

TRABAJO DE INVESTIGACION FINAL

"Los riesgos que toma un usuario en relación a la privacidad cuando él mismo acepta los términos y servicios/condiciones en una plataforma durante la última década".

Autor/es:

**Caruso Lombardi, Joan y Herrero Castellano,
María Emilia**

Carrera:

Licenciatura en Ciencias de la Comunicación

Tutor:

Ciarleglio, Gonzalo

Año: 2021

Resumen

En la presente investigación se propuso explorar acerca de la recopilación de datos que extraen las Big Five (Google, Facebook, Amazon y Apple, entre otras) y hacia dónde van los mismos. El trabajo consiste en analizar las diferentes cláusulas y condiciones que presentan las redes sociales antes de la creación de la cuenta, en determinar riesgos específicos que se corren gracias a esta navegación sin regulación.

Los resultados demostraron que los usuarios no leen dichas cláusulas en dónde se informa que la aceptación implica ceder todo tipos de datos personales y la navegación de la página, es decir, que podemos comprobar que la aceptación de los términos y condiciones de las redes sociales aumenta la comercialización de los datos personales vulnerando el derecho a la privacidad.

Si bien comprendemos que en la actualidad estamos inmersos en el mundo digital, y la pandemia forzó aún más este punto, esto es uno de los factores principales por los cuales los usuarios aceptan todo lo que las plataformas les exijan con tal de pertenecer al círculo virtual.

Palabras Clave: *Plataformas digitales, términos y condiciones, datos personales.*

Abstract

This investigation's purpose is to explore the data thrown by the Big Five (Google, Facebook, Amazon, Apple, among others) and where they are going. This piece consists of analyzing different clauses and conditions presented in Social Media before the user profile creation and determining specific possible risks which can be taken due to unregulated navigation.

The results demonstrated that users do not read the mentioned clauses which inform that accepting implies giving in and conceding all personal data and the website navigation, which means that it can be proved that the acceptance of Social Media's Terms and Conditions increases personal data commercialization, infringing privacy rights.

Although it is understood that currently, we are immersed in the digital world and that the pandemic forced yet this more, this is why this is one of the main factors by which users accept whatever the platforms demand to belong to the virtual circle.

Keywords: Digital platforms, terms and conditions, personal data

Agradecimientos

A cada familia por acompañarnos a transitar este largo camino dándonos fuerzas y motivándonos a continuar.

A nuestro Tutor, Gonzalo Ciarleglio, por brindarnos su apoyo y dedicación en cada respuesta y corrección.

A nosotros por haber formado un equipo en dónde cada uno demostró su vocación y perseverancia y así su compañerismo para con el otro.

Índice

Introducción.....	1
Problemas planteados para esta investigación	2
Justificación.....	3
Objetivos.....	3
Hipótesis General	4
Estado del Arte.....	5
Marco Teórico	10
Tipo de investigación.....	42
Marco metodológico	42
Conclusión	59
Bibliografía general	62
Anexo	65

Tema

Los riesgos que toma un usuario en relación a la privacidad cuando él mismo acepta los términos y servicios/condiciones en una plataforma durante la última década.

Introducción

Para introducirnos en el mundo de las plataformas, lo primero que debemos pensar a la hora de abordar los riesgos que supone la aceptación, si se quiere a ciegas, de las aplicaciones que utilizamos día a día, es que todos los datos y todo nuestro recorrido dentro de las mismas quedará registrado y guardado en algún recóndito lugar que es desconocido o ignorado por todos o varios de los usuarios del mundo digital.

En la actualidad, la vida de muchos de los usuarios o de una gran mayoría de personas gira en torno a las aplicaciones y las plataformas, es impensado en este siglo encontrar un ciudadano sin un registro en el mundo virtual. Dichas plataformas se alimentan de los datos que nosotros, los usuarios, dejamos día a día. El mundo virtual se alimenta de forma directa de toda la información que diariamente dejamos.

Información que posteriormente las redes van a utilizar para sus propios fines. Información deslocalizada, que es la nueva materia prima del mundo, de la nueva “economía de la información”.

Otro de los objetivos de este estudio es poder determinar y detallar de manera minuciosa cual es el marco legislativo que regulan a estas plataformas, tanto en Argentina como en el mundo entero. Zonas grises, gobernanza en internet, ¿poca regulación?, todos estos aspectos serán abordados en este análisis.

El derecho a la privacidad es uno de los puntos clave en este estudio. Dentro del nuevo ecosistema digital, la información vuela, la inmediatez es un concepto de esta nueva era, mismo los gobiernos han tenido conductas que pueden llegar a parecer desleales en cuanto al tratamiento de la información y la vigilancia.

La tecnología e internet han pasado a formar parte de la vida de toda la sociedad y es cuestionable cuando detectamos a una persona que no cuente con un perfil creado en alguna de las diversas redes sociales.

Ahora bien, ¿Los usuarios leen los términos y condiciones luego de completar el formulario que da acceso a la creación de la cuenta?, ¿Todos los usuarios tienen conocimiento de hacia dónde van los datos personales ingresados? y por último, ¿Cuáles son las consecuencias de no pertenecer a un círculo virtual?

El objetivo de esta investigación será analizar por un lado si los usuarios consideran cuál es la implicancia de la aceptación de la cláusula obligatoria que impone la misma plataforma y cómo se comercializan a futuro la información privada que ya deja de serlo pasando a vulnerar el derecho a la privacidad de cierta manera.

Problemas planteados para esta investigación

La presente propuesta de investigación consiste en indagar las cláusulas de "términos y condiciones" de plataformas específicas que están dentro de las big five y que el usuario debe aceptar obligatoriamente dicha cláusula que implican el consentimiento de ceder sus datos personales que luego, van a ser utilizados a futuro para su comercialización a terceros.

Además se indagaran los diversos riesgos que supone la aceptación de términos y la divulgación de la información personal de los usuarios dentro del ecosistema digital.

Asimismo, se identificará tanto el conocimiento de los usuarios de lo que sucede una vez inmerso en el mundo virtual.

