UNIVERSIDAD HEMISFERIOS

Facultad de Comunicación

Tema:

LA ÉTICA Y EL USO DE LOS DATOS POR PARTE DE COMPAÑIAS COMO FACEBOOK, INSTAGRAM, YOUTUBE Y TIKTOK.

Trabajo de Titulación para la obtención del Título de Licenciatura en Comunicación

Presentada por:

Fabián Andrés Escuntar Ruiz

Tutor:

Amaya Arribas

Quito, diciembre del 2022

RESUMEN

En estos últimos años la importancia de la seguridad de los usuarios de redes sociales se ha vuelto un dilema importante de discutir. Las personas exponen sus datos a varias compañías diariamente sin tener el conocimiento adecuado sobre los peligros que conlleva esto. Las compañías de redes sociales han explotado esta ignorancia durante la última década, sin tener en cuenta las necesidades del usuario. Por esta razón, han surgido problemas tangibles que se deben evitar a toda costa, como lo es la manipulación psicológica de los usuarios de redes sociales. Las compañías de redes sociales logran esto mediante la construcción de perfiles con todo tipo de información que exista sobre el usuario, incluidos: números de teléfono, localizaciones, transacciones monetarias, edad, sexo, preferencias e incluso perfiles psicológicos. Por esta razón es importante entender cuáles son las amenazas que se presentan para el usuario debido al mal uso de las redes sociales y a las prácticas poco éticas de las compañías que las manejan.

El objetivo de esta investigación es demostrar a los usuarios de redes sociales las prácticas más comunes que utilizan las compañías más conocidas de redes sociales, tales como Facebook, Instagram, Youtube y Tiktok, para recolectar datos del usuario. También se busca demostrar que estas prácticas que utilizan son, como mínimo, poco éticas, y no se tiene en cuenta el bienestar del usuario o el daño que se le puede causar por utilizar estos datos de distintas formas indebidas.

Para este proyecto se utilizó una investigación del tipo cuantitativo y cualitativo. La investigación cualitativa se basó en utilizar datos de varios profesionales, como de conocimiento de redes y Big Data, para compararlos con datos obtenido en la investigación cuantitativa. La investigación cuantitativa se basó en obtener datos de usuarios promedio de redes sociales mediante una encuesta. Esta encuesta contiene preguntas que buscan entender el conocimiento general del usuario sobre el uso de sus datos, tales como si están al tanto de los permisos que otorgan a las compañías como Facebook, para utilizar sus datos personales.

Esta investigación llegó a los siguientes resultados más relevantes. Primero, que las redes sociales se construyen de tal forma que la obtención de los datos del usuario es la prioridad de las redes sociales. No importa qué intente hacer el usuario, de una forma u otra se obtendrán sus datos para utilizarlos. Segundo, que el uso de estos datos no se utiliza de

forma debida, ya que incluso se utiliza para razones poco éticas como el esparcimiento de desinformación. Por último, que los usuarios no están al tanto de lo que conlleva aceptar políticas de privacidad y de uso de datos o no les importa entender lo que conlleva. Incluso hay usuarios que conocen sobre el tema pero que se rinden ante la inhabilidad de poder hacer algo al respecto para evitar que se recojan sus datos.

Palabras Clave: Big Data, Ciber seguridad, Redes Sociales, Datos.

DECLARACIÓN DE ACEPTACIÓN DE NORMA ÉTICA Y DERECHOS

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Por tal motivo, autorizo a la Biblioteca a que haga pública su disponibilidad para lectura dentro de la institución, a la vez que autorizo el uso comercial de mi obra a la Universidad Hemisferios, siempre y cuando se me reconozca el cuarenta por ciento (40%) de los beneficios económicos resultantes de esta explotación.

Además, me comprometo a hacer constar, por todos los medios de publicación, difusión y distribución, que mi obra fue producida en el ámbito académico de la Universidad Hemisferios.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Fabian Escuntar

C.I.

1715791099

DEDICATORIA

Agradezco a mis padres Fabian y Mercedes, por haberme dado todas las herramientas necesarias para llegar hasta donde estoy ahora. Les dedico este trabajo con todo mi corazón sabiendo que me apoyaron tanto en las buenas como en las malas.

A todos mis hermanos que igualmente me han apoyado en mis mejores y peores momentos. Me han sabido aguantar incluso en estas épocas difíciles que estamos viviendo.

A mis amigos de la universidad que me han brindado apoyo y conocimientos útiles para poder crear este trabajo.

A mis profesores que hicieron lo todo los posible para que pueda salir adelante.

Finalmente, hago una dedicatoria especial a Carolina Villagómez, que es la persona que más me ha apoyado en estos tiempos difíciles. Gracias por darme las fuerzas para salir adelante en los momentos más difíciles. Y más que nada gracias por ser la mejor amiga que una persona pueda tener.

ÍNDICE

ÍNDICE DE GRÁFICAS

LA ÉTICA Y EL USO DE LOS DATOS POR PARTE DE COMPAÑIAS COMO FACEBOOK, INSTAGRAM YOUTUBE Y TIKTOK.

Fabian Andrés Escuntar Ruiz

fabianandrese029@gmail.com

Resumen

En estos últimos años la importancia de la seguridad de los usuarios de redes sociales se ha vuelto un dilema importante de discutir. Las personas exponen sus datos a varias compañías diariamente sin tener el conocimiento adecuado sobre los peligros que conlleva esto. Las compañías de redes sociales han explotado esta ignorancia durante la última década, sin tener en cuenta las necesidades del usuario. Por esta razón, han surgido problemas tangibles que se deben evitar a toda costa, como lo es la manipulación psicológica de los usuarios de redes sociales. Las compañías de redes sociales logran esto mediante la construcción de perfiles con todo tipo de información que exista sobre el usuario, incluidos: números de teléfono, localizaciones, transacciones monetarias, edad, sexo, preferencias e incluso perfiles psicológicos. Por esta razón es importante entender cuáles son las amenazas que se presentan para el usuario debido al mal uso de las redes sociales y a las prácticas poco éticas de las compañías que las manejan.

El objetivo de esta investigación es demostrar a los usuarios de redes sociales las prácticas más comunes que utilizan las compañías más conocidas de redes sociales, tales como Facebook, Instagram, Youtube y Tiktok, para recolectar datos del usuario. También se busca demostrar que estas prácticas que utilizan son, como mínimo, poco éticas, y no se tiene en cuenta el bienestar del usuario o el daño que se le puede causar por utilizar estos datos de distintas formas indebidas.

Para este proyecto se utilizó una investigación del tipo cuantitativo y cualitativo. La investigación cualitativa se basó en utilizar datos de varios profesionales, como de conocimiento de redes y Big Data, para compararlos con datos obtenido en la investigación cuantitativa. La investigación cuantitativa se basó en obtener datos de usuarios promedio de

redes sociales mediante una encuesta. Esta encuesta contiene preguntas que buscan entender el conocimiento general del usuario sobre el uso de sus datos, tales como si están al tanto de los permisos que otorgan a las compañías como Facebook, para utilizar sus datos personales.

Esta investigación llegó a los siguientes resultados más relevantes. Primero, que las redes sociales se construyen de tal forma que la obtención de los datos del usuario es la prioridad de las redes sociales. No importa que intente hacer el usuario, de una forma u otra se obtendrán sus datos para utilizarlos. Segundo, que el uso de estos datos no se utiliza de forma debida, ya que incluso se utiliza para razones poco éticas como el esparcimiento de desinformación. Por último, que los usuarios no están al tanto de lo que conlleva aceptar políticas de privacidad y de uso de datos o no les importa entender lo que conlleva. Incluso hay usuarios que conocen sobre el tema pero que se rinden ante la inhabilidad de poder hacer algo al respecto para evitar que se recojan sus datos.

Palabras Clave: Big Data, Ciber seguridad, Datos del Usuario.

Abstract

In recent years, the importance of the security of social network users has become an important dilemma to discuss. People expose their data to various companies on a daily basis without having the proper knowledge about the dangers this brings. Social media companies have exploited this ignorance for the past decade, disregarding user needs. For this reason, tangible problems have arisen that must be avoided at all costs, such as the psychological manipulation of social network users. Social media companies accomplish this by building profiles with whatever information exists about the user, including: phone numbers, locations, monetary transactions, age, gender, preferences, and even psychological profiles. For this reason, it is important to understand what threats are presented to the user due to the misuse of social networks and the unethical practices of the companies that manage them.

The objective of this research is to demonstrate to social network users the most common practices used by the most well-known social network companies, such as Facebook, Instagram, Youtube and Tiktok, to collect user data. It also seeks to demonstrate that these practices they use are, at the very least, unethical, and do not take into account the well-being of the user or the damage that may be caused by using this data in different improper ways.

For this project, a quantitative and qualitative type of research was used. The qualitative research was based on using data from various professionals, such as knowledge of networks and Big Data, to compare them with data obtained in quantitative research. The quantitative research was based on obtaining data from average users of social networks through a survey. This survey contains questions that seek to understand the general knowledge of the user about the use of their data, such as whether they are aware of the permissions they grant to companies, such as Facebook, to use their personal data.

This research reached the following most relevant results. First, that social networks are built in such a way that obtaining user data is the priority of social networks. No matter what the user tries to do, one way or another his data will be obtained for use. Second, that the use of this data is not used properly, since it is even used for unethical reasons such as the spread of disinformation. Finally, that users are not aware of what it entails to accept privacy and data use policies or do not care to understand what it entails. There are even users who know about the subject but give in to the inability to do anything about it to prevent their data from being collected.

Key words: Big Data, Cyber Security, User Data.

INTRODUCCIÓN

1. Con las nuevas tecnologías surgen nuevos dilemas con el uso de los datos del usuario.

La tecnología que utilizamos diariamente ha avanzado a una velocidad descomunal en estas dos últimas décadas. Hoy en día el 48,53% (3.80 billones) de las personas de todo el mundo utilizan un teléfono inteligente de acuerdo a datos obtenidos por Statista, una empresa dedicada a obtener datos de todo tipo. La cifra sube cuando se trata de dispositivos móviles en general a 67,03% (5.28 billones). Más de la mitad de personas del mundo tiene la capacidad de conectarse a la internet desde casi cualquier lugar. Esto ha generado una nueva era de conectividad global donde es casi indispensable estar conectado a diferentes redes. Entre las redes más importantes y grandes de la industria están las redes sociales. Las redes sociales son servicios que nos permiten conectar con otros usuarios alrededor del mundo y compartir todo tipo de información personal con ellos. Gracias a estos servicios la humanidad se ha conectado más que nunca con los demás y ha logrado evitar las barreras comunicativas que antes nos separaban como el tiempo y la distancia. Ahora los mensajes llegan a su destino de forma inmediata y somos capaces de compartir todo tipo de información con nuestros seres queridos.

Sin embargo, con el auge de estas nuevas tecnologías, se crean nuevos dilemas que el ser humano debe afrontar. El ser humano está generando una mayor cantidad de datos en esta última década que en toda la historia de la humanidad combinada. Sin embargo, ya entramos a una época donde el valor de ese conocimiento se vuelve invaluable para los que saben qué hacer con ello. La nueva tecnología que surgió de todo esto es la Big Data, que como su nombre implica, se trata de grandes cantidades de datos que pueden ser procesados y utilizados para varios fines. Hoy en día los datos tienen un valor masivo en el mercado debido a la facilidad que otorgan a las compañías para entender las tendencias de sus clientes. Con los datos se puede generar perfiles del usuario para saber lo que le gusta y lo que no, cuanto está dispuesto a pagar y hasta el tipo de publicidad que le influirá más en el momento de decidir si hacer una compra. Por ende, las compañías que manejan este tipo de datos, se han convertido en los nuevos gigantes industriales. Entre estas nos encontramos a compañías gigantes de redes sociales tales como, Facebook, Youtube, Instagram, Twitter, Snapchat,

Whatsapp y más recientemente Tiktok. Estas compañías generan cientos de millones de dólares al año gracias a la utilización de los datos de los usuarios. ¿Pero, cual es el problema? El problema es que las redes sociales utilizan nuestros datos personales de formas poco éticas para generar ganancias.

Las compañías de redes sociales nos conocen más que nosotros mismos y lucran con esa información. Cuando venden estos datos a otras compañías están exponiendo nuestra vida entera sin que el usuario sepa nada al respecto. Incluso si se conocen las implicaciones de estos actos, no hay nada que se pueda hacer al respecto. Si el usuario quiere usar redes sociales, debe entregar sus datos y su privacidad sin objeciones. Por eso se requiere tener un mayor conocimiento del asunto, de tal forma que podamos objetar estas prácticas fraudulentas y ejercer nuestros derechos como consumidores.

Ya ha sucedido antes que se crean regulaciones para evitar acciones poco éticas como la creación de monopolios. En este caso las redes sociales tienen monopolios de nuestra información. Debemos volver a implementar nuevas restricciones para estos nuevos conceptos de forma que evitemos el mal uso de nuestros datos. Así podremos evitar que las compañías de redes sociales lucren por montones a cuesta de la información del usuario.

1.1. Objetivo general

Con los datos obtenidos se busca responder al objetivo general de la investigación: si es que los usuarios de redes sociales consumen una gran cantidad de tiempo en redes sociales, para así demostrar que el algoritmo hizo su trabajo y los mantuvo más tiempo para obtener más datos.

1.2 Objetivos específicos

Este trabajo de investigación busca resolver los siguientes objetivos específicos:

1. Explicar que los algoritmos de las mayores redes sociales (Facebook, Instagram Tiktok etc..) están construidas para ser los más adictivas posible.

2. Indicar que las redes sociales tienen todo el control sobre los datos del usuario.

3. Determinar si las redes sociales utilizan los datos de los usuarios de formas éticas o teniendo el bienestar del usuario en mente.

Con estos objetivos podemos ver si la a la hipótesis de este trabajo es correcta: Las redes sociales utilizan nuestros datos personales de formas poco éticas para generar ganancias. Del mismo modo se busca responder a las siguientes preguntas de investigación para saber si los datos del usuario son mal utilizados por las compañías de redes sociales: ¿Cómo se obtienen los datos que utilizan estas redes sociales? ¿Qué elementos tienen las políticas de privacidad y datos de las compañías de redes sociales que afecten a los usuarios de manera negativa? y ¿Qué puede hacer el usuario para tener más control sobre el uso de sus datos?

MARCO TEÓRICO

2. ¿Cómo se obtienen los datos del usuario y porque es importante usar estos datos de forma ética?

En tiempos contemporáneos, el análisis de Big data se ha convertido en uno de los métodos principales para crear modelos de representación de actividades de consumo de los usuarios. Esto se refiere a que la Big Data permite a las compañías entender mejor a los clientes. Se puede averiguar cuáles son las tendencias de compras, el tipo de información que consumen, sus hábitos de navegación en línea y todo tipo de comportamientos que permiten predecir lo que el usuario podría querer comprar. En este capítulo se explicará cómo se pueden obtener los datos del usuario y porque es importante usar estos datos de forma ética.

2.1. Construcción de los algoritmos para redes sociales y la utilización de los datos del usuario.

Casi todos los sitios web que manejan un gran tráfico de usuarios utilizan herramientas de Big Data, incluyendo a las redes sociales. Los pioneros en la utilización de estos datos fueron grandes empresas de tecnologías, tales como Amazon, Google, Facebook, Instagram, Twitter y Snapchat. Desde que se desarrollo está tecnología de recolección de datos, las redes sociales han utilizado estas herramientas para mejorar la experiencia individual de los usuarios y ofrecer productos y servicios basado en sus necesidades y hábitos. Un algoritmo de búsqueda en Internet es un conjunto de instrucciones que describen el procedimiento a seguir para lograr encontrar un resultado determinado y concreto en la red, dentro de una estructura de datos de mayor envergadura (Hernandez, 2021). Todo lo que buscamos, publicamos o vemos en redes sociales (o incluso en los motores de búsqueda) se queda guardado. Los algoritmos utilizan toda esta información para predecir lo que nos gusta y promover contenido que nos puede parecer interesante. Esto incluye tanto contenido gratis como pago (anuncios).

