, intereses y actividades en función de los datos que recopilan y que los usuarios y otras personas proporcionan (incluidos aquellos datos con protecciones especiales que el usuario facilite), así como la forma en la que los usuarios utilizan los Productos e interactúan con ellos, y las personas, los lugares o las cosas con los que se conectan y que les interesan, tanto dentro como fuera de los productos de la compañía (*Política de datos*, 2018).

Se puede entender entonces de acuerdo con lo descrito en la política de datos, que los usos que da la red social a la información se representan a través de 5 formas que se describen a continuación:

- **Vínculos a los dispositivos:** Se encarga de realizar sugerencias de acuerdo a contactos o amigos de amigos, vincula dispositivos en los que tenga conocidos o amigos y los muestra para que los agregue.
- **Registros de ubicación:** Mediante el uso de GPS, lugares que les gusta a los usuarios o donde viven para así mejorar los productos y dirigir publicidad relacionada que llamen la atención.
- **Mejora de productos:** Mediante el uso de la información que se tiene o la realización de encuestas.
- **Identificación por rostros en fotografías, videos:** Realiza reconocimiento facial entre todas las fotografías, videos entre otros que estén en Facebook.
- **Publicidad:** Usan información que los usuarios ponen en Facebook para dirigir y poner publicidad u ofertas de su interés.

Otro manejo que se le da a estos datos va enfocado en fomentar la seguridad de la información y dar acceso a sus socios a una parte de la información, esto se puede corroborar de acuerdo a la expresado por los autores en el artículo (Dance et al., 2018)donde mencionan que durante años, Facebook otorgó a algunas de las compañías de tecnología más grandes del mundo un acceso más intrusivo a los datos personales de los usuarios de lo que ha revelado, eximiendo efectivamente a esos socios comerciales de sus reglas de privacidad habituales, según registros internos y entrevistas. Lo anterior nos permite conocer que el uso que se le da a esa información que tienen para ayudar a los anunciantes y otros socios a medir la eficacia y distribución de sus anuncios y servicios, así como a entender qué tipo de personas usan sus servicios y cómo estas interactúan con sus sitios web, apps y servicios (*Política de datos*, 2018).

Uno de los puntos importantes a resolver en este interrogante es conocer los tipos de socios de Facebook, remitiéndose a lo mencionado en las políticas de datos se pueden identificar los tipos que se describen de manera general a continuación:

- **Los que usan los servicios de análisis:** Usan estadísticas y observaciones para conocer cómo interactúan los usuarios en los diferentes contenidos multimedia desde imágenes y videos hasta los anuncios.

- **Los que proporcionan Anuncios:** Permiten a estas compañías ver que anuncios y que reaccione tiene el usuario frente a estos.
- **Medidores:** Compartimos información sobre ti con empresas que la consolidan para ofrecer análisis e informes de medición a nuestros socios (*Política de datos*, 2018).
- **Bienes y servicios:** Mediante la suscripción o compras premium a productos, pueden tener acceso a la información personal del usuario, ya sea para completar las transacciones o verificar el estado de ellas.
- **Ventas:** Dan información necesaria a sus proveedores para el mejoramiento de su compañía.
- **Investigaciones y educativo:** Permite a entidades de investigación tener acceso a la información que les aporte mejoramiento e innovación.
- **Autoridades:** Dan acceso a las autoridades en casos que se requiera según sea el caso de gravedad o si atañe un delito.

Facebook en sus políticas menciona que no venden la información a nadie ni nunca lo harán. También imponen estrictas restricciones sobre la manera en que nuestros socios pueden usar y divulgar los datos que proporcionamos (*Política de datos*, 2018). Pero uno de los autores que contradice al decir que Facebook permitió que el motor de búsqueda Bing de Microsoft viera los nombres de prácticamente todos los amigos de los usuarios de Facebook sin consentimiento, según muestran los registros, y les dio a Netflix y Spotify la capacidad de leer los mensajes privados de los usuarios de Facebook. De igual modo la red social permitió a Amazon obtener los nombres de los usuarios y la información de contacto a través de sus amigos, y le permitió a Yahoo ver transmisiones de publicaciones de amigos tan recientemente como este verano, a pesar de las declaraciones públicas de que había dejado de compartir ese tipo de años antes (Dance et al., 2018).