Justificación

El tema presentado en el trabajo de investigación es viable para ser analizado, ya que, en la actualidad, las investigaciones sobre la recolección de datos y que finalidad tienen los mismos se encuentran latentes. Este estudio aportará una ampliación de conocimiento acerca de qué datos se comercializan una vez que ingresamos a las plataformas y cuáles son los riesgos que se corren en función de la privacidad de sus usuarios.

Los medios utilizados para la investigación hacen posible este estudio. La bibliografía consultada está fuertemente nutrida de información con respecto a las plataformas, a la recolección de datos y a sus características más importantes. La relevancia de este tema es inobjetable, los datos son la materia prima del mundo, como ya comentamos anteriormente en la introducción, es algo que veamos o no y que nos influye cada vez más.

Otro aspecto significativo y no menos importante sobre el tema expuesto es el del posible desconocimiento sobre la comercialización de los datos a anunciantes, es decir, cuando la venta de datos pasa a terceros o socios.

Objetivos

Objetivos generales

Determinar qué riesgos asume un usuario en relación a la privacidad cuando se aceptan los términos y condiciones en una plataforma.

Objetivos específicos

- 1- Determinar el grado de conocimiento por parte del usuario a la hora de aceptar la venta de sus datos a terceros, por parte de las plataformas.
- 2- Describir los usos posteriores que le dan las empresas que compran datos personales de usuarios a plataformas.
- 3- Analizar cuáles son los factores principales que llevan a un usuario a aceptar las condiciones que proponen las aplicaciones y determinar qué valoración les dan a su propia seguridad en las redes.

Hipótesis General

La aceptación de los términos y condiciones de las redes sociales aumenta la comercialización de los datos personales vulnerando el derecho a la privacidad.

Hipótesis Específicas

- 1- A mayor cantidad de usuarios en las plataformas, mayor tráfico de los datos personales.
- 2- La creación de cuentas aumenta la violación al derecho de la privacidad por cláusulas impuestas por las plataformas.
- 3- Los datos son directamente vendidos a anunciantes para catalogar perfiles de usuarios.

- 4- La edad, geolocalización e intereses son los datos más valiosos para formar perfiles para luego intercambiar los intereses de los usuarios con empresas.
- 5- A mayor desconocimiento en las redes sociales por parte de los usuarios, mayor es la frecuencia de extracción de los datos personales.

Estado del Arte

La última década ha sido sin dudas la década en la cual las redes sociales y las plataformas han hecho un boom en la sociedad. Medios como Google, Facebook, Amazon, fueron tomando el control de todo este mundo de plataformas y han crecido de forma exponencial. Plataformas digitales en las cuales dejamos prácticamente todas nuestras pertenencias: información personal, fotos, vínculos, gustos o intereses, entre otras cosas. Plataformas que incluso te conocen más que a uno.

La vida diaria de las personas, en este contexto de globalización, están guiadas por las nuevas tecnologías. La difusión y el crecimiento que ha tenido esta industria no se compara con ninguna otra: ha cambiado totalmente el paradigma en el que nos encontrábamos.

Las relaciones humanas se han modificado, las relaciones laborales también –ni hablar del contexto pandémico que estamos viviendo actualmente-. La sociedad entera ha cambiado sus formas. En cuanto a lo social, las redes han traído beneficios incomparables en cuanto a comunicación y marketing.

Si bien las redes sociales han beneficiado a nivel comunicacional a la sociedad no tardaron en pensar de qué manera se favorecerá su negocio. Detrás de las mismas se esconde una doble cara que pocos conocen. En este último tiempo el tema de los datos ha cobrado una mayor relevancia. Cada año se transforma en una materia prima fundamental para las empresas que quieren expandirse, crecer y agregar valor a su empresa, y según el tipo de plataforma que sea funciona de distinta manera en el manejo comercial de la información.

Sin dudas, en la actualidad, todavía hay gente que no tiene el conocimiento de la comercialización de datos. Cierta público aún cree que las redes sociales tienen como función otorgar un espacio para interactuar con amigos, compartir fotos, etc. Pero pocos se preguntarán... ¿A dónde van a parar todos los datos que les damos a las plataformas?

Según la autora José Van Dijck, en su libro *Platform Society*, los datos son moneda de cambio en internet. Los datos dejaron de ser parte de la privacidad para pasar a ser la base de la economía digital. Dichos datos se almacenan en diversos servidores físicos y virtuales, repartidos por todo el mundo (Van Dijck, 2018). Los servidores se encuentran deslocalizados según Jorge Morell, fundador de la empresa española “Legaltechies”, que se dedica a asesorar jurídicamente a las plataformas en cuanto a sus términos y condiciones, asegura en un estudio hecho por él mismo, que de 100 páginas web que investigó -para saber dónde se almacenan nuestros datos-, solamente 42 revelaban el lugar donde se encuentran los diversos servidores.

El estado de la cuestión que se investiga en este proyecto es que los datos son la materia prima fundamental para que una empresa crezca, por lo tanto, las empresas harán lo que sea para sacar rédito de esto. Los datos que quedan ingresados y dejan la estela de nuestro paso por la app pueden ser comercializados, es decir, vendidos a empresas para mejorar sus productos.

Antes de continuar profundizando las ideas principales de esta investigación, debemos definir dos de los conceptos más importantes que más adelante se abordarán: privacidad e intimidad.

En relación a estos términos que parecen significar lo mismo, debemos diferenciarlas, ya que en cuanto al marco legal, existen leyes que no suponen una diferencia entre estos dos conceptos, pero aquí nos vemos obligados a exponerlo.

En cuanto a privacidad, debemos referirnos como lo expresa el Diccionario de la Real Academia Española como un ámbito de vida privada que se tiene derecho a proteger de cualquier intromisión, esto quiere decir que se goza de protección jurídica en cuanto al

entrometimiento a nuestra vida privada. En estos términos, privado entonces tiene que ver con un espacio, con la propiedad de un individuo.