2.1.1. Factores que se toman en cuenta al construir el algoritmo de una cuenta de red social.

En el libro escrito por García Canclini, Néstor "*Ciudadanos reemplazados por algoritmos*" se presenta la idea del ciber ciudadano. El ciber ciudadano es aquel que está presente en varios eventos noticiosos y que presenta una opinión publica gracias a herramientas como los blogs o las redes sociales. Hoy en día casi todos somos ciber ciudadanos, no solo con la capacidad de opinar desde cualquier lugar del mundo, sino también de influir en las decisiones de otros. El algoritmo de redes sociales se alimenta de esta interacción entre usuarios y la plataforma. Lo que compartimos con nuestros amigos, familiares y conocidos; y al mismo tiempo lo que ellos nos comparten a nosotros, crea una espiral infinita de retroalimentación del que las redes aprenden más sobre el usuario. Por ejemplo, el algoritmo de Facebook ve que las publicaciones de un usuario son humorísticas, por lo que le recomendará estas mismas publicaciones. Si varias personas comparten la misma información, el algoritmo se encarga de analizar que la información no rompa con sus políticas de privacidad y la denomina como "relevante". En el 2021, Facebook comenzó a utilizar un nuevo sistema que está tomando mucho apego. Otras redes sociales tales como Tiktok, Instagram y Youtube utilizan un modelo similar. El modelo es el siguiente:

1. Facebook primero busca todas las publicaciones en lo que se conoce como "inventario" del usuario (la totalidad de las publicaciones en la red del usuario) y se encarga de hacer un ranking de estas siguiendo diferentes parámetros como relevancia, tipo de publicación, viralidad etc.…

2. Después el algoritmo se encarga de quitar los posts no relevantes para el usuario y también delimita que contenido el usuario no quisiera ver (clickbait, desinformación, entre otras cosas).

3. El siguiente paso es tomar los posts restantes y pasarlos por una red neural (Inteligencia Artificial). Esta red crea nuevos rankings basados en parámetros más estrictos y personalizados para el usuario.

4. Finalmente el sistema apunta a una sección de contenido variado que el usuario puede considerar interesante o relevante.

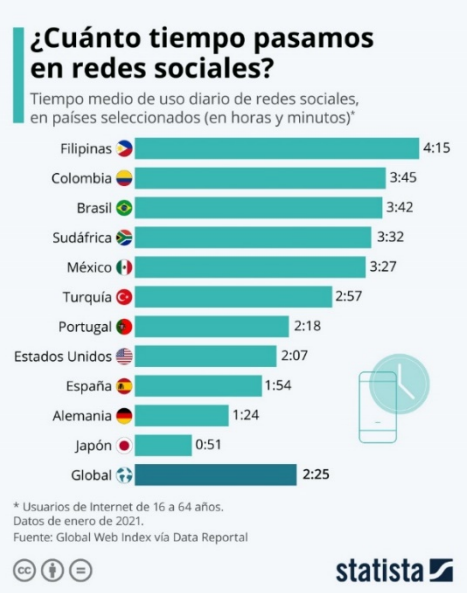
2.1.2. *Efectividad de estos algoritmos para entender las tendencias del usuario.*

El algoritmo va creciendo y aprendiendo del usuario cada vez más. De acuerdo a nuevos datos expuestos por Facebook, la efectividad del algoritmo de acertar en tus gustos es mayor del 95% ¿A veces no ha sucedido que estás pensando o hablando de algún artículo y de repente Facebook, Instragram o Tiktok te dan una oferta de lo mismo? Eso hace pensar que pareciera que nos están escuchando o espiando. Pero la realidad es que el algoritmo es tan increíble que es capaz de adivinar lo que queremos incluso antes de saberlo. Esto nos ha llevado a una nueva forma de consumir productos que se denomina como capitalismo electrónico. Gustavo Lins, empresario y autor del libro "*El precio de la palabra: la hegemonía del capitalismo electrónico-informático y el* googleísmo*".* denomina a esta nueva forma de capitalismo como "el capitalismo electrónico informático" (García, p. 81). Este nuevo modelo de negocios se enfoca en conocer al cliente más que nadie (incluso el cliente mismo). Si nos ponemos a pensar en redes sociales tenemos todo tipo de información relevante o sensible; desde nuestra fecha de nacimiento hasta nuestras inclinaciones políticas. Por esta razón los algoritmos son capaces de procesar nuestra información y saber exactamente en lo que pensamos o hacemos. Existe el ejemplo concreto y accesible que cualquiera puede usar llamado "Akinator". Akinator es nada más que un simple algoritmo de aprendizaje. No es ni remotamente tan complejo como el de Facebook, y sin embargo es capaz de adivinar lo que estamos pensando realmente. Si un juego web o móvil es capaz de saber lo que estamos pensando, imaginen lo que saben de nosotros las compañías a las que les damos literalmente toda nuestra información.

2.1.3. *Retención del tiempo del usuario.*

Las redes sociales buscan que retener al usuario por la mayor cantidad de tiempo posible. Para lograr esto se emplean tácticas psicológicas muy sutiles para que el usuario siga conectado (Moreno et alt,. 2020). Muchos hemos sentido que podemos ver un video o publicación más en Youtube o Tiktok antes de dormir, o podemos conseguir unos cuantos niveles más en ese juego de Facebook. Talvez, nos enteramos de algún escándalo interesante en Twitter y queremos ver lo que dice la gente por un momento más. Sin darnos cuenta ya pasó 1 hora más. De esta forma el usuario da más de su información y está expuesto por mayor tiempo a la publicidad. La gráfica 1 ilustra la cantidad de horas promedio que el usuario utiliza en redes sociales de acuerdo a datos recogidos este 2021.

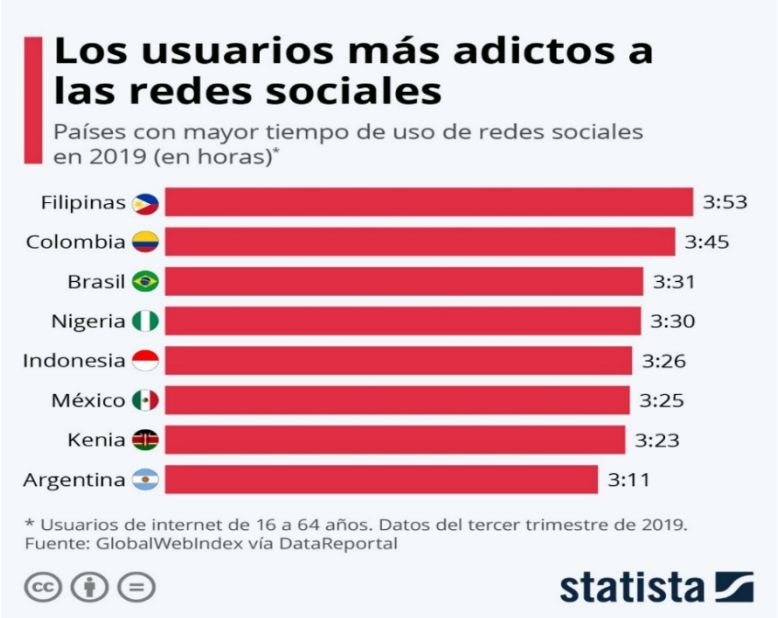
Gráfica 1: Promedio de uso de redes sociales en varios países 2021.



Fuente: Statista (2021)

Si lo comparamos con una encuesta similar realizada por la misma encuestadora en el año de 2019 en la gráfica 2, veremos que en varios países ha habido un pequeño incremento en el consumo de tiempo en redes sociales.

Gráfica 2: Promedio de uso de redes sociales en varios países 2019.



Fuente: Statista (2019)

Filipinas tuvo el incremento más grande con 22 minutos extra diarios, mientras que Colombia fue el único país que no presentó cambios. Si tomamos en cuenta al país con mayor consumo de redes sociales en esta encuesta, que es Filipinas con 4 horas y 15 minutos veremos que de hecho si se invierte una gran cantidad de tiempo estando en redes sociales. Es probable que los números sean aún mayores de lo que muestran las estadísticas. Por lo que se puede concluir que en varios países las personas emplean una gran parte de su día consumiendo redes sociales.

2.2. Manejo de datos del usuario de acuerdo a los términos y condiciones de varias redes sociales populares.

Las redes sociales tales como Facebook y Tiktok han crecido a ser algunas de las empresas más grandes de todo el mundo. Es verídico pensar que invierten millones y millones de dólares solo en publicidad. El claro propósito es el tener un sistema refinado y automático que trabajé y se mejoré por sí solo. En otras palabras, las redes sociales invierten mucho dinero para obtener nuestros datos y compartir esos datos con compañías para así poder vendernos todo tipo de publicidad. ¿Pero y que tipo de datos pueden utilizar o vender? ¿Pueden vender nuestros datos o no? De acuerdo con el sitio oficial del gobierno de Argentina, Argentina.gov, las redes sociales guardan toda la información que hemos ingresado en nuestras páginas desde el principio. Desde las conversaciones que hemos tenido, hasta la primera foto que publicamos. También nuestros contactos y datos personales. Incluso nuestra actividad en la web, si no estamos usando un servicio de encriptación o un VPN. También son capaces de saber que electrónicos utilizas, tales como celulares, televisores. Lo interesante es que todas las redes sociales si te avisan que pueden tener acceso a esta información, e incluso varias aplicaciones te piden permiso para acceder a tus contactos, cámara e incluso tu ubicación. De esta manera pueden conocerte y saber qué es lo que estas buscando. Esto incluye la publicidad que nos muestran.

Estos datos son utilizados para personalizar lo que vemos en nuestras redes. Facebook, Tiktok y Snapchat recomiendan videos que le pueden interesar al usuario; Facebook te recomienda nuevas amistades y Twitter personaliza el tipo de tweets que aparecen en tu página. También se utiliza estos datos para ofrecernos publicidad que esté personalizada a nuestras necesidades. ¿Sin embargo, que tanto se regula el uso de estos datos realmente?

2.2.1. *El uso de Big Data en redes sociales.*

En los últimos años las preocupaciones debido a brechas en varias compañías que se supone que son seguras, tales como Facebook o Sony, han crecido de manera significativa. Accidentes como la filtración de datos de cuentas de Playstation Network en 2014 o el caso de Facebook y Cambridge Analytica manipulando las elecciones de 2016, han hecho que varios gobiernos empiecen a reflexionar sobre la libertad que tienen estas compañías. El problema es que aún queda por hacer un largo trabajo. Las compañías de redes sociales solo han tomado rutas alternativas para continuar lucrando con el uso de nuestros datos para evitar problemas como el que tuvo Facebook contra el congreso de Estados Unidos. Ahora se utilizan APIs bien construidas, protocolos de intercambio de datos y aplicaciones de terceros para "compartir" la información de los usuarios con compañías (Jacobson, et alt., 2020, p. 2). El gráfico 3 explica cómo funciona este sistema.

Gráfico 3: Función general de un API

Fuente: Google (2020)

Es bastante razonable hacer esto para estas compañías. Después de todo los datos tienen un valor increíble en el mercado. Solo en 2018, Facebook generó 35.2 billones en ingresos publicitarios, el 63% del total de sus ingresos (ya incluido los costos del manejo y procesamiento de datos) (Shapiro, 2019). El valor de los datos obtenidos en redes sociales se ha incrementado en 85% desde el 2016 (Shapiro, 2019). Aunque no venden la información directamente, los nuevos sistemas les permiten dar toda la información a las empresas, mediante la intervención de terceros, sin tener que relacionarse directamente.

2.2.2. *Estatutos de los términos y condiciones de redes sociales.*

Cuando queremos comenzar nuestra propia cuenta en una red social, no tenemos más opción que aceptar los términos y condiciones. ¿Pero, y que estamos aceptando realmente? Muchas personas ignoran las implicaciones que puede haber al aceptar y simplemente lo hacen sin pensarlo. En este apartado se resumirá lo que algunas de las redes sociales más populares pueden hacer cuando se aceptan sus términos.

Facebook: al momento en el que hacemos click en aceptar, le estamos dando permiso a Facebook para utilizar nuestra propiedad intelectual (fotos/videos). En cuanto a lo que publicamos, si **nuestra cuenta está en modo "público" cualquiera es capaz de ver la información, incluyendo compañías y terceros**. Permites a Facebook **que una compañía le pague para recibir información de tu perfil** sin que el usuario reciba ni un solo centavo. Incluso **otras personas pueden distribuir la propia información del usuario a pesar de que se haya tomado medidas para que esta información no sea pública**. Si se comparte una foto en la que apareces, por ejemplo, ya estás dando información tuya sin siquiera haber dado permiso realmente. Ofreces tus datos de compra, transacciones, ventas entra otras cosas. Esto incluye **números de tarjetas de crédito**, datos de facturación, datos de contactos, proveedores, envíos y datos de cuentas. También estas dando información sobre tu **navegación web**, localización, paquetes de datos, proveedores web y telefonía, e incluso tus actividades (Facebook, 2016).

Whatsapp: a pesar de haber sido adquirida por Facebook, esta compañía tiene un poco más de control. Whatsapp puede utilizar tu información de contacto, así como de tu libreta de contactos. También les ofreces una licencia para utilizar cualquier información que utilices para reproducirla, distribuirla, **ejecutar la información**, o incluso **crear obras derivadas de esta**. No pueden utilizar los mensajes, guardarlos ni leerlos. Solo contenido que haya sido subido como fotos o videos (Whatsapp, 2021).

Instagram: Facebook compró Instagram en 2012. Por esta razón, sus políticas son bastante parecidas. Instagram puede acceder a datos personales de publicaciones y fotos que hayas subido que sean públicas. Ellos también **reciben una licencia donde pueden utilizar tu contenido de forma totalmente pagada** por utilizar su servicio. También estas aceptando que se pueda poner anuncios sobre, cerca o junto a tu contenido. Igual que con Facebook, el contenido que subas lo puede ver cualquiera, incluidos terceros y compañías. Tienen información de tus contactos, ubicaciones y dispositivos. (Instagram, 2021).

Tiktok: Tiktok es una de las redes sociales que ha emergido en los últimos años como una de las más populares. Tiktok puede acceder a datos personales de la cuenta del usuario, tales como fecha de nacimiento, correo, número telefónico, así como información de fotos y videos. Tiktok recopila información mediante encuestas, desafíos y competencias en las que el usuario participa. Igualmente pueden tener acceso a la información de navegación, datos del modelo de dispositivo, dirección IP, proveedores de internet y telefonía y ubicación. Igual que en varias otras redes, les otorga una licencia para poder usar **cualquier material, sin derecho a regalías** (Tiktok, 2021).

2.3. La importancia de la ética

Primero debemos definir lo que es la ética para empezar a hablar del tema y poder entender la importancia de la misma cuando se trata de tratar con los clientes y consumidores.

> "La ética es el estudio sistemático de la naturaleza de los conceptos axiológicos, como "bien", "mal", "correcto", "equivocado", etc., y de los principios generales que justifican la aplicación de ellos a alguna acción o acto. Su importancia radica en su relación con las nociones fundamentales de moralidad, y éstas pueden tener grandes consecuencias en relación con la conducta de las personas." (Soto y Pineda, 2007, p5).

La ética trata con el estudio y la definición de lo que en sí es bueno o malo. Por ejemplo, tratar de definir si la guerra y todas sus implicaciones resultan en algo malo o bueno. Es importante entender que la ética es un concepto que nos ayuda a clasificar que creemos que está mal. Sin ética, las personas se guiarían por instintos, por las decisiones de otros o adoptarían conductas basadas en el darwinismo para maximizar el provecho. Estableciendo reglas es como la sociedad crea moralidad y evita que se aprovechen unos con otros. A medida que pasa el tiempo, hemos creado nuevas formas de ética donde tenemos en cuenta a las grandes empresas que manejan grandes partes de nuestras vidas cotidianas.

Por ende, hay que mantener una ética estricta, en especial cuando se trata de empresas que afectan nuestras vidas diarias. ¿Pero, porque es importante tener una buena ética? La razón más importante es que hay que poner menos importancia al beneficio personal y pensar

más en la necesidad de las personas. Muchas veces hemos visto que las grandes compañías prefieren obtener beneficios rápidos en vez de pensar en el daño que pueden generar. Por ejemplo, las compañías petroleras que prefieren destruir a nuestro planeta incluso sabiendo el daño que causa. En el caso de esta investigación veremos más adelante como las compañías de redes sociales tienen esta misma forma de pensar. En varios casos, prefieren generar ganancias, a costa de los datos de las personas. Es importante tener en cuenta que tener una buena moral y ética puede ayudar a una compañía a generar la misma cantidad de ingresos que usando prácticas poco éticas. Es cuestión de generar confianza y ser transparentes con los usuarios. De esta forma evitamos que las compañías hagan lo que quieran sin tener consecuencias ante acciones poco éticas.