Otros de los socios de importancia y los que según lo dicho por Facebook no le compartió o vendió información fue el artículo (Voss, 2018) donde habla de la información que Facebook le proporcionó a Cambridge Analytica donde recopiló datos sobre las identidades de los usuarios, redes de amigos y "me gusta". La idea era mapear los rasgos de personalidad basados en lo que a la gente le había gustado en Facebook, y luego usar esa información para apuntar a audiencias con anuncios digitales. Los investigadores en 2014 pidieron a los usuarios que realicen una encuesta de personalidad y descarguen una aplicación, que eliminó información privada de sus perfiles y de sus amigos, actividad que Facebook permitió en ese momento y desde entonces ha prohibido. La técnica había sido desarrollada en la Universidad de Cambridge.

En el momento en que Facebook habla de Privacidad en sus Políticas, en el artículo (Dance et al., 2018) los autores mencionan que en investigaciones realizadas en documentación revelada se habla que algunos ingenieros y ejecutivos consideraban que las revisiones de privacidad eran un impedimento para la innovación y el crecimiento rápidos. Y el equipo central responsable de coordinar las revisiones, con una docena de personas para 2016, se movió dentro de la organización en expansión de Facebook, enviando señales mixtas sobre la seriedad con la que la compañía lo tomó, lo cual nos muestra el poco interés que mostraba la compañía de Facebook en mejoramiento o el respeto hacia la privacidad de los millones de usuarios, no solo por el hecho de que cada uno tenga su privacidad sino porque es lo que les genera económicamente ingresos, por ese mismo motivo esta Red Social es completamente gratuita.

En total, los acuerdos descritos en los documentos beneficiaron a más de 150 empresas, la mayoría de ellas empresas tecnológicas, incluidos minoristas en línea y sitios de entretenimiento, pero también fabricantes de automóviles y organizaciones de medios. Sus aplicaciones buscaron los datos de cientos de millones de personas al mes, según los registros. Las ofertas, la más antigua de las cuales datan de 2010, estuvieron activas en 2017. Algunas todavía estaban vigentes este año, entre otras compañías que se mencionan son Sony, Microsoft, Amazon y otros podrían obtener las direcciones de correo electrónico de los usuarios a través de sus amigos, Facebook también permitió a Spotify, Netflix y el Royal Bank of Canada leer, escribir y eliminar mensajes privados de los

usuarios, y ver a todos los participantes en un hilo, privilegios que parecían ir más allá de lo que las compañías necesitaban para integrar Facebook en sus sistemas (Dance et al., 2018).

Otro de los registros encontrados de Facebook muestra que Yandex tuvo acceso en 2017 a las identificaciones de usuario únicas de Facebook incluso después de que la red social dejó de compartirlas con otras aplicaciones, citando riesgos de privacidad. Además de esto se habla de que Facebook, a su vez, utilizó listas de contactos de los socios, incluidos Amazon, Yahoo y la compañía china Huawei, que ha sido señalada como una amenaza de seguridad por parte de los funcionarios de inteligencia estadounidenses, para obtener una visión más profunda de las relaciones de las personas y sugerir más conexiones, según los registros (Dance et al., 2018).

Estos son de los registros conocidos en los que se hablan de los socios y uso que Facebook le da a la información que tienen de los millones de usuarios, muy a pesar de que la mayoría de estos socios niega haber recibido dicha información se ve reflejada en mucha de las evidencias halladas a lo largo del tiempo.

RGDP y los incumplimientos de la red social Facebook

Para inicios de 2018 las redes sociales eran organizaciones poco reguladas en cuanto a la protección de datos de sus usuarios, esto debido, a que la forma en que operan estas compañías tecnológicas fue durante mucho tiempo un punto de contención para los reguladores estadounidenses. La Comisión Federal de Comercio (FTC) es el organismo administrativo encargado de proteger a los consumidores contra prácticas comerciales engañosas e injustas. (Layton, 2006) No obstante, esta organización ha luchado por proteger los datos de los usuarios por encima de los intereses de las empresas, sin embargo, se ha visto limitada en lo que puede hacer debido a la falta de legislación de privacidad y seguridad de datos. (Layton, 2006)

Luego de los esfuerzos infructuosos de la FTC por proteger los datos personales en EE. UU, surge en Europa como lo explica de manera concreta la firma Grant Thornton en su informe sobre RGDP y Blockchain: “La Directiva 95/46 CE derogada por el RGPD, contemplaba una serie de objetivos generales de protección de datos que los Estados miembros debían cumplir. Sin embargo, dicha Directiva contaba con una serie de puntos débiles, como el amplio margen otorgado a los legisladores nacionales para articular sus legislaciones de protección de datos personales, siempre y cuando cumpliesen con los objetivos establecidos en la Directiva. Esta libertad producía divergencias entre los Estados miembros a la hora de interpretar y aplicar la norma. El resultado era una evidente falta de homogeneidad entre países que, en muchos casos, llevaba a la restricción de actividades en el mercado comunitario. Esta falta de homogeneidad regulatoria en la libre circulación de datos generaba obstáculos dentro la economía digital europea.” (Grant Thornton, s.f.)