Por otro lado, cuando nos referimos a intimidad, estamos hablando de las cosas internas de una persona o un ser. El DLE –Diccionario de la Lengua Española- se refiere como una zona íntima y reservada de una persona o de un grupo, especialmente de una familia. En relación a esto, la palabra intimidad se refiere a todo lo que pasa internamente por un ser humano, sus pensamientos, sentimientos, creencias, valores, etc.

Por lo general se refieren a privacidad e intimidad como si fueran lo mismo, aquí queda claro que el alcance de ambos conceptos es diferente.

Volviendo a las plataformas y a la comercialización de datos, la autora Van Dijck brinda un ejemplo en su libro: “En el capítulo 6, encontramos plataformas de salud y fitness que venden datos recopilados desde usuarios de aplicaciones hasta instituciones públicas y empresas. La plataforma de salud personalizada, *PatientLikeMe*, por ejemplo, vende datos de usuarios a grandes empresas farmacéuticas, que los utilizan para desarrollar y mejorar productos”.

Por lo tanto, los riesgos que corremos a la hora de dejar información importante dentro de un servidor pueden ser variados. Pueden incitarnos a actuar como quieren y las preferencias también se verán afectadas. Los datos recopilados le dan a la plataforma un perfil de usuario, el cual explota desde anuncios, publicidad y contenido.

El autor bielorruso, Evgeny Morozov, tiene una mirada crítica en cuanto a la recopilación de datos y los algoritmos impuestos por las nuevas tecnologías. En el título de su libro ya se puede vislumbrar su subjetividad y punto de vista con respecto a esto: “La locura del solucionismo tecnológico”. En el texto aborda temas como la Big Data o la personalización de usuarios. Retomando el foco sobre lo que son los datos, el autor manifiesta que la cantidad de datos que se obtienen de las *cookies*, concepto que desarrollaremos más adelante, es inmensa. Además el autor pone un ejemplo: “Los editores de sitios de alta calidad

no pueden vender tanta publicidad en sus propios sitios como les gustaría, por eso recurren a intermediarios para que les otorguen información registrada en las cookies sobre los usuarios”.

Por otro lado, estos editores que se hacen de la información de los usuarios a través de las cookies, intentan aprovechar al máximo estos datos para poder generar dinero a través de la publicidad.

Existen diversas aplicaciones que piden datos variados, pero por lo general el fin exclusivo de la recopilación de datos es poder perfilar al usuario para poder dirigir más exitosamente la publicidad. Y ya aquí podemos detectar una característica importante de este sistema propuesto por las plataformas: que te bombardeen de publicidades específicas según tus gustos y preferencias. Muchas veces estas publicidades pasan a ser propaganda política buscando así, influir en el voto del usuario; Más adelante profundizaremos en el caso más icónico de este riesgo, el de Facebook y Cambridge Analytica.

En su libro “La Era de la Información”, el sociólogo Manuel Castells ya desde el año 1998 vaticinaba lo que el llamo “La Sociedad Red”, concepto que utilizó para referirse a la nueva estructura social que dominaba el mundo en aquella época -y que sigue haciéndolo-, en el contexto de una nueva era de información. A finales del siglo XX, el autor vio venir la nueva revolución tecnológica, a la que denomina “tecnologías de la información”.

Estas tecnologías se centran –y se centran- en la acumulación de información y su procesamiento. En el libro se habla de que además de ser una herramienta, podían convertirse en procesos de desarrollo –así como la Big Data actualmente-. Desde esa época se tomaron conceptos que hasta el día de hoy son esenciales como que la información es una materia prima, que la flexibilidad que poseen las nuevas tecnologías de información eran únicas, además de tener esa capacidad de reconfigurarse y actualizarse constantemente y por último, la capacidad de penetrar dentro de la sociedad a través del control de la información.

El concepto de las TIC (Tecnologías de la Información y Comunicación) es un concepto que permite adquirir, producir registros en todo tipo de formato, ya sea imágenes, sonidos o datos. Con el correr del tiempo, estas tecnologías fueron soportadas y llevadas a cabo por diversos artefactos electrónicos, como teléfonos, celulares, computadoras, tablets, etc.

Una de las características más importante de estas tecnologías tienen que ver con su digitalidad, y como mencionábamos antes, su flexibilidad es muy aprovechable por quien las utilice. Gracias a esta digitalidad, se pueden almacenar grandes cantidades de información y a su vez se puede acceder a esta información desde cualquier dispositivo.

La instantaneidad es la otra cara de esta tecnología, la inmediatez va de la mano con este concepto y es igual de importante.

Gracias a las TIC la sociedad dio un giro en cuanto a relaciones interpersonales, laborales y demás, hasta un cambio importante en la educación –todavía más acentuado estos últimos años-.

Si bien la disrupción tecnológica benefició a la sociedad en cuanto a la comunicación, la aceptación de los términos y condiciones no demoró en favorecer a las plataformas. De esta manera surge el capitalismo cognitivo, el mismo es un sistema económico que se basa en las transacciones o en la comercialización de mercadería que en la actualidad van a ser los datos personales. Hoy esa mercadería es inmaterial y es la economía del conocimiento.

Por otro lado, Nick Srnicek describe en “Capitalismo de plataformas” el nuevo paradigma que atraviesa la sociedad. El autor hace referencia a una cuarta revolución industrial que ha permitido crear nuevos términos como economía on demand o economía app, esos términos plantean el término del capitalismo cognitivo. El punto principal de Srnicek es que, durante el Siglo XXI, el capitalismo mutó hacia un gran interés en la extracción y utilización de datos, los cuales pasaron a ser la materia prima.

“Las plataformas publicitarias se apropian de los datos como materia prima. Las actividades de los usuarios, instituciones, si se graban y se transforman en datos, se convierten en materia prima que puede ser utilizada por las plataformas de distintas maneras” (Srnicek, 2018).