Eduardo Soto Pineda y José Antonio Cárdenas, realizaron un extenso trabajo sobre la ética en las organizaciones. En el capítulo 1 de este trabajo explican que mantener una buena moral debería ser una de las prioridades de las compañías. Esto debido a que se está perdiendo el pensamiento de moralidad sobre el bienestar de la persona. En los últimos años, se está dando más énfasis al consumismo. Grandes compañías de redes sociales, como Facebook y Twitter, invierten millones en buscar nuevas formas de utilizar sus datos, sin pensar en los aspectos éticos y morales. Se debe tener en cuenta la importancia de mantener una moral correcta debido a la cantidad de datos que se obtienen de los usuarios. Con estos datos se pueden generar perfiles inmensos de las personas, a tal punto que es posible incluso arruinar sus vidas. Por eso, se restringe la cantidad de datos que se pueden utilizar (en especial después de los acontecimientos del 2016 con la presidencia de Trump, en la cual se utilizaron datos para generar perfiles de votantes y poder manipular los votos). Sin embargo, aún se debe trabajar mucho para evitar que sea posible construir este tipo de perfiles. Cualquier uso de datos por parte del usuario es más que suficiente para generar todo un perfil del mismo (características, gustos, pensamientos hábitos, entre otras cosas). No es ético convertir a las personas en perfiles de datos que se estudian para maximizar las ganancias. Es importante que dejemos atrás el pensamiento de maximizar la productividad o las ganancias a costa de el bienestar de las personas. Si seguimos con este pensamiento, poco a poco se irá convirtiendo en algo más grave, donde las compañías van olvidando otros aspectos como el respeto a los trabajadores y los consumidores. Todo con tal de maximizar las ganancias.

2.4. La ética empresarial en redes sociales.

Soto y Cárdenas explican como los valores empresariales reflejan los principios de las personas o entidades que manejan a la empresa.

> "Los principios empresariales unen las razones de ser o de existir de una empresa con la forma en que ésta desempeña su función en la sociedad, integrando valores como honestidad, confianza, respeto, justicia y ética. Estos valores se convierten en prácticas empresariales a la hora de tomar decisiones. Por lo tanto, las prácticas empresariales son un fiel reflejo de los principios y valores de una empresa" (Soto y Pineda. 2007, p. 11).

Por ende, es importante mantener una ética alta en las empresas de redes sociales, donde las personas juzgan cada movimiento que harán estas empresas. Sin embargo, parece ser que el conflicto de intereses entre lo que quieren los usuarios y los accionistas es lo que dicta al final lo que hacen las empresas de redes sociales. Por ejemplo, Facebook y Twitter son conocidos por ser centros de mucha desinformación, que si llega a ganar tracción puede ser hasta promovida. Esto con el fin de generar el mayor tráfico posible en sus páginas.

Para muchas otras empresas, exigimos que tengan una actitud responsable, tanto para la comunidad como para el ambiente. Pero en el caso de las redes sociales, apenas si estamos empezando a darnos cuenta de que hay que hacer lo mismo. Por muchos años, parecía que las redes sociales tenían pase libre para hacer lo que quieran, ya que casi nadie entendía el valor de los datos. No es sino hasta el 2017 que se empezó a hacer escrutinio de lo que se podía y no hacer con los datos del usuario, gracias al caso de Zuckerberg contra Washington D.C. Las redes sociales deberían ser las compañías que más se acoplen a tener prácticas éticas y una moral alta. Después de todo, manejan uno de los aspectos más importantes de nuestras vidas: nuestra imagen pública. Sin embargo, vimos que estaban tratando de utilizar nuestros datos fraudulentamente el mayor tiempo posible, intentando no ser atrapados. Por esa razón, se les ha obligado a comenzar a cambiar sus políticas. Sin embargo, apenas se está comenzando y aún falta mucho trabajo para descubrir cómo utilizar los datos de las personas de forma correcta.

Soto y Cárdenas nos explican que "es importante evitar someterse a influencias impropias, favoritismos basados en intereses personales o presentar conductas que afecten la integridad de los ejecutivos" (Soto y Pineda. 2007, p15). La imagen de una empresa es lo

más importante que puede tener. Si las personas ven que no cumplen con lo que se promete, se genera desconfianza y la compañía sufre. Por esa razón, estamos viendo últimamente como las personas pierden la confianza en las redes sociales. Más adelante en este trabajo, veremos algunas repercusiones que sufrieron varias compañías de redes sociales por utilizar nuestros datos para lucrar. Las empresas deberían tratar de mantener una gran confianza con los consumidores. En cambio, muchas compañías de redes sociales tratan de tapar a toda costa lo que hacen con nuestros datos. En vez de tratar de confundir a los usuarios con términos de privacidad gigantes y palabras confusas, se debería ser claro y conciso con lo que la compañía puede o no utilizar. Así la gente podría controlar sus datos y estarían contentos con lo que las redes sociales les ofrecen, en vez de generar una gran desconfianza.

2.5. Implicaciones éticas del uso de datos del usuario de redes sociales.

Hay una clara responsabilidad ética que las redes sociales deben tener debido a la cantidad de datos que manejan. Es un tanto aterrador imaginar que existen compañías que saben todo sobre ti. Lo que te gusta, lo que no te gusta, tus miedos, tus metas, cuantas veces has fallado en algo y muchas cosas más. Es aún peor saber que puede ser un individuo que busque dañarte el que tenga acceso a tu información por culpa de una brecha de seguridad. El problema yace en que no existe tal cosa como privacidad en redes sociales. Legalmente, toda la información que está en redes sociales es considerada como pública, a menos que se configure como privadas. Esto se decidió en un caso de 2010 Romano vs Steelcase, en el que la compañía Steelcase buscó información del usuario en sus redes sociales para defenderse de la demanda impuesta por Romano (Moreno et alt,. 2013. p. 2). ¿Entonces para estar seguros simplemente se requiere ir a nuestra configuración y poner todo en privado y quitar todos los permisos de las aplicaciones? No realmente. Existe lo que se conoce como Data Scrapers (raspadores de datos). El Data scrapping se trata de recoger datos no estructurados de sitios web con bases de datos, para reestructurarlos y transformarlas en información útil (Messdaghi, 2020). Este es uno de los sistemas clave que se utiliza para ofrecer experiencias personalizadas para los usuarios, como anuncios relevantes o videos que te pueden gustar. El problema recae en que hay personas fraudulentas que utilizan este sistema para recrear datos personales y venderlos a terceros o incluso utilizarlos para beneficio propio. De hecho, pocas veces estos son hackers, y más veces son compañías que tratan de evadir las reglas de los términos de condiciones en las redes para vender la información. El sistema que Facebook utiliza para controlar esto es automatizado, por lo que es propenso a muchas fallas. Igual ocurre con LinkedIn, Instagram, Youtube, Twitter y

Tiktok (Scroxton, 2020). Las redes sociales han visto mucha atención negativa en los últimos años debido a que estos fallos están empezando a ocurrir más frecuentemente. ¿Está realmente protegida la información que exponemos en redes sociales?

2.5.1. *Manejo indebido de los datos del usuario en los últimos años.*

Los casos más conocidos del manejo poco ético de datos son los de Brexit y Cambridge Analytica, quienes obtuvieron datos de Facebook que explotaron para influir en diferentes elecciones en 2016 (Estados Unidos y Bretaña). En 2018 y 2019 ocurrieron varias brechas de seguridad en Facebook que llevó a la filtración de más de 533 millones de usuarios. Sin embargo, dos años más tarde, la misma filtración volvió a resurgir. LinkedIn tuvo el mismo problema en 2021, con la filtración de 500 millones de usuarios. Ambas compañías trataron de justificarse diciendo que la información era pública, y que no tuvieron la culpa de que los data scrappers hayan aprovechado esto (Hutchinson, 2021). En 2019 Facebook accidentalmente filtró información por su cuenta de 1.5 millones de usuarios (Price, 2019). En 2020 ocurrió un suceso similar implicando a Youtube, Tiktok e Instagram. Una compañía tercera (que igualmente era data scrapper) dejó una base de datos sin seguridad de más de 235 millones de usuarios de las tres redes sociales (Scroxton, 2021). Otro elemento más general es que muchas redes sociales, tienen un bajo escrutinio de las aplicaciones y servicios de terceros que pueden conectarse a las mismas.

> En 2019, existieron varios casos en las cuales aplicaciones que pagan al usuario por realizar encuestas, utilizaron los datos recopilados para diferentes cuestiones poco éticas. Entre estas se encuentran: la creación de cuentas fantasmas para monitorear a no usuarios de redes, el uso de los datos para investigaciones psicológicas con el fin de incrementar el tiempo de uso de redes, y el uso de información por parte de instituciones como instituciones educativas, gobiernos y negocios para mantener el control (Farooqi, 2020).

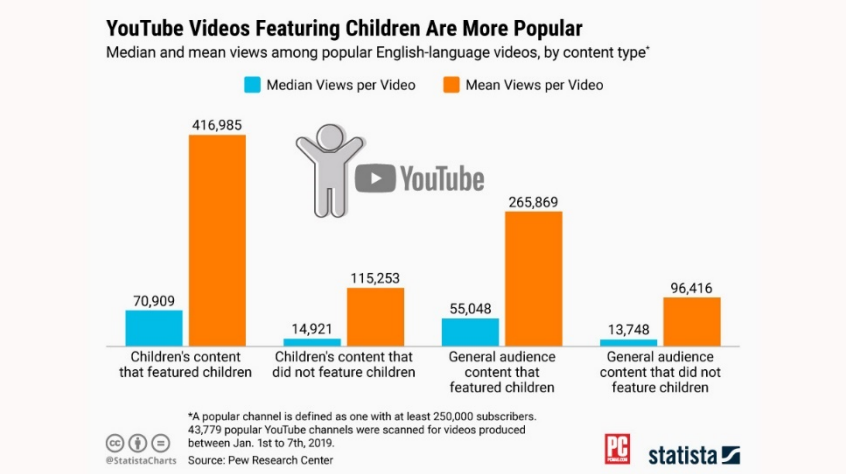
Otro punto importante que tocar es el de Youtube. Youtube genera sus ganancias mediante el uso de publicidad dirigida a los usuarios, como todas las redes sociales. Youtube se ha convertido en la principal plataforma para que las personas vean reseñas de productos pagadas (sponsors) y decidan hacer compras. En la gráfica 4 se muestra el nivel de crecimiento en los últimos años de la plataforma en cuanto a ventas se refiere.

Gráfica 4: Crecimiento en ventas de Youtube

Fuente: Think With Google (2021)

Youtube es una plataforma que tiene su mayor público en las visitas de niños menores de 13 años. En los últimos años la FTC (Federal Trade Comissión), que es una organización que protege a los consumidores de Estados Unidos, puso a Youtube bajo un increíble escrutinio. Esto debido a que los algoritmos de Youtube elegían contenido totalmente inapropiado para niños ya que era lo que más se veía. Ahora Youtube ha creado elementos como Youtube Kids o la creación de un nuevo sistema que te obliga a decir si tu contenido es para niños. Sin embargo, esto resulta ser una fachada que tapa que realmente están continuando con el contenido poco ético. Chandra Steele es una escritora de la revista PC Mag, una revista de tecnología. Ella quería saber e investigó si todavía los niños eran el público más grande en 2019. Descubrió que los videos vistos por niños reciben 3 veces más visitas que todos los demás videos. La gráfica 5 nos muestra los números.

Gráfica 5: Niños viendo Youtube en 2019



Fuente: Statista (2019)

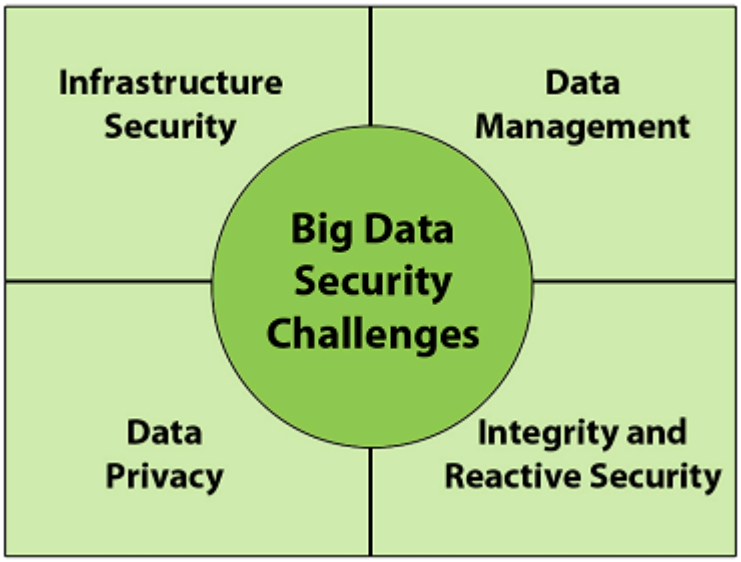
Realmente la implementación de Youtube Kids y las restricciones de contenido para menores no ayudo en mayor medida. El algoritmo de Youtube continúa recomendando contenido inapropiado para menores. El problema yace en que el sistema de todas las redes sociales es fácil de acceder para cualquier persona. Cualquier niño o niña puede mentir sobre su edad y solo continuar viendo cualquier contenido. ¿Pero, es realmente factible pedir a las redes sociales que cambien este sistema? Tendría que existir un cambio fundamental de como funcionan las redes sociales para proteger a los menores del uso de sus datos para ofrecerles contenido inapropiado. Aún estamos lejos de tales cambios, ya que por el momento las ganancias monetarias son la prioridad. Se debe abrir canales de discusión para entender y manejar estos temas de mejor manera.

2.5.2. *¿Qué sistemas utilizan las redes sociales para proteger nuestra información?*

Hay un último elemento importante que se debe hablar cuando se trata de la seguridad del usuario en redes. Este es que las redes sociales han preferido utilizar tecnología vulnerable para manejar su Big Data debido al bajo costo de mantenimiento. Este sistema es conocido como Hadoop. Hadoop es un sistema que permite almacenar y procesar una inmensa cantidad de datos en varios servidores, gracias al manejo simple de conglomerados de computadoras (Moreno et alt,. 2020. p. 2). Es prácticamente el servicio predeterminado en lo que a Big Data se refiere. Es un servicio muy útil, eso no se puede negar. Sin embargo, sufre mucho en lo que a los 4 pilares de Big Data se refiere. Estos 4 pilares se refieren a un

esquema que demuestra las amenazas que conlleva el utilizar la Big Data. La gráfica 6 muestra el esquema de los 4 pilares.

Gráfica 6: Esquema de los 4 pilares de la seguridad en Big Data



Fuente: Research Gate (2020)

Principalmente son cuatro aspectos diferentes de la seguridad de Big Data: seguridad de la infraestructura, privacidad de los datos, gestión e integridad y seguridad reactiva (Moreno et alt,. 2020. p. 2). El servicio de Hadoop falla bastante en casi todos los ámbitos. En cuanto a la seguridad de infraestructura, el sistema de Hadoop ha sido tópico de discusión entre los expertos de seguridad informática. En resumen, los problemas de seguridad comienzan cuando el enorme volumen de datos almacenados en una base de datos no está en formato normal o no están cifrados (Moreno et alt,. 2020. p. 2). En cuanto al manejo de datos, el sistema muestra problemas debido a la inmensa cantidad de datos que se manejan. No todos los datos terminan siendo protegidos y los data scrappers y los hackers aprovechan esta información (Moreno et alt,. 2020. p. 9). En cuanto a la privacidad de datos, este sistema utiliza esquemas simples de protección de información, tales como controles de acceso (para evitar a los indeseados) y criptografía simple. Esto termina siendo poco eficiente para proteger la información del usuario ya que al final la información que ofrecen las redes es pública (Moreno et alt,. 2020. p. 7). Finalmente, en cuanto a gestión e integridad y seguridad reactiva se trata, la información necesita seguir un proceso para verificar que no haya sido alterada o modificada al momento de procesarla. Este es el momento donde la información es más vulnerable a ser copiada o robada. El problema yace en que este sistema todavía no

tiene una solución factible, ya que la inmensa cantidad de datos hace difícil cumplir esta tarea (Moreno et alt,. 2020. p. 10). Con todo esto podemos ver que el sistema que utilizan, tanto redes sociales como otras compañías, es explotable. Y no es sino hasta recientemente que se ha puesto bajo escrutinio a las compañías que manejan las redes sociales, como es el caso de Facebook y LinkedIn con la filtración de información este 2021. Sin embargo, se puede ver un paterno donde las compañías de redes sociales admiten que hubo un error, se disculpan y todo vuelve a la normalidad, con poca o casi ninguna consecuencia, con excepción de Facebook que si tuvo que pagar una multa de 5 billones por filtrar información crucial de los usuarios en 2016. Aun así, continúa siendo la red social más grande del mundo y generando ganancias inmensas a costas de nuestra información.