La ausencia de homogeneidad entre las diferentes regulaciones creadas por los países miembros de la Unión Europea (UE), género que esta comunidad política tomara cartas en el asunto y diera origen al Reglamento General de Protección de Datos (RGPD) cuyas principales características también son expuestas por la firma Grant Thornton en su informe sobre RGDP y Blockchain en donde se indica: “A diferencia de su predecesora, el RGPD es aplicable a los datos personales de cualquier persona física, con independencia de su nacionalidad o lugar de residencia, siempre que se cumplan los requisitos que estipula el artículo 3. El RPGD define los datos personales como “toda información sobre una persona física identificada o identificable (el interesado)”. Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.” (Grant Thornton, s.f.)

A continuación, la operación de la red social Facebook comenzó a ser regulada tanto en Europa como en aquellas naciones que reciben transferencia de datos personales de algunos de los países miembros de la UE, situación que comenzó a generar grandes inconvenientes para Facebook, debido a una serie de incumplimientos que han generado controversia en varios medios a nivel mundial, a continuación se realiza un consolidado de 5 antecedentes importantes en los cuales la red social se ha visto inmersa por malos manejos de la información personal de sus usuarios y se relacionan con los respectivos lineamientos de 2 normativas (FTC de EE.UU y la Unión Europea) presentaron incumplimientos por el actuar de esta red social.

Tabla 1. Comparativa antecedentes y normativas

ANTECEDENTES	NORMATIVAS
Este caso fue presentado por Maximillian Schrems, ciudadano austríaco, con respecto a la transferencia de datos transfronteriza de Facebook. Como usuario de Facebook, los datos personales de Schrems se transfirieron de servidores en Irlanda a servidores en los EE. UU (Voss, 2018).	La Directiva 95 solo permite transferencias transfronterizas si el país receptor garantiza un nivel adecuado de protección en virtud de la legislación nacional o los acuerdos internacionales. Debido a que las revelaciones de Snowden revelaron que la ley de los Estados Unidos no ofrecía una protección real contra la vigilancia del gobierno de los Estados Unidos con respecto a los datos transferidos allí, Schrems presentó una acción ante el Comisionado de Protección de Datos de Irlanda (CPD). El DPC desestimó el caso de Schrems indicando que la transferencia estaba permitida bajo el acuerdo de Safe Harbor entre los EE. UU. Y Europa. Después de que Schrems apeló, el caso fue enviado al TJCE, que en 2015 invalidó el acuerdo de Safe Harbor en el que las empresas estadounidenses habían confiado en Transferencia de datos desde Europa a los Estados Unidos (Voss, 2018).
	Según (Voss, 2018) el TJCE consideró que el acuerdo de Safe Harbor no era válido porque los datos personales transferidos a los EE. UU. Por Facebook Ireland Ltd. a los servidores pertenecientes a su empresa matriz, Facebook Inc. en los EE. UU., No recibieron la protección adecuada debido al "alcance excesivo" de entre otras cosas, la vigilancia de la Agencia de Seguridad Nacional.159 Específicamente, el TJCE dictaminó además que el Marco de Puerto Seguro era inválido por varias razones:• Permitió la interferencia del gobierno de las protecciones de la Directiva 95, no proporcionó remedios legales para las personas que buscan acceder a datos relacionados con ellos o que se borren o modifiquen sus datos, y evitó que las autoridades nacionales de supervisión ejerzan adecuadamente sus poderes (Voss, 2018)
Facebook le dio acceso sin restricciones y sin autorización a información personal identificable (PII) de más de 87 millones de	Facebook recibió formalmente una histórica sanción por parte de la Comisión Federal de Comercio de EE. UU. (FTC) a raíz de investigaciones por el escándalo