Ahora bien, ¿Quién es propietario de los datos que se comparten en internet? Para el autor, Tirole, los datos deberían ser del cliente, el agregado de los datos son de las plataformas dado que creó la tecnología para poder captarlos y puede beneficiarse con ellos, pero los datos personales de cada uno, son propios. Los datos que se fueron generando con la participación de la plataforma y ella debería ser portátil, los puedo llevar de una plataforma a otra (Tirole, Jean, 2017). Por ejemplo si quiero utilizar Cabify en vez de Uber, podría poder portar mis datos personales para pertenecer a la aplicación.

Marco Teórico

La tecnología fue uno de los cambios más importantes de la sociedad, su alcance trasciende lo cotidiano e impacta de modo directo en diversos ejes de la vida cotidiana modificando la forma en la que nos comunicamos, producimos y trabajamos. El economista Clayton M. Christensen clasifica a la tecnología en dos categorías: sostenida y disruptiva. La primera hace referencia a mejoras incrementales a una tecnología ya establecida, por ejemplo, los discos duros se crearon con un espacio de 1 gb y actualmente se producen de 1 tb. Por otro lado, es disruptivo cuando el cambio modifica completamente lo ya existente, es decir, anteriormente se utilizaba un CD para almacenar material, y en la actualidad se utiliza un pendrive que cumple la misma función.

Cuando la tecnología evoluciona, la sociedad se adapta a ella en diversos aspectos, incluso en lo económico. Este último aspecto fue el último en desarrollarse y las aplicaciones fueron las principales en colaborar con esto. Es el caso de Uber, la aplicación que logró vender un servicio sin necesidad de tener una flota de vehículos propia, ya que a través de la plataforma se pone en contacto la oferta y la demanda de un servicio de transporte de pasajeros. Si bien no logró terminar con la existencia de taxis, representa una visible innovación disruptiva.

Por otro lado, nos encontramos con Internet móvil, es una de las tecnologías disruptivas más relevantes ya que permite la conexión en dispositivos como smartphones y tablets que permiten nuevas formas de entender, percibir e interactuar con el mundo exterior logrando modificar los usos y costumbres. Se estima que las conexiones a internet aumentarán con la llegada de redes inalámbricas de 5 gb y que 9 mil millones de personas tengan un dispositivo móvil dentro de cinco años y puedan acceder a internet con ellos.

La tecnología está transformando el mundo, la virtualidad permite que muchas actividades puedan desarrollarse digitalmente facilitando su crecimiento económico más allá de fronteras jurídicas y territoriales por su sistema basado en almacenamiento de datos, compartidos en tiempo real.

Toda la bibliografía, estará encabezada, fundamentalmente, por el libro *Platform Society* de José Van Dijck, texto que expone desde una definición puntual sobre qué es una **plataforma**: “Una plataforma en línea es una arquitectura digital programable, diseñada para organizar interacciones entre usuarios” hasta un abordaje más bien político-legal, quizás aún desconocido como es el costado más controvertido de estas nuevas tecnologías:

“Mucha gente piensa en las plataformas simplemente como tecnología o herramientas tecnológicas que les permiten hacer cosas en línea: chatear, compartir, comentar, buscar, comprar cosas, escuchar música, ver videos, tomar un taxi y pronto. Pero estas actividades online esconden un sistema cuya lógica y logística se tratan más que facilitar: en realidad dan forma a la forma en que vivimos y a cómo se organiza la sociedad" (Jan Gehl, 2011).

Otra de las fuentes más importantes es la de Nick Srnicek con su libro *Capitalismo de plataformas*. El texto se centra en la nueva economía digital impuesta por este nuevo mundo - que a partir de ahora llamaremos “**ecosistema**”- de plataformas- y su estrecha relación con el capitalismo. La contratapa del libro es concreta y sentencia: “Economía inmaterial, cuarta revolución industrial, son algunos de los términos que intentan mistificar las virtudes o señalar los peligros del nuevo paisaje tecnológico”.

Existe un nuevo paradigma que atraviesa la sociedad, una cuarta revolución que se desarrolla con nuevos términos como “economía on demand” o “economía app”. Esta definición es aportada por Nick Srnicek y se refiere a que durante el siglo XXI, el capitalismo mutó hacia un gran interés en la extracción y utilización de datos, estos mismo pasaron a ser la materia prima del nuevo modelo de negocio.

El avance de internet y el crecimiento de la dependencia en las comunicaciones digitales por parte de las empresas generaron que los datos se transformen en un foco vital a la hora de cumplir con las funciones capitalistas.

Se entiende por plataforma a una estructura digital que cumple la función de permitir que dos caras, en este caso, la oferta y la demanda interactúan. El principal beneficio de la plataforma es que les permite a los usuarios construir sus propios productos, servicios y espacios de transacciones. A mayor cantidad de usuarios utilizando la plataforma, más valiosa se vuelve la misma aunque puede concluir también en una monopolización.

Srnicek plantea cinco tipos de plataformas distintas. En primer lugar, la plataforma más antigua del mundo empresarial, la **plataforma publicitaria**. Este tipo se apropia de los datos como materia prima, se extraen los datos a través de la interacción del usuario con el sitio web y la utilización de cookies que funciona como una suerte de rastreo. El objetivo de este tipo de plataforma es la extracción de datos que a futuro son vendidos a anunciantes. De esta manera se conecta a los anunciantes con usuarios correctos.

En segundo lugar, se encuentran las **plataformas de la nube**, en este caso se consolidaron como un modelo de negocio único y poderoso. Dicho modelo comenzó con el e-commerce en 1990. Este tipo de plataforma permite la extracción de datos constantemente ya que las mismas desarrollan la infraestructura básica de la economía digital para que otros puedan alquilarla. “Las plataformas de la nube permiten básicamente la tercerización de gran parte del departamento de la tecnología de la información de una empresa”. En resumen, la importancia de dicha plataforma es la recolección de datos y su modelo de alquiler colabora

con el rejunte de los mismos, si bien antes se vendían, hoy en día los utilizan las mismas plataformas para desarrollar su propia economía.

Por otro lado, la **plataforma industrial**, y quizás la menos conocida, incluye “la inserción de sensores y chips de computadoras al proceso de producción y de rastreadores al proceso de logística”, esto significa que las mismas son ensambladas en el proceso productivo y generan información específica. Por ejemplo, las computadoras que poseen windows tienen la inserción de intel.