2.5.3. *Posibles repercusiones debido a la mala utilización de los datos del usuario.*

Para todas las redes sociales este debería ser el punto más importante que trabajar y mejorar. Sin embargo, al menos en los últimos años, parece ser que las compañías de redes sociales están dejando de lado estos aspectos para enfocarse más en mejorar sus algoritmos de recolección de datos. Es importante no olvidar que el usuario no es simplemente un número que puede ser procesado y explotado. Existen repercusiones graves para el usuario cuya información es filtrada o compartida con terceros que no respetan las condiciones impuestas en las redes.

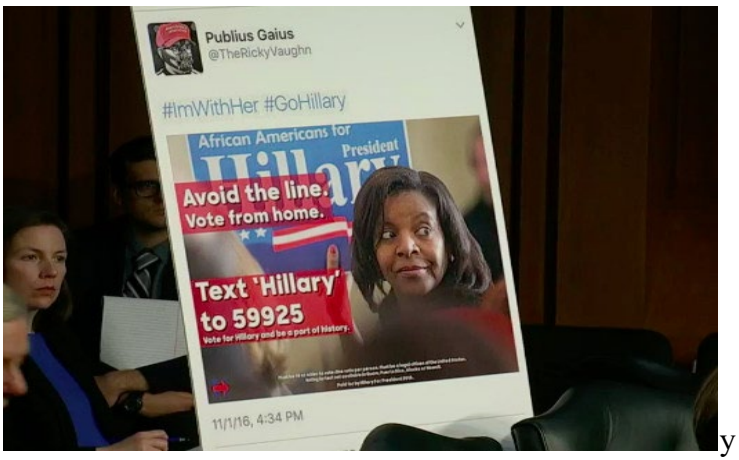
> "En el caso de Facebook y LinkedIn en 2021, los hackers postearon la información de 2 millones de usuarios solo para probar que podían hacerlo. Varias contraseñas fueron vulneradas, incluida cualquier información de tarjetas de crédito que estuviera guardada en las cookies. También se compartieron datos de ubicaciones, nombres y hasta lugares de trabajo" (Hutchinson, 2021).

Google acudió rápidamente a tratar de ayudar a las personas vulneradas pidiendo que cambien cualquier contraseña que detectaron que fue vulnerada, pero los datos ya se podían conseguir fácilmente en sitios de la Deep web.

Las noticias falsas también han surgido como un evento en el cual la información y la publicidad pueden ser usadas de maneras dañinas. Utilizando el mismo ejemplo de la campaña de 2016, varias cuentas fueron creadas para publicitar desinformación. En la gráfica 7, veremos una cuenta creada en Rusia que utilizó $100.000 dólares para difundir publicaciones que trataban de engañar a la gente para que no votará en las elecciones de

Estados Unidos en 2016 (The Great Hack, 2019). El algoritmo de las redes sociales más prominentes (Facebook, Twitter, Instagram), vio la popularidad de estas publicaciones y comenzó a mostrarlas a más personas influyendo negativamente en las votaciones de ese año en Estados Unidos. Esta era solo una de las muchas que fueron creadas para estas elecciones, que fueron creadas con la información obtenida de Cambridge Analytica y estaban diseñadas con un público específico en mente (este público fue seleccionado de manera específica utilizando los datos de las personas que eran más vulnerables a ser engañados de acuerdo con el logaritmo obtenido de las redes sociales).

Gráfica 7: Voten por texto por Hillar



y

Fuente: Vox (2020)

Finalmente, una repercusión bastante importante es que se está creando un ámbito social donde la importancia de un individuo se mide por sus logros en redes sociales. El algoritmo de las redes sociales promueve la creación de perfiles unidimensionales que no muestran la realidad del usuario (Grupo Cyberwaters, 2021). Hemos visto en varias redes, como Instagram o Facebook, que las personas pasan horas retocando sus fotos para crear la imagen perfecta. Estos perfiles suelen tener más visitas y clicks, lo que hace que el algoritmo de redes sociales promueva estas tácticas. Las personas empiezan a proyectar realidades que no son verdad para aparentar estar mejor de lo que realmente están. Esto crea una peligrosa espiral donde las personas que fabrican realidades son las que son aceptadas socialmente, mientras que las personas que no siguen al algoritmo tienen menos valor social y por ende contribuyen menos a la sociedad (Grupo CyberWaters, 2021). Pero esto solo resulta ser una táctica poco ética para que las personas que estén compartiendo la mayor cantidad de datos sean las más promovidas en las diferentes plataformas. Si no estas compartiendo hasta el último detalle de tu vida, el algoritmo de redes sociales prefiere ignorar tu perfil, mientras

que aquellos que lo comparten todo son el público preferido ya que están compartiendo más datos. Sin darnos cuenta, nos condicionan mentalmente para ofrecerles todos nuestros datos en bandeja de plata.

2.6. Opinión experta sobre la relación entre los datos del usuario y las redes sociales.

2.6.1. *La apatía del usuario ante el uso de sus datos.*

Hoy en día no está de más decir que una gran cantidad de gente tiene al menos una red social que utiliza casi todos los días. Hay muchas consideraciones importantes que se deben tener en estos tiempos de conectividad casi perpetua. Sin embargo, casi nadie tiene en cuenta los problemas que existen debido al uso indebido de datos de las personas. Esto preocupe a varios expertos en uso de datos que creen que se debería tener más control sobre estas actividades. Carlos Barriuso Ruiz, profesor asociado de Informática Jurídica Universidad de Alcalá, es uno de los muchos expertos que explica cuál es el problema con los datos. De acuerdo con el profesor Ruiz las compañías no buscan la obtención de datos por buscar mejorar la experiencia del usuario. Más bien se busca encontrar como mejorar la publicidad sabiendo lo que le gusta y no le gusta al usuario, siendo la diferencia que el usuario no entiende la cantidad de información que se obtiene del mismo. Esto se puede comparar con la publicidad normal. Es verdad que la publicidad ha existido desde hace mucho y existirá siempre. Pero en el pasado, la publicidad no tenía mucho con que trabajar. Se podían crear grupos focales para ver que le gustaba a la gente. Esto no va a funcionar con todas las personas obviamente. Pero, realmente desde antes ya se utilizaban formas de control psicológico. Una de las primeras formas de esto fue el FOMO (Fear of missing out). Esto es el miedo que se genera en las personas de no formar parte de algo, como por ejemplo tener el último Iphone. Y esto se logró descubrir sin tener los datos de lo que querían realmente los usuarios. Ahora con el poder que tienen los expertos de marketing para conocer todo sobre nosotros con nuestros datos, imagínense el nivel de control que pueden tener sobre nosotros. El profesor Ruiz explica que mientras más datos estén disponibles para el análisis y más poderosas sean las herramientas de análisis, más significativa será la información que se obtenga y más riesgos habrán de vulnerar la intimidad y las prescripciones sobre protección de datos personales. Pero, lo realmente preocupante de esto es que al usuario no le importa que se tenga este nivel de control. Se ha vuelto una relación en la que el usuario cede sus derechos sobre sus datos como si fuera algo tan normal como respirar, lo que no debería ser el caso.

2.6.2. *Los usuarios son más importantes siendo números explotables.*

Con la implementación de la red 2.0, que fue la red que comenzó con la conectividad interpersonal o las redes sociales como se conocen, vino una nueva oleada de empresas que vieron la oportunidad que se generaba. La autora del libro "*La cultura de la conectividad: Una histórica critica de las redes sociales*", José Van Djick, investigadora y profesora de la Universidad de Amsterdan, explica que las compañías como Facebook o Twitter no vieron esto como una oportunidad para conformar una comunidad de usuarios, sino más bien como una oportunidad para obtener acceso a datos personales.

Debido al increíble crecimiento de la conectividad social que se ha generado en estas dos últimas décadas, es difícil no decir que las redes sociales son los actores de cambio más grandes en la sociedad. El problema de esto yace en la cotidianidad que se le ha otorgado a la práctica del uso de redes sociales. Ahora ya es casi imprescindible tener cualquier red social, simplemente por la necesidad de estar conectado con los seres queridos. Djick explica que es esto lo que las compañías de redes sociales apuntan a lograr. Que seas dependiente, que no puedas existir sin ellas, el tenerte atrapado. No se puede negar la utilidad infinita que nos otorgan estas herramientas. Sin embargo, hay que hacer esa distinción: es una herramienta. No controla nuestras vidas ni somos dependientes de ellas. Pero, ¿cuántas veces hemos visto que nuestro familiar o conocido no salen sin su móvil? Djick explica que las redes sociales lograron su cometido de convertirse en el verbo. ¿Qué significa esto? Significa que las redes sociales se inmiscuyeron tanto en nuestras vidas que, sin darnos cuenta, hasta sustituyeron a palabras reales para alguna acción. Por ejemplo, uno ya no dice buscar en internet, sino Googlealo. Tampoco decimos estoy haciendo microblogging, decimos haz un tweet. O tampoco decimos que estoy escuchando música, sino estoy escuchando Spotify. A tal punto llegaron las redes sociales que mucha gente no puede desempeñar sus actividades diarias sin ellas e incluso algunos se vuelven adictos. Los expertos como Djick, Ruiz y Ramonet se preocupan por esto debido a que no ven acción mayor por parte de las compañías de redes sociales para regular este dilema y al usuario no le interesa hacer un problema sobre esto. Es más, a ellos les conviene mucho que el usuario esté pegado al celular todo el día y este expuesto a la publicidad. De esta forma se puede obtener la mayor cantidad de datos posibles del usuario.

2.6.3. *Los usuarios no reclaman los derechos de sus datos.*

Otro problema importante que ven los expertos es el estado del derecho de los datos. Yasmina Soto, Licenciada en Humanidades de la Universidad de Barcelona explica en su trabajo "*Datos masivos con privacidad y no contra privacidad* " que la anonimización de los datos se había considerado la garantía para cumplir con las regulaciones existentes sobre la protección de datos personales. Sin embargo, la mayoría de las veces ese ya no es el caso. Esto se refiere a que ya no existe tal cosa como anonimización de los datos. El usuario puede hacer todas las trabas posibles para esconder sus datos personales en redes sociales. Sin embargo, las redes están construidas de forma que todo está conectado. Una vez que alguien más comparte tu información, sea por una foto compartida o porque subieron sus contactos, ya no estas en estado anónimo, incluso si no estas en redes sociales. Se crea una cuenta fantasma, que igualmente tiene tus datos obtenidos mediante la persona que creo su cuenta. Entre más gente que conozcas se una, y den sus contactos que te incluyan, más aprenden las redes sociales sobre ti, todo esto pudiendo suceder sin que siquiera hayas creado una cuenta. Hay formas de evitar esto, pero se requiere de un conocimiento exhaustivo de la red social que utilizas para cambiar estas opciones. En otras palabras, es lo más difícil posible a propósito. Ni siquiera se ayuda a los que ya fueron afectados por esto, solo a los futuros contactos que tenga el usuario. Y siendo realistas, ningún usuario se toma la molestia de cambiar esto, o ni siquiera saben que pueden ya que las redes sociales hacen lo posible para esconder estas reglas tras páginas de texto. Los datos del usuario no son suyos ni son privados, a pesar de que se le diga que sí lo son. Por eso, los expertos como Yasmina, buscan que se haga responsable a redes sociales como Facebook y Twitter, por el uso indebido de los datos de las personas.

2.6.4. *La dicotomía del aspecto social y el aspecto económico de las redes sociales.*

Un último aspecto importante que topa Djick en su libro es el tema del aspecto "social" en las redes sociales y la dicotomía que existe en las redes. Nos explica que el uso de la palabra en estas plataformas sociales implica un centro del interés en el usuario y facilitan la realización de actividades comunitarias. Se entiende que las redes sociales potencian, la interactividad y conectividad humana y lo promueven como un valor social importante. Y ya que son conexiones humanas se entiende que las personas serán afectadas en su modo de pensar y hacer. El énfasis se encuentra en el humano y sus conexiones con otros. Pero de igual manera, las redes sociales se construyen con sistemas automatizados que

diseñan y manipulan estas conexiones. Para poder dar a la gente lo que desea, se les reduce a algoritmos y números. ¿Entonces se está realmente fomentando la conexión humana? Hay una complicada dicotomía entre lo que se quiere como compañía y lo que se quiere como herramienta para ayudar a la humanidad. Por un lado, somos números que se cuentan, y por otro lado estamos conectados con nuestros seres queridos. Las grandes redes sociales tienen que lidiar con ese dilema ético todos los días (y muchas de ellas como Facebook caen ante la tentación de vernos como números y dinero). Para ofrecernos un mejor servicio de conectarnos, tienen que convertirnos en números. Es en ese momento cuando las redes sociales nos recuerdan porque generan tantos millones de dólares al año. Muchas se inclinan más al lado técnico y se olvidan de lo social. El propósito se convierte en generar ganancias, y conectar a las personas queda en segundo plano. Es por eso que, en estos últimos años, hemos tenido que ver caso tras caso de redes sociales teniendo que disculparse porque vendieron nuestros datos a terceros. Y tras todas estas disculpas, continúan haciendo todo esto, generando ganancias billonarias cada año.

METODOLOGÍA

3. Importancia de los datos

En este apartado se determinará cual es el método más efectivo para responder a las preguntas que nos ayuden a lograr los objetivos de la investigación. También se va a desarrollar el método de recopilación de datos más efectivo para desarrollar un marco de referencia de datos. Esto se hace con el propósito de entender cuál es el nivel de entendimiento de los usuarios de redes en varias cuestiones propuestas por las preguntas de investigación y los objetivos generales y específicos.

La obtención de datos es un tema polémico que se ha tratado muy poco en los últimos años. Hasta el día de hoy se sigue discutiendo sobre cómo se deberían manejar los datos de las personas. ¿Son los datos propiedad del usuario? ¿Las compañías pueden saber tanto de nosotros? ¿Cuál es la línea que no se debe cruzar entre privacidad y personalización? El objetivo de esta investigación es averiguar hasta qué punto sabe el usuario sobre el manejo de sus datos personales por parte de las compañías de redes sociales.

3.1. Determinación del tipo de proyecto y recolección de datos.

Este proyecto requiere de una investigación del usuario tipo cuantitativo. Es importante utilizar la recolección de datos para comprender cual es el nivel de entendimiento del usuario sobre el uso de sus datos personales. Así se podrá afirmar o desmentir la hipótesis. Por eso el método de recolección de datos más efectivo para esta investigación es utilizar encuestas. Las encuestas permiten obtener datos primarios de los mismos usuarios de redes. De esta forma podemos hacer uso de los datos y saber si el usuario está afectado negativamente por el uso de los datos en redes. La encuesta está compuesta por 10 preguntas, en las cuales se buscó ver el nivel de conocimiento de 40 usuarios sobre big data y cuanto conocen sobre el uso de sus datos. Los encuestados son usuarios promedio de redes sociales entre 20 a 30 años que utilizan redes sociales por más de 2 horas al día. Estas son las personas que más permiten que se utilicen sus datos personales.

RESULTADOS

4. Análisis de los datos

El método de análisis de datos es un análisis descriptivo de las opiniones de los usuarios de redes. En este método se busca tener un entendimiento de las características detectables de los usuarios, mediante un entendimiento de los datos procesados. Con este análisis se puede entender las tendencias e indicadores de los usuarios y permite definir y demostrar la hipótesis. En este trabajo en específico, se busca analizar si la hipótesis del estudio es correcta.