usuarios desprevenidos de Facebook a la firma de datos da la privacidad y el bienestar de los ciudadanos. Cambridge Analytica se dio cuenta de que podían integrar esta información con una variedad de datos de plataformas de redes sociales, navegadores, compras en línea, resultados Cambridge Analytica. Ha votación y más para crear "más de 5,000 puntos de datos sobre 230 millones de adultos en los Estados Unidos". Al agregar el análisis OCEAN a los demás datos privados y públicos adquiridos, Cambridge Analytica desarrolló la capacidad de "micro-focalizar" consumidores individuales o votantes con mensajes con mayor probabilidad de influir en su comportamiento (Isaak & Hanna, 2018)	de Cambridge Analytica. Deberá pagar una multa por 5 mil millones de dólares, la más alta que ha dictaminado la entidad, pero además estará en la obligación de cambiar su modelo de uso de datos y privacidad (TIEMPO, 2019). Lo más contundente del fallo, que se basa en un acuerdo que acorrala a la red social, es que por primera vez se le pondrá un alto en el camino a la autoridad final del director ejecutivo y fundador, Mark Zuckerberg, sobre las decisiones de privacidad de la empresa. La FTC exigirá que Facebook cree un comité independiente de directores en la compañía para tomar decisiones sobre políticas de tratamiento de datos (TIEMPO, 2019)
El intercambio tenía la intención de beneficiar a todos. Al impulsar un crecimiento explosivo, Facebook consiguió más usuarios, elevando sus ingresos publicitarios. Las empresas asociadas adquirieron funciones para hacer que sus productos sean más atractivos. Los usuarios de Facebook se conectaron con amigos a través de diferentes dispositivos y sitios web. Pero Facebook también asumió un poder extraordinario sobre la información personal de sus 2.200 millones de usuarios, control que ha ejercido con poca transparencia o supervisión externa (Dance et al., 2018). Facebook permitió que el motor de búsqueda Bing de Microsoft viera los nombres de prácticamente todos los amigos de los usuarios de Facebook sin consentimiento, según muestran los registros, y les dio a Netflix y Spotify la capacidad de leer los mensajes privados de los usuarios de Facebook(Dance et al., 2018).La red social permitió a Amazon obtener los nombres de los usuarios y la información de contacto a través de sus amigos, y le permitió a Yahoo ver transmisiones de publicaciones de amigos tan recientemente como este verano, a pesar de las declaraciones públicas de que había dejado de compartir ese tipo de años antes(Dance et al., 2018).	Pero el Sr. Vladeck y otros ex funcionarios de la FTC dijeron que Facebook estaba interpretando la exención de manera demasiado amplia. Dijeron que la disposición tenía la intención de permitir a Facebook realizar las mismas funciones cotidianas que otras compañías, como enviar y recibir información a través de Internet o procesar transacciones con tarjeta de crédito, sin violar el decreto de consentimiento (Dance et al., 2018). Según Facebook, la mayoría de sus asociaciones de datos caen bajo una exención al acuerdo de la FTC. La compañía argumenta que las compañías asociadas son proveedores de servicios, compañías que usan los datos solo "para y bajo la dirección de" Facebook y funcionan como una extensión de la red social (Dance et al., 2018).
Otro de los antecedentes importante y en la cual también tuvo participación Cambridge Analytica, son las elecciones de Brexit, en donde nuevamente Facebook proporciono información a Analytica para crear	La Comisión Federal de Comercio de Estados Unidos (FTC, por sus siglas en inglés) ordenó a la red social a pagar US$5.000 millones como sanción por las malas prácticas en el manejo de la seguridad de los datos de los usuarios.