Una de las últimas clasificaciones en aparecer fue la **plataforma de productos**, en esta infraestructura la primera cara posee productos propios que ofrece para su comercialización a la otra cara, la demanda. Zipcar es una empresa que alquila automóviles, es decir, que pone a su propio producto para comercializar. Este tipo de plataforma se relaciona con la **plataforma austera** la cual posee servicios pero no productos propios. Volviendo al ejemplo de Zipcar, esta plataforma es la más actual, si pensamos en Uber también alquila el servicio de traslado pero no ofrece sus propios vehículos, es decir, utilizan la infraestructura o la plataforma para conectar la oferta y la demanda.

Como conclusión podemos afirmar que todas las plataformas requieren de datos para alimentarse y generar de alguna u otra forma su ganancia. Los datos son el principal recurso y los usuarios se crean cuentas no sólo para pertenecer al círculo social virtual sino también para poder acceder a los servicios que las mismas ofrecen.

“Todas estas características hacen de las plataformas un modelo central para la extracción de datos como materia prima a ser utilizada de distintas formas”.

“Estas plataformas se están convirtiendo en dueñas de las infraestructuras de la sociedad”.

El libro de la economía digital analizada por Srnicek, argumenta que existe una convergencia de **vigilancia** -ya que “las plataformas publicitarias necesitan monitorear y registrar las actividades online” (Srnicek, 2018) y de actividad lucrativa por parte de estas plataformas. La recolección de datos no es la única acción importante aquí, el análisis de la información es clave en este proceso de venta. Los anunciantes prefieren datos trabajados, que les permitan a ellos una conexión más eficiente con potenciales consumidores.

El control que tienen todas las plataformas a las cuales ingresamos de alguna manera moldea nuestra forma de vida. Los datos almacenados que provienen de la actividad del usuario, de su comportamiento, convierten a este en objeto de vigilancia. Y aquí se puede descifrar otro de los riesgos importantes, ya que la cesión de datos personales lleva al usuario a comportarse de maneras que no lo haría si no estuviese inmerso dentro del ecosistema.

La existencia de un ente tan inmenso (plataformas y redes sociales) y la palabra “vigilancia” nos remite directamente al concepto del *Panóptico* de Jeremy Bentham. El panóptico es una estructura carcelaria que está compuesta de una torre de vigilancia en el centro de la prisión, donde se puede ver directamente todas las celdas sin que el vigilante dentro de la torre pueda ser visto. Además, el panóptico tiene la función de producir en los presos la sensación de vigilancia en todo momento, llevándolos a comportarse de manera distinta a lo que harían si no tuviesen la torre en frente suyo.

Este concepto puede ser aplicable a este sistema de control que proponen las plataformas: el usuario está expuesto, otorga datos voluntariamente y la plataforma moldea sus comportamientos a futuro en función de sus gustos. Son juzgados por estos algoritmos.

La autonomía del usuario dentro de las plataformas también es una de las aristas más importantes dentro de este estudio. Las decisiones dentro del ecosistema se encuentran sesgadas por este control social en el que están inmersos: la libre elección y la confidencialidad de las personas queda vulnerada al no estar informado de que harán posteriormente las empresas con los datos personales, ya que una vez cedidos se puede llegar a generar patrones asociados al usuario, por ende los anuncios serán en función de los gustos y preferencias. La autonomía del usuario se debilita.

Pero antes de seguir desarrollando el tema, debemos comprender a qué nos referimos cuando hablamos de cláusulas o de términos y condiciones/servicios. Los términos y condiciones son las reglas del juego impuestas por cada aplicación. Más precisamente son las cláusulas legales propuestas por estas páginas web o redes sociales que rigen la forma de consumo de sus contenidos e información a la que se puede acceder dentro de la misma. Estas

disposiciones además establecen que se hará con los datos personales que ingresan al sistema al crear un usuario y los datos que se crearán durante el paso del mismo dentro de la aplicación.

Según el abogado Luis Nocera, presidente de la Asociación Argentina de Lucha Contra el Cibercrimen, desde un punto de vista jurídico, estos términos son contratos de adhesión, esto quiere decir que las cláusulas no se pueden negociar, por lo tanto se acepta lo que sea, sin opciones. Nocera nos da una pauta sobre la privacidad y las consecuencias de aceptarlos:

“¿Hasta dónde juega mi privacidad? Vos aceptaste un contrato y cada país lo ve distinto, pero sí, se corren riesgos. Lo que sucede es que existe una posibilidad de que tus datos o información sean utilizados siempre con una lógica empresarial, la idea de la empresa es generar ingresos”.

Otra definición precisa que nos proporciona Daniel Monastersky, abogado especializado en protección de datos y Director del Centro de Estudios en Ciberseguridad y Protección de Datos de la Universidad del CEMA, es la de considerar a los términos y condiciones como un documento que define los derechos y obligaciones que van a existir entre las partes. Pero agrega que: “A veces los términos no son tan vinculantes como uno creería, ya que pueden existir cláusulas leoninas”. Dichas cláusulas son las impuestas por una de las partes sin dar la posibilidad al usuario de negarse a aceptarlas, por lo que pueden llegar a ser nulas desde el punto de vista legal.

Las plataformas se alimentan de nuestra confianza en ellas, pero ¿Realmente podemos confiar? Muchas veces sucede que uno no sabe para que la van a usar gracias a la ambigüedad que presentan, no se sabe a quién van a vender los datos, nunca se puede estar 100% confiado de que sucederá. Nocera dice que ninguna empresa es confiable ya que hasta las aplicaciones de los bancos tienen problemas como el de la suplantación de la identidad.

Es imperioso aceptar estas condiciones para poder utilizar los servicios de la aplicación. El usuario al aceptar da su consentimiento para que se gestione, comercialice, procese su información. Información que va desde datos bancarios, tarjetas de crédito, fotos/videos, y toda la estela de su paso por la misma.