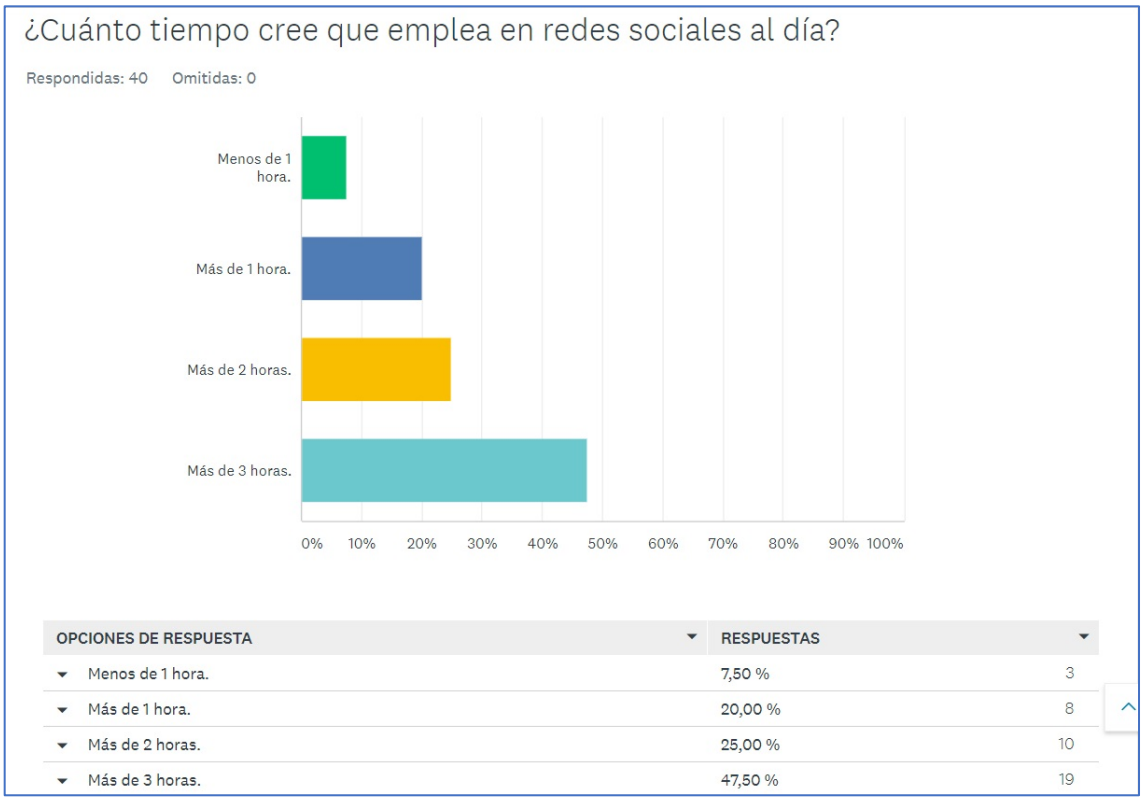
En este capítulo se muestra el análisis de los datos presentados en la encuesta. Con los datos cuantitativos obtenidos en la encuesta se podrá determinar si las personas sienten que las redes sociales están creadas con el fin de mantenerlos conectados el mayor tiempo posible, para así poder obtener y explotar sus datos. También se determinará si las personas sienten que las redes sociales utilizan su información de forma ética o no.

Con esta información se puede reforzar la hipótesis sabiendo que las personas reconocen los comportamientos que se explicaron en este trabajo, como, por ejemplo, la adicción que existe a las redes sociales o la apatía que existe, ante el uso de los datos, para generar ganancias mediante el uso de estos datos para fines comerciales.

4.1. Tiempo consumido utilizando redes sociales por el usuario promedio.

Lo primero que se quería saber en esta investigación es el tiempo de consumo en redes sociales.

Gráfica 8: Tiempo consumido en redes sociales por usuarios de Quito al día



OPCIONES DE RESPUESTA	RESPUESTAS	
Menos de 1 hora.	7,50 %	3
Más de 1 hora.	20,00 %	8
Más de 2 horas.	25,00 %	10
Más de 3 horas.	47,50 %	19

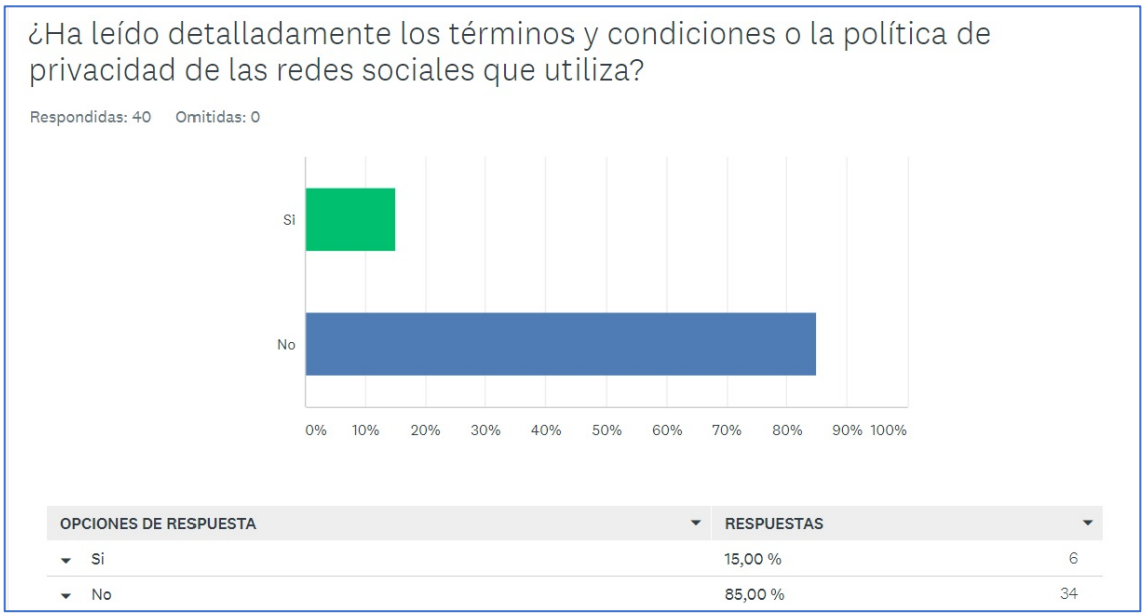
Fuente: Elaboración Propia

El 47,5% de los usuarios emplean más de 3 horas en redes sociales, mientras que solo el 7,5% emplea menos de 1 hora. Esto demuestra que las redes sociales ocupan una gran cantidad de tiempo en la vida diaria del usuario.

4.2. Conocimiento de los términos y condiciones.

Segundo se investigó si las personas que consumen redes sociales están al tanto de los términos y condiciones o de las políticas de privacidad de las redes sociales que utilizan.

Gráfica 9: Porcentaje de usuarios que han leído los términos y condiciones.



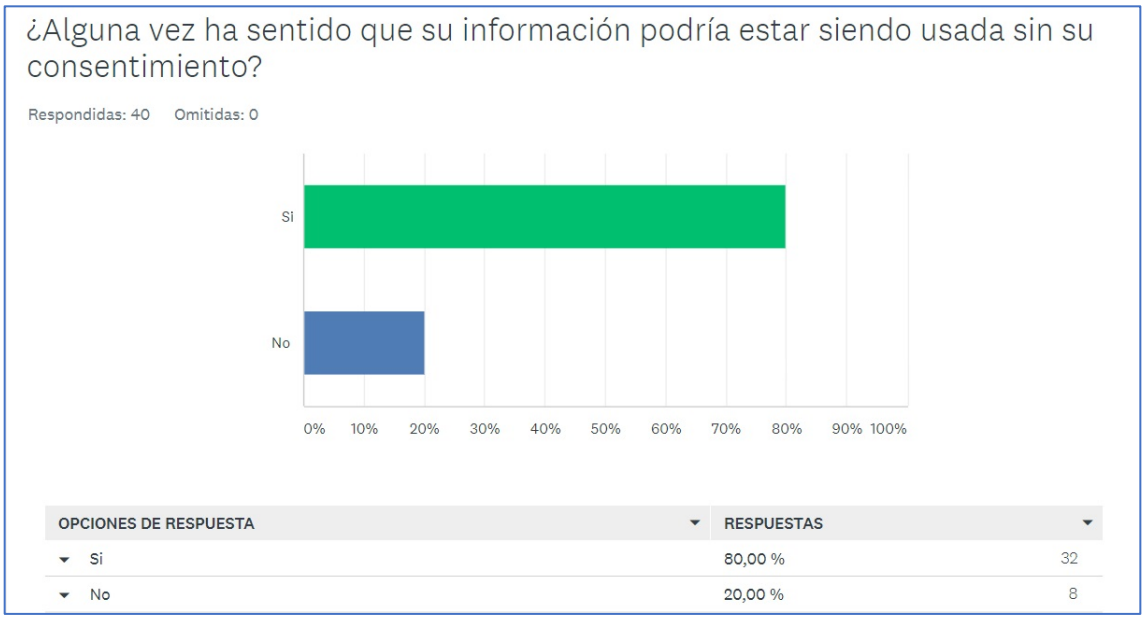
Fuente: Elaboración Propia

El 85% de las personas indicaron que no han leído detalladamente los términos y condiciones. Esto se puede deber a muchos factores, tales como que estas políticas y términos están escritos para que el usuario se aburra y no los lea. Se emplean muchísimas líneas de texto y se utilizan términos confusos para la persona promedio. Si lo comparamos con la firma de un contrato legal importante, no existe diferencia. Después de todo estás cediendo muchos derechos personales al aceptar los términos. Sin embargo, no se toma el mismo escrutinio para leer entre líneas que se toma con otros tipos de documentos. Esto se puede deber a elementos demostrados en este trabajo como la dificultad y longitud de los textos empleados a propósito.

4.3. Uso sin consentimiento.

Tercero se investigó si los usuarios creen que su información ha sido usada alguna vez de manera indebida o sin su consentimiento.

Gráfica 10: Uso de información sin consentimiento.



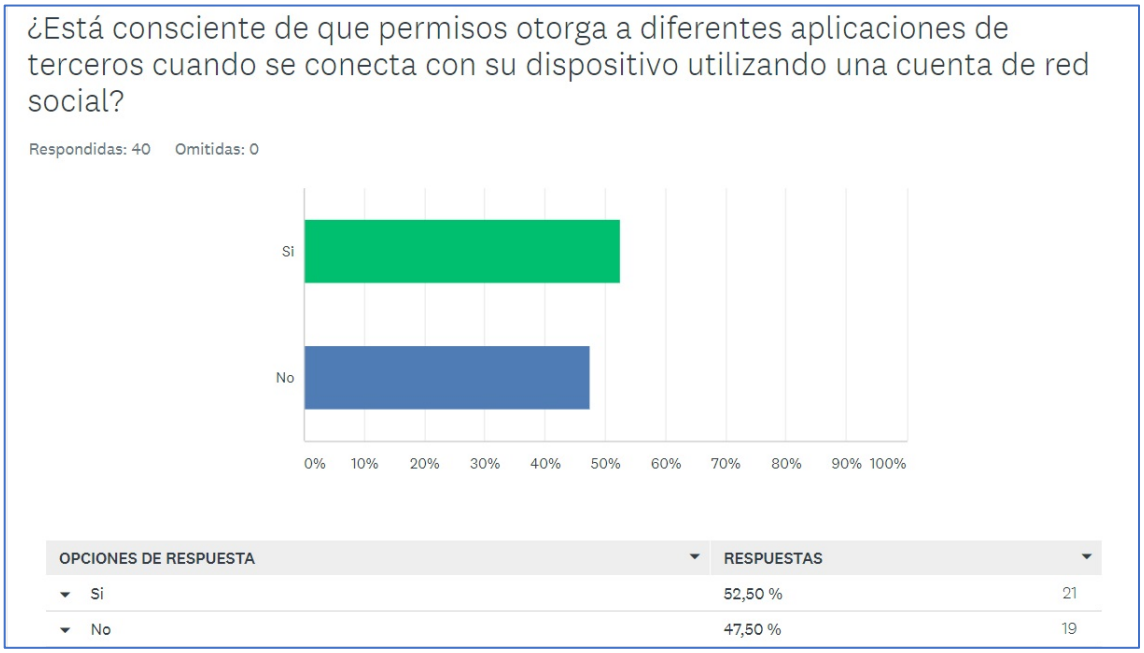
Fuente: Elaboración Propia

El 80% de los usuarios demostraron que sienten que en alguna ocasión su información ha sido utilizada sin su permiso. Esto es destacable sabiendo que las personas emplean una gran cantidad de tiempo en redes. ¿Aun temiendo de que su información esté siendo compartida, porque se emplea tanto tiempo en redes? Esto demuestra una tendencia a la dependencia o una adicción. A pesar de que la mayoría entiende que hay un comportamiento dañino hacía ellos, continúan regresando diariamente.

4.4. Permisos otorgados

Cuarto se investigó si las personas conocen que permisos están otorgando a las diferentes redes sociales cuando aceptan que se utilices cosas como su cámara o su ubicación.

Gráfica 11: Conocimiento de permisos otorgados para redes sociales.



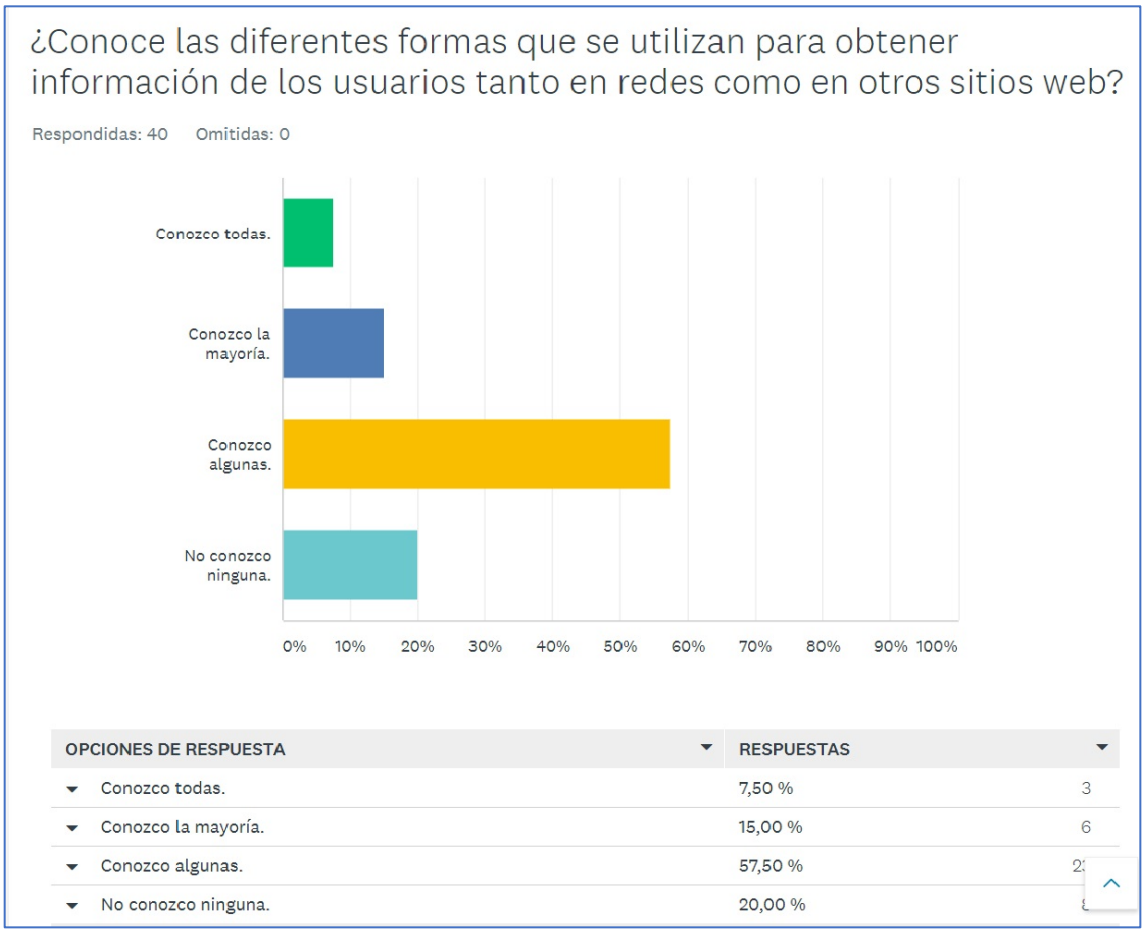
Fuente: Elaboración Propia

El 52,5% de usuarios dijeron conocer que permisos otorgan, mientras que el 47,5 no sabe. Sin embargo, aquí se ve una contradicción con los datos obtenidos anteriormente. Esto lo podemos ver debido a que en la pregunta 2 el 85% de usuarios dijo que no han leído detenidamente los términos y condiciones. Para conocer realmente los tipos de permisos que otorgan al aceptar es necesario leer los términos. Podemos inferir que muchas personas creen que saben lo que están aceptando, pero realmente solo están aceptando sin pensarlo realmente. El otro 47,5% muestra que realmente no conocen lo que están aceptando.