publicidad dirigida a miles de usuarios.	
	Las autoridades del Reino Unido impondrán una multa de 500.000 libras (565.000 euros) a la empresa estadounidense de comunicación social Facebook por violar la ley de protección de datos en este país. Las organizaciones defensoras de los datos del consumidor han lamentado la poca cuantía de la multa a Facebook, que es la máxima que puede imponer la ICO en base a la ley de protección de datos de 1998, que es la que se aplica en este caso y no la nueva legislación europea que entró en vigor este año, que contempla mayores penalizaciones. La multa ha sido comunicada a la empresa estadounidense, que tiene ahora un tiempo para presentar nuevas alegaciones.
En 2011, la Comisión Federal de Comercio (FTC) teniendo razones para considerar que Facebook Inc. había violado el Federal Trade Commission Act (FTC Act) inició investigación en contra de la compañía por haber incurrido en conductas para engañar a los usuarios sobre su política de privacidad. En particular, se hacía referencia a que la red social aparentemente permitía a los usuarios "controlar" los ajustes de privacidad de su información y restringir su acceso a terceros, pero al mismo tiempo y de manera recurrente estaba permitiendo compartir o divulgar públicamente. En el comunicado de prensa de la Comisión expresamente se destaca que dentro de las conductas denunciadas por los usuarios se encontraban quejas sobre el uso de información que hacían aplicaciones de terceros que el usuario instalaba y vinculaba a su cuenta. Según Facebook, dichas aplicaciones únicamente utilizaban la información necesaria para operar, cuando en realidad accedían a casi toda la información de los usuarios (Lizet, 2018).	Facebook se comprometió frente a la Comisión a adoptar medidas tendientes a proteger los datos de sus usuarios, y entre otras, a cumplir con las siguientes condiciones: (i) se prohíbe brindar información falsa o imprecisa sobre las condiciones de privacidad y seguridad de la información personal de los usuarios; (ii) debe obtener autorización de los usuarios para realizar cambios en la plataforma que modifiquen sus preferencias de privacidad (Lizet, 2018).
	(ii) debe diseñar y mantener un programa integral de privacidad tendiente a mitigar los riesgos de privacidad asociados al desarrollo de sus servicios (los existentes y nuevos) y proteger los datos personales de sus usuarios y la confidencialidad de los mismos; (iv) se requiere que cada dos años durante 20 años (contados a partir del acuerdo) obtenga auditorías externas independientes que certifiquen que cuenta con un programa de privacidad que cumple o excede los requerimientos dados por la Comisión y para garantizar que la privacidad de la información de los usuarios se encuentra adecuadamente protegida(Lizet, 2018).

Fuente: Elaboración propia (2020)

Finalmente, luego de recopilar diversos antecedentes acerca del incumplimiento de las normativas de protección de datos personales por parte de Facebook, la situación más escandalosa por la cual se dieron a conocer los antecedentes de esta red social fue por el uso que Cambridge Analytica le dio a la información de más de 87 millones de usuarios que Facebook le suministro. Teniendo en cuenta el anterior evento se da origen a regulaciones por parte de la Comisión Federal de Comercio (FTC) en EE. UU y el Reglamento General de Protección de Datos (RGPD) en la Unión Europea.

La FTC encargada de velar por los derechos del consumidor, lleva años tratando de restringir el incumplimiento normativo por parte de Facebook, sin embargo, estas normativas presentan

debilidades con respecto a la regulación de las redes sociales y el tratamiento de la información (recolección, almacenamiento, uso, circulación y supresión) aplicado por esta.

De acuerdo con los hechos negativos que se han revelado con respecto al uso y tratamiento de la información por parte de Facebook, que, aunque se intentó regular tenía la habilidad de modificar las políticas de manera en que más lo beneficiara sin dar prioridad a un buen uso de la información personal. Por último, las redes sociales actualmente no cuentan con una normatividad que regule de manera rotunda el uso de la información que almacenan y es importante que como usted tenga en cuenta que información está suministrando a estas plataformas, con el propósito de minimizar el conocimiento que las redes sociales pueden tener sobre usted y su personalidad.

Conclusiones

En las redes sociales constantemente se generan miles de pensamientos, sentimientos, opiniones, críticas y demás de manera textual sobre temáticas sociales, económicas, educativas, de mercadeo, salud, etc.(Gil & Quintero, 2019) esto permite a redes sociales como Facebook, recolectar datos íntimos de las personas y le brinda la posibilidad de conocer las características de la personalidad de cada usuario y de acuerdo con lo analizado en esta revisión esta acción se considera intrusiva, hecho que las situaciones polémicas en las cuales se ha visto relacionada Facebook respaldan. Y es que aunque actualmente se cuenta con normativas que intentan regular la acciones que la red social ejecuta sobre la información que posee de cada uno de sus usuarios, hay que tener en cuenta que algunos países ni siquiera cuentan con normativas para el tratamiento de la información personal y sumado al hecho de que ni esta ni ninguna red social cuenta con una normativa específica que limite el uso de la información que almacenan, lo cual crea un amplio campo de acción para que la compañía establezca políticas con mínimo cumplimiento sin que esto afecte su principal modelo de negocio como lo es la publicidad dirigida por mencionar alguno.

Se trae a colación nuevamente una idea que ya se había mencionado a lo largo del trabajo pero que es bastante llamativa y descriptiva que indica que “cuando un servicio es gratuito el producto eres tú”(Plazas Porras, 2018) y vaya que se pudo evidenciar como Facebook explota este producto de diferentes maneras y de una forma tan óptima que pudo llegar a cotizar en grandes bolsas de valores como la de Nueva York, sin dar prioridad a que la divulgación de datos personales puede vulnerar la vida íntima de las personas y dejar al descubierto aspectos de su vida privada.