Según Bárbara Peñaloza, abogada especialista en derecho informático y cibercrimen, existe una infinidad de aplicaciones que piden distintos tipos de datos y que por lo general no se leen los términos, pero aclara que los riesgos en general no hacen a su integridad física o psicológica, sin embargo, al aceptarlos se otorgan permisos que suponen una intromisión a la intimidad –que muchas veces pasa desapercibida- de las personas, que según Peñaloza:

“Es un derecho humano y muchas veces la persona desconoce que la aplicación accede a esos datos. Por ejemplo, cuando una app accede a la libreta, puede acceder a datos de los contactos que tienen las personas en su lista. También se permiten accesos a las galerías, donde hay fotos tanto del usuario como de terceras personas”.

Se asume que este contrato legal explica que es lo que van a hacer con la información personal recolectada: donde se guardan (solo un porcentaje lo expone), para que se van a utilizar los datos, si serán compartidos con otras personas, las políticas de privacidad y los derechos del usuario. Por estas razones y una extensa lista es que es importante leer estos contratos.

Según la periodista española Blanca Delgado en su tesis de grado “Términos y condiciones de uso en Internet: La normativa es inútil sin la autorregulación del usuario”, manifiesta que: “Los datos de la vida privada o laboral que propiciamos de forma inconsciente al aceptar los términos y condiciones de uso serán comercializados y hasta exhibidos de forma pública en internet”. Además Delgado asegura que son muy pocos quienes leen estos términos y condiciones de uso al registrarse en alguna página web. Aquí yace uno de los problemas más importantes de este estudio: el desconocimiento por parte de los usuarios.

María Julia Giorgelli, abogada encargada de temas de Cibercrimen en el Ministerio de Seguridad de la Nación, dice que lo que nos rige hoy por hoy es un paradigma relacionado a lo que tiene que ver con la denominada autorregulación. Las aplicaciones y plataformas establecen sus términos y condiciones y nosotros como usuarios decidimos si adherirnos o bajarnos de ese contrato de adhesión. Es utilizarlas o someterse a un “apagón digital”.

“No hay duda que la navegación en internet y el exponer nuestra información personal habilita que uno sea víctima de delitos por parte de personas que acceden a nuestra información. Sin embargo no tiene que ver estrictamente con las plataformas, sino con uno mismo, el usuario”.

La inmediatez es uno de los conceptos más actuales que existen. Los usuarios cada vez requieren más rapidez y es por esto que la mayoría no lee los términos y servicios, el cliente no quiere invertir tiempo en saber qué sucederá una vez dentro de la app, solo quiere disfrutar de los beneficios que le ofrece. Términos y condiciones que, dicho sea de paso, no son de lectura fácil; Las empresas utilizan un vocabulario difícil de comprender. En estos términos, esta inmediatez se ve reflejada directamente en la llamada Big Data.

La **Big Data** colabora en la recopilación de datos de las plataformas. Es una de las herramientas más influyentes dentro de esta Web 2.0 y este nuevo mundo digital. Reconocido por cosechar grandes volúmenes y cantidades de datos a través de algoritmos. Un documento publicado por la Revista de Bioética y Derecho de la Universidad de Barcelona en 2017 afirma que el fin del Big Data es “establecer correlaciones entre dichos datos, predecir tendencias y tomar decisiones”.

La información recopilada por el Big Data se encuentra almacenada en diversos servidores por todo el mundo y es por esta deslocalización que es tan difícil regular. Facebook y Google son los dos más grandes ejemplos de captación y análisis de datos a través de esta herramienta.

En este estudio podemos advertir que la Big Data puede llegar a tener aspectos contraproducentes y Maria Julia Giorgelli también afirma:

“Puede ser contraproducente, pero es el estado de situación en el que estamos. La aplicación de inteligencia al tratamiento masivo de datos es uno de los problemas de la época, respecto a esto la ley de protección de datos habla de que el tratamiento automatizado de datos personales, **tiene que ser explicitado específicamente** a las personas. Tienen que saber cómo se hacen, con que lógica.”

Van Dijck en su libro explica ciertas herramientas y mecanismos que utilizan las plataformas para esta recolección de datos que terminan dentro de la red de la Big Data. Ella habla de la “datificación”, “mercantilización” y “selección”.

La datificación es un mecanismo que se basa en la conversión en datos de ciertos aspectos que normalmente no podrían ser catalogados como tales. Gracias a este proceso, las plataformas datifican perfiles ofrecidos voluntariamente por clientes, comportamientos de los usuarios dentro de sus teléfonos inteligentes o geolocalización a través de GPS.

La parte comercial del planteo de Van Dijck se centra en la “mercantilización” de estos datos. Según la autora se transforman actividades, emociones e ideas en línea en productos comercializables. Dentro de esta commoditización están los algoritmos que personalizan a los usuarios, que comparten el interés exacto y preciso de lo que el público consume. Aquí entra en juego el último mecanismo que propone la autora, el de “selección”: la plataforma selecciona qué publicidades o anuncios mostrar a cada uno de los usuarios en función de los datos que fue arrastrando durante su navegación dentro de la red.

Toda actividad humana dentro de este ecosistema, sean “me gusta”, “retweets”, seguir o dejar de seguir a alguien que parecieran ser acciones totalmente normales o cotidianas, para las plataformas son datos valiosos que son recolectados. Datos que son analizados por infraestructuras digitales descentralizadas a través de algoritmos.

El caso de Facebook es emblemático, ya que al recolectar la actividad humana dentro de su plataforma, perfila según gustos, preferencias y características demográficas para penetrar con anuncios y servicios ofrecidos de manera más directa y eficaz.

Los datos son una de las materias primas más importantes de la actualidad, es tanta la información que corre dentro de internet que prácticamente es incontable. El autor y abogado español Javier Puyol Moreno comenta en un documento publicado en la Revista de la Universidad Nacional de Educación a Distancia que Big Data recoge datos de diversas fuentes: videos, imágenes, redes sociales, transacciones de comercio electrónico.