4.5. Conocimiento de obtención de datos

Quinto se investigó si el usuario sabe las formas que se utilizan para obtener sus datos.

Gráfica 12: Porcentaje de conocimiento sobre obtención de datos en redes.



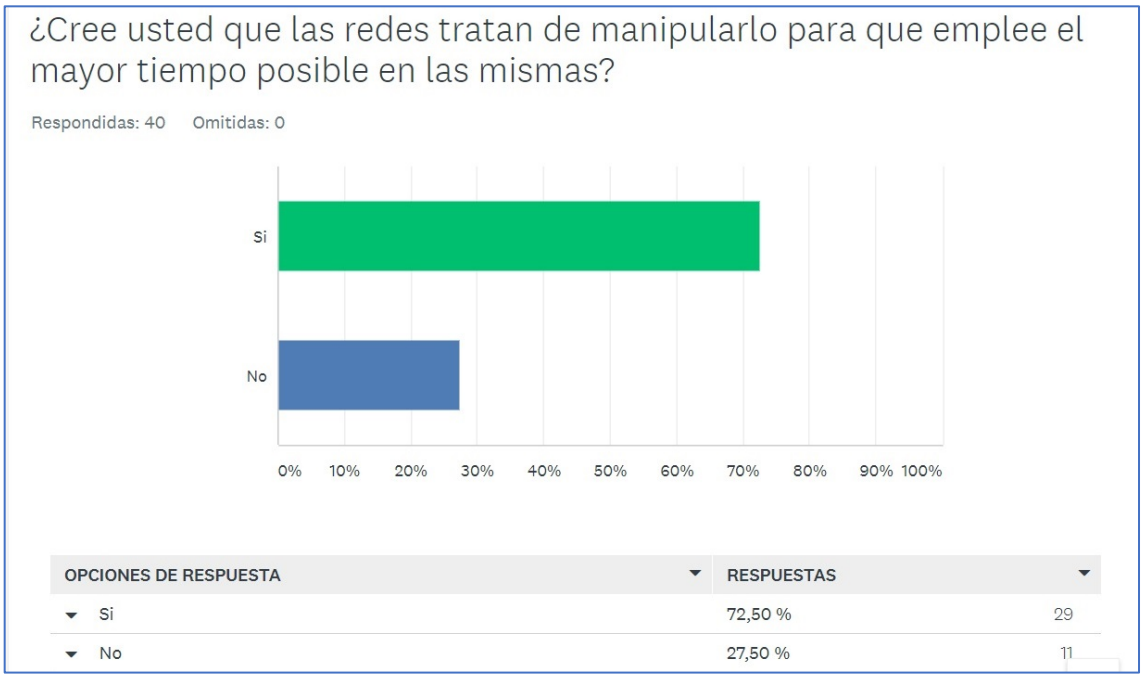
Fuente: Elaboración Propia

Un pequeño porcentaje de personas (7,5%) respondió que conoce todas las formas. Otro pequeño porcentaje (15%) respondió que conoce la mayoría. Estos porcentajes correlacionan con la población nicho que talvez es más familiar con la tecnología del Big Data. En cambio, parece ser que el usuario promedio sabe que se están recogiendo sus datos de alguna forma, pero no sabe específicamente como. El 57,5% respondió que conoce algunas formas. Mientras tanto, el 20% de los usuarios no saben cómo se están recogiendo sus datos. Estos dos porcentajes correlacionan con la mayoría de la población que sabe nada o muy poco sobre tecnología de Big Data. Y como ya se explicó en este trabajo las redes hacen muy poco para que se conozca que datos pueden estar siendo compartidos.

4.6. Percepción del usuario sobre la manipulación utilizada por las redes sociales.

Sexto se averiguó si el usuario de redes cree que está siendo manipulado de alguna forma.

Gráfica 13: Manipulación de redes en los usuarios.



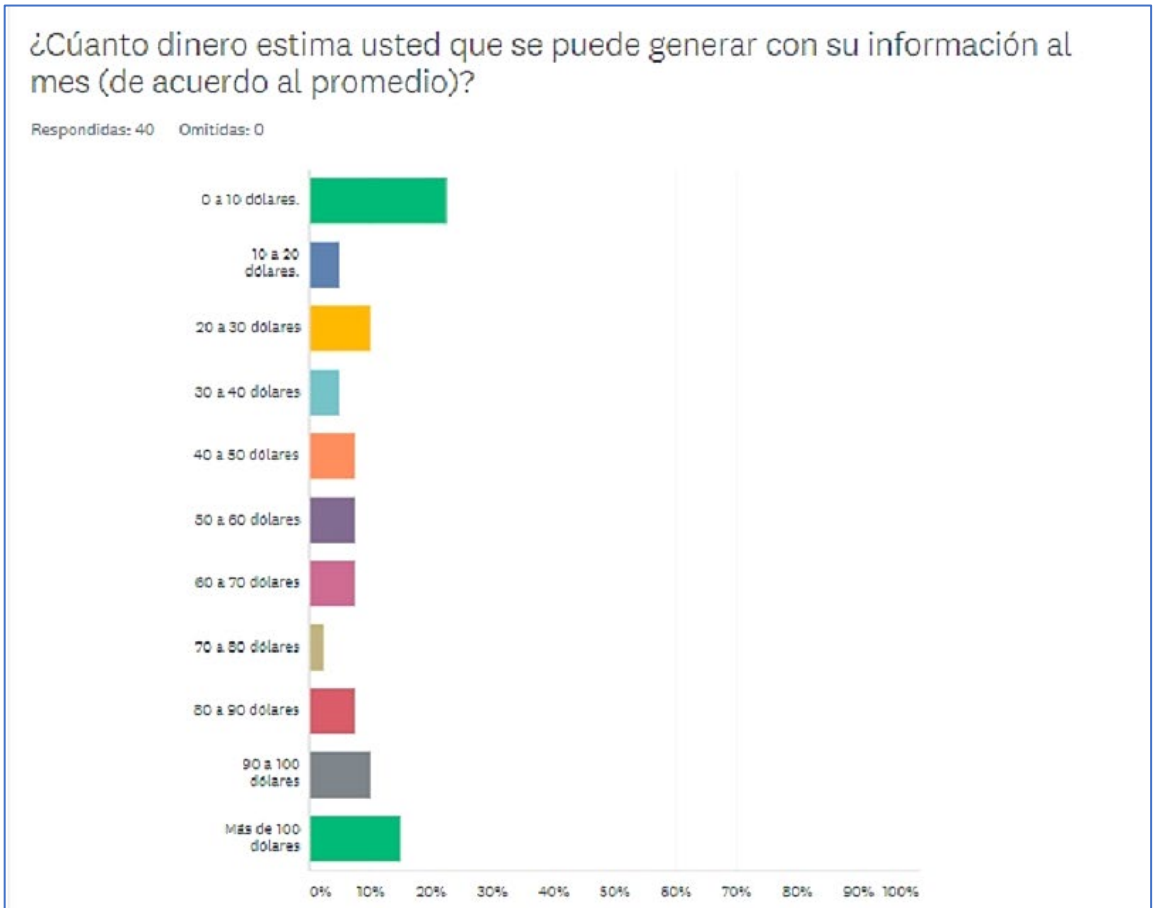
Fuente: Elaboración Propia

El 72,5% de los usuarios están conscientes de que las redes sociales tratan de mantenerlos conectados el mayor tiempo posible. Sin embargo, continúan consumiendo más de 3 horas al día de redes sociales.

4.7. Dinero generado por la venta de información.

Séptimo se quería saber si el usuario tiene una idea de cuánto dinero genera solo una persona en datos al mes. Esto se hace para crear un marco de referencia para entender porque es más rentable pensar en una persona como datos que como persona.

Gráfica 14: ¿Cuánto valen los datos del usuario?



OPCIONES DE RESPUESTA	RESPUESTAS	
0 a 10 dólares.	22,50 %	9
10 a 20 dólares.	5,00 %	2
20 a 30 dólares	10,00 %	4
30 a 40 dólares	5,00 %	2
40 a 50 dólares	7,50 %	3
50 a 60 dólares	7,50 %	3
60 a 70 dólares	7,50 %	3
70 a 80 dólares	2,50 %	1
80 a 90 dólares	7,50 %	3
90 a 100 dólares	10,00 %	4
Más de 100 dólares	15,00 %	6

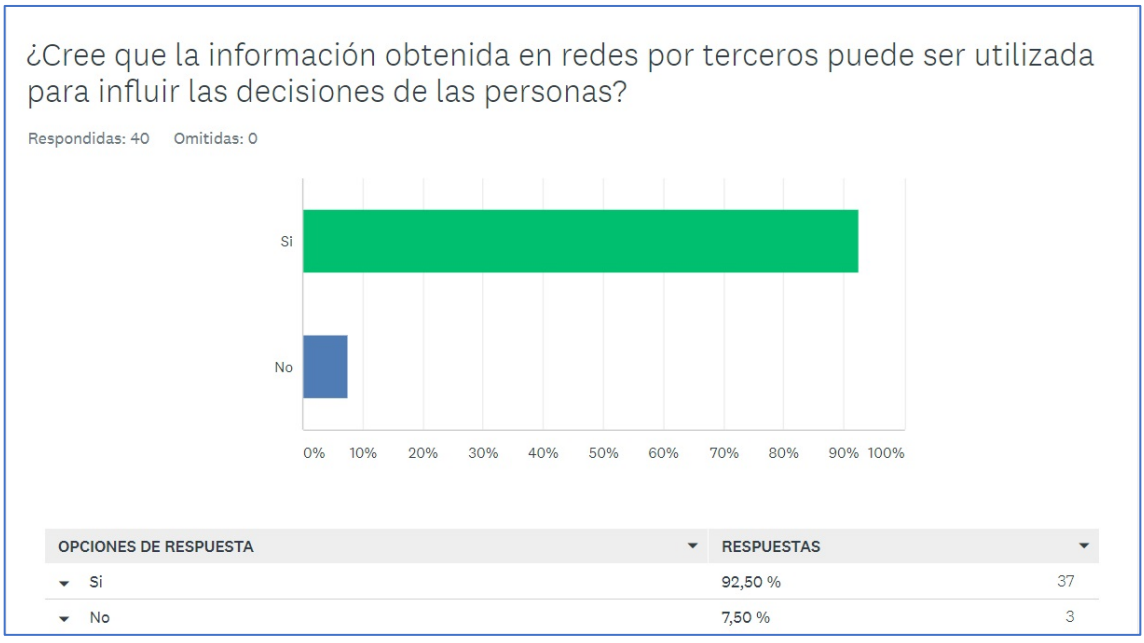
Fuente: Elaboración Propia

El valor estimado en 2020 al mes en dólares que genera una persona es de $36. Apenas un 5% de los usuarios de redes lograron acertar con esta cantidad. En cambio, la mayoría de usuarios o sobrevaloraron (15%) o infravaloraron (22,5%) el valor real de los datos de un usuario que se puede generar al mes. Una buena parte de la población no está consciente de que sus datos tienen un alto valor (37,5%), mientras que la mayor parte de la población parece tener una idea vaga de que sus datos tienen un valor alto, pero no están seguros cual es. El 62,5% de usuarios piensa que sus datos tienen un valor en el rango de 30 a más de 100 dólares. Por ende, el público en general sabe que sus datos tienen un valor importante.

4.8. Influencia de la utilización de datos en redes sociales por terceros.

Octavo se investigó si el usuario cree que se puede influir en las decisiones de otras personas utilizando la información obtenida en redes sociales.

Gráfica 15: Influencia de los datos en las decisiones de las personas.



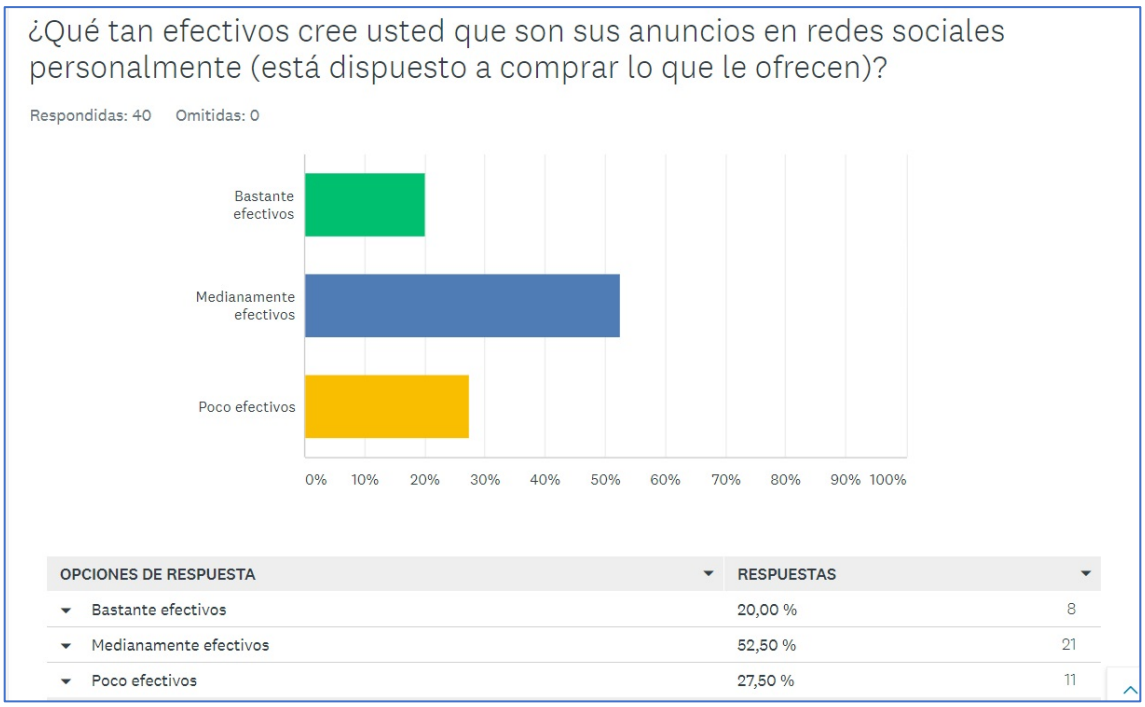
Fuente: Elaboración Propia

El 92,5% indicó casi de forma unánime que los datos se pueden utilizar para influir las mentes de las personas. Si tanta gente concuerda con esto, es factible pensar que se puede utilizar los datos de formas poco éticas para facilitar el esparcimiento de falsas narrativas.

4.9. Efectividad del algoritmo para generar interés en la publicidad.

Noveno se investigó como las personas reaccionan ante la publicidad dirigida.