Es una realidad que, aunque algunas personas no se registren en redes sociales como Facebook, mínimamente tendrán amigos o conocidos que, si están registrados en la red social, cuentan con una aplicación de mensajería instantánea como WhatsApp, navegan en Internet o realizan compras en línea, entonces por cualquiera de estos medios Facebook estará recolectando información y por ende vulnerando su privacidad sin tan siquiera usted darse cuenta y tomando provecho de su información.

Para finalizar, una posible investigación a futuro que se considera pertinente realizar es la creación de un modelo de cumplimiento normativo basado en regulaciones sobre tratamiento de datos personales para las redes sociales, una base conceptual que se puede utilizar sería el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

Referencias

BBVA. (2016). *Qué es una API y qué puede hacer por mi negocio*. https://bbvaopen4u.com/es/actualidad/que-es-una-api-y-que-puede-hacer-por-mi-negocio

Comisión GDPR. (2020). *Reglamento general de protección de datos*. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Cookies. (2018). ¿Qué son y para qué sirven las cookies? *Cookies*.
Dance, G. J. X., LaForgia, M., & Confessore, N. (2018). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants.
Facebook. (19 de abril de 2018). *Política de datos*. https://www.facebook.com/about/privacy/update.
FTC. (2020). *Acerca de la FTC*. https://www.ftc.gov/es/acerca-de-la-ftc
Gil, V., & Quintero, C. (2019). Aceptación del M – learning: Un Análisis de Sentimientos basado en Minería de Texto. *Cuaderno Activa*, *11*, 45–50. http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/577
Graham-Harrison, E., & Cadwalladr, C. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 1–5.
Grant Thornton. (s.f.). *RGPD y Blockchain* https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/rgpd-y-blockchain-final.pdf
INTERNET, A. (2019). *SDK*. https://www.atinternet.com/es/glosario/sdk/
Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56–59. https://doi.org/10.1109/MC.2018.3191268
Iván, J., Martínez, E., Carlos, L., & Rojas, Q. (2015). *Vulnerabilidad en dispositivos móviles con sistema operativo Android. Vulnerability in Mobile Devices with Android Operating System*. 2027–8101. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/248/240
KEMP, S. (2020). *DIGITAL 2020: GLOBAL DIGITAL OVERVIEW*. https://datareportal.com/reports/digital-2020-global-digital-overview
Layton, C. (2006). *GDPR: ¿The end of Google and Facebook or a new paradigm in data privacy? XXV*(June), 1–109.
Lizet, M. N. (2018). *Notas sobre el caso de Facebook y Cambridge Analytica: modelos de negocio que se basan en la explotación de datos personales*. https://doi.org/10.1542/peds.2006-2099
Plazas Porras, A. (2018). FACEBOOK: De red social a monopolio de información. Kairós Gerencial, 3(6). Recuperado a partir de https://revistas.unicolmayor.edu.co/index.php/kairos/article/view/863
Software, K. (2018). *Balizas web: pautas para notificación y elección La*. 1–6.
Team, D. (2019). *¿Qué es un píxel de seguimiento?* https://www.diligent.es/que-es-un-pixel-de-seguimiento-marketing-digital-para-empresas-en-barcelona/
Technology, U. of A. I. P. & I. (2018). *Comisionado de Protección de Datos Personales de Irlanda*. http://www.uaipit.com/es/ficha-enlace?/60/comisionado-de-proteccion-de-datos-personales-de-irlanda
TIEMPO, P. EL. (2019). Histórica Multa a Facebook :5 mil millones de dólares. *El Tiempo*. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/millonaria-multa-a-facebook-por-el-caso-de-cambridge-analytica
Tribunal de Justicia de la Unión Europea (TJUE). (2020). *Tribunal de Justicia de la Unión Europea (TJUE)*.
Tufekci, Z. (2019). *Think You're Discreet Online? Think Again* https://www.nytimes.com/2019/04/21/opinion/computational-inference.html
Vaca Cedeño, M. S., & Ibarra Segovia, G. R. (2019). *Derecho a la intimidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales*. Retrieved from http://repositorio.ug.edu.ec/handle/redug/39445
Voss, K. A. H. & W. G. (2018). *GDPR: The end of google and Facebook or a new paradigm in data privacy*. *XXV*(June), 1–109.
Vu, M. D. (2019). *Qué es el Nasdaq*. https://esbolsa.com/blog/bolsa-americana/que-es-el-nasdaq/