Es evidente que la venta de datos a terceros y la vigilancia que proponen las aplicaciones puede llegar a ser un riesgo y la regulación queda obsoleta tras los pasos agigantados que da la tecnología. En este estudio proponemos una pregunta: ¿Qué sucedería si los datos de una persona son vendidos a una empresa que contrata personal y el perfil de esa persona no encaja en ciertas empresas? Esta pregunta deja entrever que hasta el futuro de las personas puede verse afectado tan solo por las búsquedas que haga, los likes, los comentarios son pequeñas huellas que se van dejando en la aplicación.

Dentro de las plataformas existe un intercambio entre usuarios y las mismas. Según José Luis Fernández en *Plataformas Mediáticas: elementos de análisis y diseño de nuevas experiencias*, ese **tráfico de clics**, de informaciones y contactos derivados que se da dentro de las aplicaciones son objeto de búsqueda por parte de empresas y hasta de sectores políticos:

“Las marcas, sus productos y servicios, tanto como sectores políticos y de opinión operan y **pagan** para que el tráfico de clics converja con sus objetivos comerciales o de persuasión” (Fernández, 2018).

Los riesgos que asumen los nuevos usuarios en las plataformas son, en algunos casos, el acceso a las fotos, mensajes, ubicación actual y la venta de los datos personales a empresas privadas. A consecuencia de la aceptación, las empresas beneficiadas utilizan los datos para adaptar la publicidad según las preferencias de cada uno además de vender los datos personales y tener acceso a todo el material que porte el usuario.

A medida que fueron pasando los años, esta nueva era tecnológica acapara casi todos los espectros de nuestra sociedad. Tanto empresas como gobiernos fueron involucrándose cada vez más durante estas últimas décadas, hoy por hoy, se le exige a internet cierta protección en los datos, el problema, según Luis Nocera, de la AALCC, es que quienes tienen que proteger los datos son las personas, internet no está hecho para la protección de datos. Uno de los casos de extracción de datos más resonantes de los últimos tiempos involucró a uno de los grandes del internet.

El escándalo de la consultora Cambridge Analytica y Facebook marcó un antes y un después. El caso se trató de la extracción y manipulación de datos e información de 87 millones de usuarios de todo el mundo -en su mayoría de los Estados Unidos- dentro de la red social, a través de una aplicación “*This is your digital life*”, que funcionaba como un test de personalidad. Fue elaborado por Aleksandr Kogan -investigador de la Universidad de Cambridge- con supuestos fines académicos.

Alrededor de 270 mil personas accedieron y para poder completar el test había que iniciar sesión en Facebook y aceptar los términos y condiciones: se permitía el acceso a la actividad del usuario y su ubicación. Pero la cláusula más importante consistió en permitir el acceso a la información de los amigos de todas estas personas, lo que trajo un profundo escándalo en términos de confidencialidad, privacidad y consentimiento por parte de los amigos de las personas que hicieron el test.

Este es un caso que legitima las dudas que hay con respecto a las redes sociales, a los riesgos que se corren cuando uno acepta términos y servicios de aplicaciones, nuestros datos están en plena exposición y pueden ser recolectados con tan solo un clic. Todos los datos recabados por Kogan fueron compartidos -sin autorización de los usuarios- con Cambridge Analytica, que llevó adelante campañas políticas -por ejemplo, las elecciones de Estados Unidos en 2017 en dónde ganó Donald Trump- basada en anuncios personalizados gracias a todos los datos recogidos.

Relacionado con el término del panóptico y la torre de vigilancia, nos encontramos con otro aspecto a desarrollar que deja aún más entrever cómo las redes sesgan de cierto modo a los usuarios con sus preferencias. Generalmente, la plataforma a través de algoritmos recomienda aspectos que interesa al usuario y funciona como un filtro de información mostrando sólo una parte de la inmensa realidad.

El autor Eli Pariser en su libro “El Filtro Burbuja: Cómo la web decide lo que leemos y lo que pensamos”, propone una mirada crítica sobre la personalización -que según el autor

es inevitable- que hacen las redes sociales y las páginas web sobre el comportamiento de las personas.

La estela y el rastro que los usuarios dejan en dichas plataformas, es alimento para estos algoritmos que, en función de mejorar la calidad de la navegación del cliente, dejan entrever que podría llegar a ser contraproducente, que podría ser un riesgo para el consumidor.

Pariser en su texto propone pensar a esta personalización como una burbuja de filtro. Una burbuja que puede tomarse como una zona de confort propuesta por las redes y las páginas web que visitamos a menudo, las que habitualizamos al visitarlas todos los días. Los intereses de los usuarios en las plataformas quedan plasmados en navegaciones posteriores. Esta personalización que critica el autor por parte de los algoritmos, tienen como efecto un bucle de identidad del cual el usuario no puede salir. Se reafirma lo que al usuario le gusta en todo momento, achica el abanico de posibilidades y marca preferencias a futuro.

El autor plantea una posible solución: “sería razonable que los datos que los usuarios proporcionan a las empresas estuvieran a disposición y que expliquen cómo utilizan los datos: que fragmentos de información están personalizados y hasta qué punto”. Los datos personales y la marca personal de los usuarios en este nuevo ecosistema digital tienen más valor que nunca.

El libro de Pariser cita a Marc Rotenberg, director ejecutivo del “Electronic Privacy Information Center” -un centro de investigación de interés público en Washington, fundado en 1994- y asegura que no podemos tener servicios gratuitos en internet sin importantes violaciones de la privacidad: de qué manera nuestros datos determinan el contenido y las oportunidades que vemos, y más importante aún, las que no vemos.

Ahora bien, ¿Cuáles son los riesgos específicos que tiene el usuario al ingresar a este ecosistema?

La pérdida de la supuesta privacidad o confidencialidad supone un riesgo para el usuario. En ningún momento uno se encuentra en un ámbito privado en términos de redes sociales e internet. Subir una foto a una red social implica un riesgo, ya que una vez que esa foto está en línea, ya no le pertenece a la persona, sino que le pertenece a la aplicación.