Gráfica 16: Publicidad en redes



OPCIONES DE RESPUESTA	RESPUESTAS	
Bastante efectivos	20,00 %	8
Medianamente efectivos	52,50 %	21
Poco efectivos	27,50 %	11

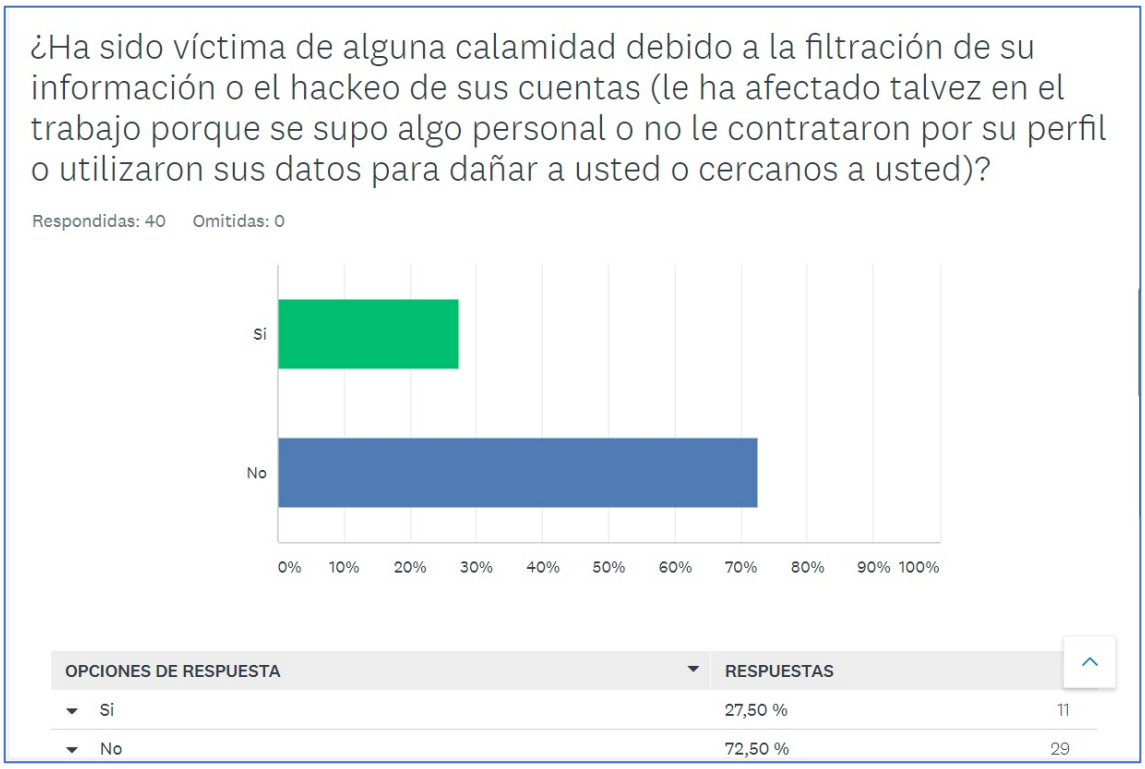
Fuente: Elaboración Propia

Un 52,5% de la población muestra que la publicidad si es efectiva en alguna medida, mientras que otro 20% muestra que es la publicidad si es bastante efectiva. Solo el 27,5% muestra que la publicidad dirigida no es efectiva. Podemos ver que existe un neto positivo para los sitios de redes sociales. Hay más gente comprando lo que le ofrecen que gente que no compra. Esto demuestra que las redes sociales si generan una gran cantidad de dinero debido a la publicidad, ya que no es necesario que se compre el producto solo que se vea la publicidad.

4.10. Víctimas de filtración de datos.

Finalmente se quería conocer si las personas han tenido problemas debido a la filtración o el hackeo de sus datos.

Gráfica 17: Porcentaje de personas malogradas por el uso ilegal o indebido de sus datos.



Fuente: Elaboración Propia

Un porcentaje bastante alto de personas (27,5%) dijo que si ha tenido problemas debido a la filtración de datos. Es un porcentaje bastante preocupante alto. Significa que hay un gran número de personas que son susceptibles a estafas o extorsiones por redes, cosa que se ha vuelto muy común (especialmente en tiempos de confinamiento y distanciamiento social).

DISCUSIÓN

5. Hay que darle importancia a la privacidad de nuestros datos.

Esta investigación tiene el propósito de hacer ver a las personas que la importancia de la ciberseguridad y de sus datos no son algo para tomarse a la ligera. La gran mayoría de personas que utilizan redes sociales no piensan en las repercusiones que tienen estas en sus vidas, o no le dan importancia al asunto. Este trabajo investigativo tiene como objetivo principal el de hacer dar en cuenta que las compañías de redes sociales utilizan métodos fraudulentos y poco éticos para mantener el control sobre las personas sin que estas se den cuenta y que poco se ha hecho para detener este problema. Es una cuestión que debería ser tomada más enserio en las futuras generaciones. De otro modo, las compañías de redes sociales tendrán la facilidad de hacer cualquier cosa que quieran sin ninguna repercusión grave.

5.1. El usuario no es más que ganancias para la compañía.

De los resultados obtenidos en esta investigación podemos ver que hay varios usuarios que concuerdan con la investigación del marco teórico. En específico que las redes sociales los manipulan de alguna forma con el fin de generar ganancias.

> "Hay grupos de interés o de poder que atesoran los contenidos de las redes sociales, entre ellos, datos personales, como información muy valiosa. No es altruismo lo que permite que estos servicios funcionen gratuitamente, quitando los beneficios por publicidad; a cambio pueden obtener información de la "inteligencia colectiva" del "neuromundo" (Ruiz, 2020).

Por ende, es necesario que tengamos restricciones sobre compañías que tienen tanta influencia en una parte bastante considerable de toda la humanidad. En 2021, existen 7,9 billones de personas en todo el mundo. De todas estas personas, 3,96 billones utilizan al menos una red social. El 50.64% de la población de toda la humanidad está afiliada a alguna compañía de redes sociales. Si nos ponemos a pensar que las compañías de redes sociales tienen información de más de la mitad de la población de toda la tierra, es hasta raro pensar que la mayoría de personas ni se ponderan que hacen las compañías de redes sociales con toda esa información, o si la están utilizando correctamente.

En esta investigación vimos que la gran mayoría de personas están al tanto de que las redes sociales utilizan sus datos para influir en sus decisiones. Por ejemplo, el 72,5% de los encuestados dijo que están al tanto de que las redes sociales pueden estar manipulándolos para que estén conectados por más tiempo. Varios expertos concuerdan de que las redes sociales están utilizando prácticas de poca ética para lograr este cometido. Si nos ponemos a pensar, realmente la humanidad está atada a sus dispositivos móviles. Esto es debido a la cantidad casi infinita de información que ofrece la internet y que es de tan fácil acceso. Sin embargo, ¿a cuántas personas realmente les importa eso? "Los ciudadanos facilitan datos sin tener en cuenta qué usos se pueden hacer de ellos" (Soto, 2017 p.5). Como vimos en esta investigación las compañías de redes sociales emplearon tácticas para mantener a las personas conectadas el mayor tiempo posible. En la media mundial, las personas pasan más de 3 horas al día en redes sociales.

A medida que pasen los años, este número solo se va a incrementar. Las nuevas generaciones cada vez aprenden a utilizar estos medios más fácilmente. Por esa razón es que hay que poner a las compañías de redes sociales sobre un mayor control y escrutinio. Por ejemplo, se debería controlar el uso de elementos de la psicología que son creados específicamente con el propósito de crear adicción. También se debería controlar el modo de uso de datos. El problema no es que tengan una increíble cantidad de datos a su disposición. Eso ya es otro problema que también debería tratarse debidamente. El problema es que no hay casi ningún control de cómo se puede obtener estos datos, ni de cómo se utilizan. Las compañías de redes sociales hacen campañas donde nos dicen a los usuarios que su seguridad es lo primero, que sus datos son usados correctamente. Sin embargo, como hemos visto en los últimos años, esto solo es una fachada para tapar lo que se hace realmente. Por ejemplo, Facebook, LinkedIn y Tiktok estuvieron bajo escrutinio de la ley debido a sus prácticas ilegales. Recibieron todo tipo de multas y tuvieron que cambiar varias políticas anti consumidor. Y después de todo eso, continúan siendo 3 de las compañías más lucrativas del mundo entero. Aunque cambiaron varias políticas para evitar que el usuario sea vulnerado, implementaron otras que prácticamente anularon el cambio. Los APIs de terceros son un ejemplo perfecto. Las compañías de redes sociales solo dejaron que los usuarios sean los que tengan la culpa. Al mismo tiempo, hicieron poco o nada para educar a sus usuarios sobre el tema. Tomaron una actitud de "ya no es mi culpa" les dimos la elección y los usuarios la aceptaron. Pero al mismo tiempo, crearon unas nuevas políticas de privacidad, con infinidad de términos legales confusos y con poca dirección hacia lo que es realmente importante de

tener en cuenta. Como pudimos ver en los resultados de esta investigación el 85% de los encuestados no leyeron las políticas de privacidad. Sin embargo, el 52% dicen que si están el tanto de lo que aceptan. Se puede inferir que los usuarios aceptaron las condiciones y creen conocer lo que aceptan sin leer o buscaron versiones resumidas de lo que están aceptando. De todas formas, se logra confundir al usuario de una forma u otra.

Esto nos lleva a otro dilema importante que se descubrió en esta investigación. El usuario está al tanto de que se utilizan sus datos para otros fines, pero no hace nada al respeto. El 80% de los encuestados respondió que si creen que sus datos están siendo usados sin consentimiento. Sin embargo, el 47% de los encuestados pasa más de 3 horas en redes sociales. Hoy en día es casi indispensable tener redes sociales para estar conectado con el resto del mundo. Incluso si el usuario considera las repercusiones, no hay nada que pueda hacer al respecto. Si el usuario quiere tener redes sociales, no tiene más opción que aceptar los términos y condiciones. ¿Por qué se permite que las compañías de redes sociales tengan el poder de obligarnos a darles todos nuestros datos? No existe ninguna opción que permita al usuario no dar su información personal al momento de crear una cuenta.

5.2. Las personas son más que sus perfiles.

Otro punto importante que se descubrió en esta investigación es que se da muy poca importancia a crear un ambiente donde no se esparza la desinformación (a menos que sean temas que hagan quedar mal a la compañía). El 92% de los encuestados cree que se puede utilizar su información o la de otros para influir a terceros. Los algoritmos, como ya se mencionó, están construidos para promover este mismo tipo de conductas negativas. Por ende, se promueve lo que digan estas personas, sea o no verdad. Así se puede recopilar la mayor cantidad de datos a costa de las personas que buscan lo más popular o las tendencias del momento. En cambio, si no públicas y ofreces tu información el algoritmo de las redes se encargará de hacerte lo menos visible posible. Esto tiene la consecuencia de que, en la sociedad en que vivimos, hacer esto te da menos estatus social. Las personas son más que los clicks que reciben y no deberían ser explotadas y manipuladas para beneficio monetario.

Esto en sí es una contradicción al objetivo original de las redes sociales, que es el de conectar a las personas. Djick y Ruiz nos explicaron en el marco teórico que las redes sociales están construidas intrínsicamente pensando en las relaciones interpersonales y la comunidad humana. Sin embargo, también pudimos ver en los resultados que el usuario no

está de acuerdo. Más bien se utiliza para fomentar la venta de datos, el control de otros usuarios mediante el uso de estos y las prácticas confusas para confundir a los usuarios.

5.3. ¿Por qué somos tan permisivos con las redes sociales?

¿Por qué se permite que las redes sociales puedan hacer lo que les plazca? Hay tres razones primarias que se descubrieron en esta investigación. Primero es que muchas otras compañías dependen de la información que se obtiene en redes sociales para generar ganancias. En esta época en la que vivimos de la tecnología, los datos se han vuelto la parte más grande e importante para generar dinero. La información de la encuesta mostró que el 52% de los usuarios creen que la publicidad es efectiva mientras que el 20% cree que es muy efectiva. Con los datos se puede saber las necesidades y entender mejor lo que el cliente quiere. Por esa razón, la mayoría de compañías hoy en día buscan formar parte de la red de información. Se invierten millones de dólares al año en asegurarse de que las compañías de redes sociales puedan continuar utilizando estas prácticas poco éticas, ya que se perdería una enorme cantidad de dinero si el usuario tiene control sobre sus datos.

Segundo es que estamos empleando nuevas tecnologías y servicios que apenas estamos empezando a comprender. Acabamos de entrar en la red 4.0 que utiliza IA (inteligencia artificial) para crear una experiencia de usuario personalizada. Sin embargo, apenas estamos empezando a discutir sobre la implementación ética de estos. Como vimos en la investigación el 27% de las personas encuestadas fueron afectadas de alguna forma por la difusión de sus datos. Los datos de estas personas fueron utilizados en contra de su voluntad para causarles algún tipo de daño como, por ejemplo, perder un trabajo. Por ende, se debe hablar sobre los peligros que conllevan seguir con la innovación.

Sin embargo, como vimos en el capítulo 2 de esta investigación, Yasmina Soto nos dice que los datos ya no son privados ni tampoco nos pertenecen. ¿La pertenencia y privacidad de los datos debería considerarse como un derecho humano? Hoy en día, es una de las cuestiones más grandes que se afrontan, debido a la gran proliferación de los datos como industria. Por un lado, los datos nos han dado una mejor comprensión de varios dilemas complejos y mejora nuestra innovación en varios sectores. Por otro lado, surgen los dilemas discutidos en este trabajo como la explotación del usuario. La verdad es que si queremos seguir mejorando tecnológicamente los datos tendrán que seguir siendo usados, pero se tendrá que crear nuevas legislaciones para controlar la distribución y el acceso de los mismos.

Las I.A están construidas para ser eficaces, por lo que existen instancias donde no se prioriza el beneficio del usuario, sino más bien su explotación. En la encuesta vimos que el 80% de los usuarios creen que están siendo manipulados para pasar más tiempo en redes sociales. Más tiempo en redes equivale a más dinero generado en publicidad y ventas. En los últimos años los expertos se han empezado a dar cuenta que el sistema actual prioriza la ganancia monetaria y no al usuario. Como vimos en la encuesta el usuario no está al tanto del valor de sus datos, ya que las respuestas fueron variadas (solo 2 personas acertaron el precio correcto de entre 30 a 40 dólares). Esto se debe a que a la persona promedio, poco le importa este dilema. Como vimos en esta investigación, las personas están dispuestas a continuar utilizando los servicios de redes sociales, a pesar de que están al tanto de las prácticas anti consumidor. Si a las personas no les importa, entonces a los gobiernos tampoco les va a importar. Además, se le da poca importancia a este dilema ya que hay cuestiones que se consideran más urgentes en el ámbito político. Los usuarios están haciendo muy poco para entender el problema que se presenta debido a la complejidad de estas nuevas tecnologías. Hasta que se empiece a hablar sobre este tema, las compañías de redes sociales pueden utilizar nuestros datos casi sin dificultades para generar ingresos, ya que no somos dueños de nuestros propios datos.

Por último, como explicaron Soto y Djick, uno de los factores más importantes es la cotidianidad de las redes sociales y la apatía de los usuarios hacia el tema. Como vimos en el marco teórico y los resultados, las personas no están dispuestas a leer páginas de políticas de privacidad por lo complicadas que suelen ser. Esto ya sabemos que se hace apropósito para que el usuario no quiera leer las políticas. Para algunos incluso resulta contraproducente ya que terminan entendiendo menos sobre el tema. Para el usuario promedio, es mucho más rápido y eficaz simplemente aceptar cualquier cosa que se le ponga en frente. Simplemente el usuario no está pensando en lo que podría suceder en el futuro, a sus hijos o incluso al mismo usuario. Los humanos estamos condicionados a pensar en corto plazo y no a lo que pueda pasar en el futuro. Se ha vuelto algo en lo que ni siquiera pensamos solo actuamos automáticamente.

CONCLUSIONES

La tecnología es un elemento de la sociedad que continuará integrándose y evolucionará cada vez más. Ya es una realidad que la sociedad funciona debido a la tecnología que utilizamos todos los días. Hemos creado una dependencia tan íntima con la tecnología que, si esta fallara, la sociedad colapsaría en gran medida. Si nos imaginamos un mundo sin redes sociales, veríamos un mundo donde la comunicación se vería lenta y tediosa. La inmediatez que proporciona la internet y la tecnología de redes sociales nos ha permitido mantenernos comunicados, conectados e informados. Sin embargo, se ha generado un nuevo problema debido al crecimiento de la tecnología. Como vimos en este trabajo de investigación, las redes sociales utilizan nuestros datos de formas poco éticas para generas ganancias. La nueva forma más eficaz de generar ingresos en línea es explotando a los usuarios, mediante el uso de sus datos personales. Como se ha vuelto una forma de negocio tan lucrativa, esto ha llevado a las compañías que utilizan estos datos a priorizar su obtención. Se fomenta el uso de cualquier método para obtener los datos, e incluso cuando se amonestan las prácticas fraudulentas, se crean nuevas formas para obtener datos. La internet es tan grande que es imposible hacer escrutinio de todas las compañías que existen. Pero, si se puede controlar a las compañías más visibles y grandes que están a la vanguardia del uso de estas tecnologías, tales como Facebook, Instagram, Tiktok, Youtube y otras. En específico debe existir un entendimiento y control de lo que están haciendo las compañías de redes sociales, ya que más de la mitad de la población del mundo las utilizan.

Si se controlan otras industrias como la alimenticia y la económica con tanto escrutinio, ¿Por qué no se hace lo mismo con lo que están haciendo las compañías de redes sociales? Al final y al cabo afectan a muchísimas personas de forma directa e indirecta. En esta investigación se propondrán cuatro soluciones concretas que ya se están empezando a poner en práctica o que están en la fase de discusión para solucionar este problema grave, que es la responsabilidad que tienen las redes sociales de cuidar a sus usuarios y no explotarlos.

El objetivo de esta investigación era el de probar que las redes sociales utilizan prácticas fraudulentas para mantener a los usuarios controlados y así poder lucrar con los datos obtenidos. Con esto se refiere a que el negocio lucrativo de la colección de datos ha

hecho que las compañías de redes sociales dejen a un lado el bienestar del usuario para concentrarse en explotar esos datos. Para poder demostrar que la hipótesis propuesta es cierta, se hizo un análisis teórico de varios ensayos y documentos científicos escritos por expertos que muestran sus hallazgos sobre el tema. Los datos recopilados en esta investigación demostraron que las personas son propensas al control psicológico, debido a varios factores incluidos en los algoritmos de construcción de redes. Las redes sociales, utilizan tácticas estilo casino de adicción para mantener a los usuarios conectados el mayor tiempo posible. Entre más tiempo estén conectados, más datos se pueden obtener, por lo que las cuentas que comparten más información son las que se promueven más. Mientras tanto las publicaciones de los usuarios que no comparten tanta información son puestas en segundo plano o incluso ignoradas.

Las redes sociales nos han dicho desde su creación que su objetivo primario es el de conectar a las personas. Sin embargo, estos últimos años hemos visto todo lo contrario. Han salido a la luz incidentes donde los usuarios son manipulados en formas poco susceptibles pero visibles a los que conocen sobre el tema. También hubo varios incidentes donde la información de los usuarios se filtró directamente. Las compañías de redes sociales están empezando a tomar el asunto de seguridad y privacidad a la ligera y, por ende, están empezando a ser menos escrupulosos. Permiten prácticas poco éticas con nuestros datos, los venden directamente o crean nuevas tecnologías para circunnavegar las restricciones que se les imponen. El valor de los datos es tan increíblemente enorme, que las compañías de redes sociales se han desviado de su propósito original, para explotar al usuario.

Pero lo más importante a sacar de esta investigación es que las compañías de redes sociales se han inmiscuido tanto en nuestras vidas que nos hemos vueltos dependientes. Esto ha llegado a tal punto de que estamos dispuestos a negar nuestros derechos sobre nuestra propia privacidad, con tal de formar parte del colectivo mundial de las redes sociales. Nos han condicionado a que no nos importe nuestra propia seguridad, para así poder obtener la mayor cantidad de datos posibles. La investigación realizada en este proyecto, mostró que las personas están dispuestas a ceder todos sus derechos sobre su contenido y lo que comparten, sin estar enterados de lo que están aceptando. Para lograr esto, las compañías de redes sociales hicieron que los procesos para obtener información sobre el tema sean complicados y largos.

6. Propuesta de Soluciones

6.1. Las compañías de redes deben ofrecer opciones reales de protección.

El problema principal que existe sobre la recolección de datos es que no tienes opción alguna. Para utilizar todas las redes sociales existentes debes aceptar sus términos y condiciones sin excepción. Esto implica que aceptas que tus datos sean recolectados. No existe una opción para deshabilitar esto, y si se quiere evitar lo único que se puede hacer es no interactuar con ninguna aplicación ni tener actividad significativa en las redes. ¿Si se hace eso cual es el punto de tener redes sociales entonces? ¿Por qué no existe esa opción que te permita mantenerte en el anonimato? Simple, no existe porque no conviene a ninguna compañía de redes sociales que no compartas tus datos en todo momento. Esto ha generado descontento en varios usuarios en los últimos años, al ver que las redes sociales están haciendo muy poco o nada para resolver este problema.

Resolver este problema es de hecho muy fácil. Simplemente las compañías de redes deben dejar de tener el interés monetario en mente y ofrecer opciones a los usuarios. Se puede fácilmente dar la opción a los usuarios de no compartir sus datos. De hecho, una compañía en específico sorprendió a todo el mundo al explotar esta premisa como una oportunidad de ofrecer valor a los clientes y al mismo tiempo bajar el valor de otras compañías de redes. Con el lanzamiento del firmware IOS 14.5 de Apple se lanzó la herramienta App Tracking Transparency. Esta simple herramienta permite controlar que aplicaciones y sitios web pueden tener acceso a la actividad del usuario mostrando todas las aplicaciones que pueden estar recolectando tus datos. Esta opción ya existe en la mayoría de sitios de redes sociales. La gran diferencia que otorga este sistema al usuario es que obliga a los desarrolladores a pedir permiso antes de poder utilizar los datos. Si los usuarios dicen que no quieren compartir sus datos entonces las compañías no pueden acceder ni vender de ninguna forma los datos. Existe una excepción y es que, si das permiso a una aplicación que pertenece a la aplicación que negaste, la aplicación secundaría puede enviar información a la aplicación negada. Por esta razón, Apple pidió a las compañías que hagan esto considerar no hacerlo, y que si se utilizan métodos fraudulentos para obtener datos (como la creación de cuentas fantasmas utilizando los datos de una aplicación en la otra), habrá multas o repercusiones graves. Apple también lanzó una campaña desacreditando las actividades de recolección de datos de las redes sociales. Este es el tipo de pasos que deben tomarse para

cambiar como las compañías de redes sociales actúan. El consumidor y su seguridad debe ser la prioridad de todas las compañías que quieran mantenerse a la vanguardia del progreso tecnológico. Igual que se hizo con la publicidad agresiva e invasiva, poco a poco iremos cambiando como actúan las compañías de redes sociales hacia el consumidor.

6.2. Se debe ser más transparente con los consumidores y ofrecer más información fácil de entender.

Las políticas que utilizan las redes sociales están compuestas de tal forma que sea lo más difícil de seguir y entender. Katherine Kemp, profesora en la Universidad de New South Wales en la facultad de leyes, presentó un proyecto donde analizó las prácticas fraudulentas utilizadas en las políticas de privacidad. En esta investigación se descubrió que las personas en general no leen las políticas de privacidad. Katherine Kemp explica que estas políticas de privacidad se han convertido en herramientas para controlar y no informar (Kemp, 2020). Por ejemplo, las políticas de privacidad de Facebook, Tiktok, Instagram, Snapchat, Twitter y Whatsapp llevan entre 6000 a 11000 palabras lo que equivale a 47 minutos de lectura hasta 1 hora y 40 minutos para el lector promedio. Kemp también explica que el 20% de las palabras de estas lecturas son complejas, y difíciles de entender para un usuario menor de 18 años. En el estudio realizado por Kemp el 62% de las personas encuestadas dijeron que no entendieron o no leyeron las políticas de privacidad por su cantidad de páginas. Esto concuerda con lo que se encontró en esta investigación. El 85% de los encuestados no han leído las políticas de privacidad.

Entonces lo que se debe hacer es restructurar como están escritas y construidas estas políticas de privacidad. Bajo ninguna circunstancia debería tomar a un usuario más de 20 minutos leer una política de privacidad. También se debe hacer todo lo posible para utilizar términos entendibles para el usuario. Lo mejor sería poner puntos específicos que expliquen de manera concreta y concisa lo que se está haciendo con los datos. Por ejemplo, debería existir un apartado que diga en viñetas fáciles de entender: esto es lo que estamos haciendo con sus datos y las formas en las que lo recopilamos. Esta información no debería estar escondida bajo capaz de texto confuso y largo que disminuyen el interés del usuario poco a poco hasta que termina rindiéndose y acepta.

También sería una buena práctica que las compañías de redes sociales creen campañas para reducir la ignorancia de las personas sobre estos temas de seguridad cibernética. Por lo general cuando se hace algún anuncio sobre estos temas, se utilizan

términos técnicos complejos. Así se mantiene el control sobre las personas que no entienden estos temas, pero se hizo una "buena campaña" que explica cómo funciona el sistema. Se debe ser más proactivo al momento de ser claro con los consumidores. Hay que poner el esfuerzo necesario para crear elementos o herramientas que ayuden al usuario a entender estos temas de manera más efectiva. Por ejemplo, se pueden crear videos cortos de Youtube explicando estos temas. Las personas de la plataforma ya hacen esto para educar a aquellos que están interesados. Entonces las compañías deberían tomar la iniciativa y utilizar sus propias plataformas para educar a los usuarios. Se debe incluir áreas más accesibles en las mismas plataformas que expliquen de una manera digerible lo que se requiere para tener una mejor ciberseguridad y lo que la compañía hace para lograr esta tarea.

6.3. Hay que generar un control sobre la explotación de los activos de la gente.

Las compañías de redes sociales deben ser puestas bajo mayor escrutinio en cuanto al uso de los datos se refiere. El nivel de control que se puede ejercer en decisiones de todo tipo, tanto políticas como sociales, es inquietante. En esta investigación se analizó los casos de Cambridge Analytica y como se manipularon las redes sociales para que las personas tomarán decisiones específicas. El nivel de control que se puede ejercer sobre las masas de personas es demasiado alto. Ninguna compañía debería tener el poder de explotar a tantas personas y sus decisiones. Entonces ¿Qué se debe hacer para evitar que haya tanto control sobre el usuario? Se deben tomar varias medidas concretas tales como: crear leyes que castiguen más gravemente a las acciones indebidas y al mal uso de nuestros datos, hacer que los derechos de los datos sea propiedad de cada individuo, que tengan la capacidad de acceder en cualquier momento a estos datos y que se les pida permisos para usarlos y que se pongan restricciones en las medidas utilizadas para crear las inteligencias artificiales que explotan las debilidades psicológicas de las personas. Hay que poner énfasis en las leyes de protección del usuario y las multas ya que no parece afectar a las compañías de redes sociales tener que pagas billones de dólares por sus acciones indebidas. Gracias a la monopolización de datos las compañías de redes sociales son algunas de las más lucrativas de todo el mundo. Esto implica que los gigantes tecnológicos pueden cometer todos los errores y no tener mayor repercusión. No podemos permitir que los datos que deberían estar conectándonos sean la razón por la cual caemos en una espiral de autodestrucción.

6.4. El usuario tiene el poder para cambiar a las compañías de redes.

El usuario debe abandonar esa apatía que siente ante estos temas, para empezar a entender que las redes sociales pueden controlar lo que hacemos y en lo que pensamos. Los usuarios del futuro deben ser capaces comprender como es que nuestros datos afectan nuestra vida. Las compañías de redes sociales pueden crear todos los videos o tutoriales del mundo para mejorar el entendimiento de estos temas, pero si los usuarios no les importa entonces el esfuerzo no sirve para nada. Las compañías seguirán con sus prácticas fraudulentas si ven que a los usuarios no les importa. Y es verdad que existe una gran apatía. Solo en esta investigación se descubrió que las personas aceptan los términos y condiciones sabiendo las repercusiones negativas. Esto se debe a que el usuario fue condicionado desde el principio a ser apático antes estos temas. Es mucho más fácil solo utilizar los servicios sin tener que pensar en las repercusiones. El usuario al final es el que decide cuanto poder pueden tener las redes sociales. Si los usuarios piden más control y un mejor escrutinio, las compañías empezaran a dar a los usuarios lo que quieren, como ya vimos con el ejemplo de Apple. Solo es necesario que se tomen los primeros pasos para entender que este dilema existe y que se puede tratar fácilmente.

BIBLIOGRAFÍA UTILIZADA

Amer, K., & Noujaim, J. (2019). *The Great Hack*. Netflix.

Gobierno de Argentina. *Cómo sé qué datos tienen sobre mí las redes sociales?* (2020, 17 diciembre). https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-hago-para-saber-que-datos-tienen-sobre-mi-las-redes-sociales

Canclini, N. G. (2020). *Ciudadanos reemplazados por algoritmos* (1.ª ed.). Transcript Verlag. https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/37414/9783839448915.pdf?sequence=1&isAllowed=y

Cooper, P. (2021, 23 febrero). *How the Facebook Algorithm Works in 2021 and How to Work With It*. Social Media Marketing & Management Dashboard. https://blog.hootsuite.com/facebook-algorithm/#How_the_Facebook_algorithm_works_in_2021

Cortellessa, E. (2019, 12 julio). *What Your Data Is Really Worth to Facebook*. Washington Monthly. https://washingtonmonthly.com/magazine/july-august-2019/what-your-data-is-really-worth-to-facebook/

Farooqi, S. (2020, 29 junio). *CanaryTrap: Detecting Data Misuse by Third-Party Apps on Online Social Networks*. ArXiv.Org. https://arxiv.org/abs/2006.15794

Fernandez, A. B., & Fernandez, I. R. (2014, 30 marzo). *Vista de Los adolescentes y el uso de las redes sociales*. Revista Infad. https://revista.infad.eu/index.php/IJODAEP/article/view/537/462

Fernández, Y. (2018, 17 septiembre). *Me he bajado todos los datos que Facebook tiene sobre mí y ahora sé que puede reconstruir mi vida cuando. . .* Xataka. https://www.xataka.com/privacidad/me-he-bajado-todos-los-datos-que-facebook-tiene-sobre-mi-y-ahora-se-que-puede-reconstruir-mi-vida-cuando-quiera

González, F. (2019, 15 junio). *Big data, algoritmos y política: las ciencias sociales en la era de las redes digitales*. Scielo. https://scielo.conicyt.cl/scielo.php?pid=S0717-554X2019000200267&script=sci_arttext&tlng=en

Hutchinson, A., & Hutchinson, A. (2021, 8 abril). *Data Hacks at Facebook and LinkedIn Spark Concerns Among Users*. Social Media Today. https://www.socialmediatoday.com/news/data-hacks-at-facebook-and-linkedin-spark-concerns-among-users/598093/

Kemp, Katharine, (2020, 5 noviembre). Concealed Data Practices and Competition Law: Why Privacy Matters European Competition Journal. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769.

Moreno, M. A., Goniu, N., Moreno, P. S., & Diekema, D. (2013). Ethics of social media research: common concerns and practical considerations. *Cyberpsychology, behavior and social networking*, *16*(9), 708–713. https://doi.org/10.1089/cyber.2012.0334

Moreno, J., Serrano, M. A., & Fernández-Medina, E. (2016). Main issues in big data security. *Future Internet*, *8*(3), 44.

Pasquali, M. (2020, 6 febrero). *Los países con los usuarios más adictos a las redes sociales*. Statista Infografías. https://es.statista.com/grafico/20744/tiempo-de-uso-de-redes-sociales-por-pais/

Pineda, E. S., & Cárdenas, J. A. (2007). *Ética en las organizaciones* (1.ª ed.). McGraw-Hill Education.

Ramonet, I., Assange, J., Chomsky, N., & Sacristán, M. (2016). *El imperio de la vigilancia*. Madrid: Clave intelectual.

Redden, J. (2017, 7 diciembre). *Six ways (and counting) that big data systems are harming society*. The Conversation. https://theconversation.com/six-ways-and-counting-that-big-data-systems-are-harming-society-88660

Ruiz, C. B. (2009). Las redes sociales y la protección de datos hoy. *Anu. la Fac. Derecho (Alcalá Henares)*, (2), 301-338.

Scroxton, A. (2020, 20 agosto). *Social media data leak highlights murky world of data scraping*. ComputerWeekly.Com. https://www.computerweekly.com/news/252487895/Social-media-data-leak-highlights-murky-world-of-data-scraping

Sharma, A. (2021, 4 abril). *Quicktake: Why Facebook is becoming the poster child for data misuse*. The National. https://www.thenationalnews.com/business/technology/quicktake-why-facebook-is-becoming-the-poster-child-for-data-misuse-1.1196740

Social media marketing: Who is watching the watchers? (2020, 1 marzo). ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0969698918307744

Soto, Y. (2017). Datos masivos con privacidad y no contra privacidad. *Revista de Bioética y Derecho*, (40), 101-114.

Van Dijck, J. (2019). *La cultura de la conectividad: una historia crítica de las redes sociales*. Siglo XXI editores.

Wagner, K. (2017, 1 noviembre). *Donald Trump and Hillary Clinton spent $81M on Facebook ads before 2016 election*. Vox. https://www.vox.com/2017/11/1/16593066/trump-clinton-facebook-advertising-money-election-president-russia

Your Data Is Shared and Sold. . .What's Being Done About It? (2019, 28 octubre). Knowledge@Wharton. https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/