La personalización de las personas dentro del ecosistema no solo “invaden” el feed de sus redes, sino que también, al poseer nombre, apellido, rostro y hasta hábitos, dejan expuesto al usuario en términos de reconocimiento. Esto puede presentar diversos riesgos que vamos a explicar a continuación:

1. **Phishing y pharming:** es la forma más común para recabar datos personales de usuarios en internet.

Según el artículo publicado por la Revista de Derecho de la Pontificia Universidad Católica de Valparaíso y escrito por Nicolás Oxman:

“El “phishing” y el “pharming” son dos tipos de fraudes informáticos que han aparecido desde mediados de la década pasada, cuya finalidad común es la de apoderarse de información personal de un usuario de Internet, para acceder a sus cuentas de correo o de redes sociales y obtener adicionalmente datos de sus contactos virtuales, a fin de comerciarlos ilícitamente, o bien, conseguir claves de “e-banking” para de este modo ingresar a las cuentas corrientes bancarias de los titulares y disponer del dinero que en ellas se encuentra”

2. **Spam y Spammer:** son quienes mandan los famosos “correos no deseados” a través de diversas redes sociales/aplicaciones, dentro de estos correos puede haber malware.
3. **Suplantación de identidad:** se trata, principalmente, de gente que se hace pasar por gente con fines maliciosos.

4. Uso de “Cookies” sin conocimiento del usuario: la página web que no comunica la utilización de cookies, una herramienta para conocer cuál es la actividad del usuario dentro de este sitio.

El autor David López Jiménez, en su artículo “Las Cookies como instrumento para la monitorización del usuario en la red: La publicidad personalizada” da una precisa definición de qué son las **cookies**:

“Las cookies pueden definirse como pequeños ficheros de texto, que algunos servidores Web piden al navegador -Chrome, Internet Explorer, etc- que escriban en nuestro disco duro información sobre lo que hemos estado haciendo en sus páginas”.

Según Monastersky las cookies hacen un monitoreo o “tracking” de nuestra información y existen diversos tipos: hay cookies con fines publicitarios y otras que son necesarias para, por ejemplo, identificarte quien sos. Algunas exceden las funciones necesarias para las que son configuradas. Un ejemplo que nos proporciona Monastersky: “Por ejemplo, te metes en Infobae y hay cookies que lo que permiten es hacer un seguimiento, buscas algo en Google y en Infobae te aparece una publicidad de eso que buscaste, ya que se generan perfiles de consumidor”.

En el caso de ingresar a un sitio que no comunica que están usando cookies con fines que violan los derechos del usuario, sí, se está vulnerando la privacidad. El sitio web debe contener, según Monastersky, un “disclaimer” -es decir un descargo de responsabilidad- que comunique al usuario que cookies desea utilizar y cuáles no. Existe un “deber de información” y agrega que la ley es clara y se habla de “responsabilidad proactiva”.

“Si haces un reclamo de que hay cookies que están creando un perfil tuyo de consumidor cuando en ningún lugar te dieron esa información sobre el alcance o finalidad que iban a hacer con tu datos, ellos deberían probar (para no tener un problema) que contaba con tu consentimiento, tiene que estar documentado”.

En la sociedad de la información, estas cookies son herramientas que sirven a la hora de concentrar mucha información, además de facilitar la navegación del usuario y ofrecer publicidad basada en hábitos de navegación, es decir, que aquí yacen la mayoría de las inversiones con fines publicitarios.

5. Ransomware: es un tipo de “malware” o software malicioso. Luis Nocera, presidente de la Asociación Argentina de Lucha contra el Cibercrimen (AALCC) nos explica su funcionamiento y el modus operandi de quien lo utiliza:

“Te bloquean tus datos, te dicen: ‘si quieres tu información tenes que pagar tantos bitcoin’, es un secuestro de datos. Si hay un hueco en el sistema pueden ingresar. Con los aplicativos hay tanto acceso a tu información, que no sabes hasta dónde puede llegar”.

6. Mercado negro de perfiles y redes sociales: Según Nocera:

“Existe un mercado negro de perfiles. Por ejemplo: un perfil armado de 40.000 seguidores vale fortuna. Son perfiles que se hackean y son vendidos a la persona que esté buscando eso mismo. También se venden perfiles con las fotos y todo para generar phishing y estafas.”

Uno de los riesgos más visibles a la hora de la extracción de datos se da cuando hackean un mail personal. Según Monastersky mucha gente no le da la importancia necesaria: “Pueden tomar acceso de tu mail, tus contactos saben y tienen validado ese correo electrónico con tu persona, imagínate que desde ahí pueden hostigar, amenazar, calumniar, contactarse con menores. También pueden llegar a alojarte contenido vinculado con el abuso y la explotación sexual infantil y te denuncia. Se puede tener un problema, ahí se habla de la cultura, vos sos víctima de un hackeo de tus datos y la gente tiene que saber que tiene que denunciar ese hecho, en caso de que pueda pasar algo, tiene que estar asentado que te hackearon”.

El problema con estos diversos riesgos que se corren en la red es que algunas cuestiones no están establecidas como “delito”: por ejemplo el hostigamiento, la suplantación de identidad, publicación de imágenes íntimas sin consentimiento. Modalidades como estas han surgido en el último tiempo, en Europa este tipo de hechos delictivos si están penalizados.

En esta región existen muchas cuestiones en las que estamos desprotegidos. Nocera argumenta que si no nos cuidamos nosotros mismos, no hay forma de evitar este tipo de cosas.

María Julia Giorgelli adhiere a que en Europa la regulación y reglamentación está mucho más avanzada, según la abogada en la Unión Europea se ha flexibilizado el consentimiento: “se habla del consentimiento libre, inequívoco”. En Europa es otro diseño institucional, allí las entidades son más fuertes, se hace un seguimiento más certero.

La suplantación de identidad tiene una particularidad. Según Monastersky en California y en tantos otros lugares, está regulado pero tiene una excepción, la suplantación no es delito en el caso de que sea con fines paródicos. Por ejemplo, si un usuario crea un perfil de Twitter de un famoso, que obviamente es falso, debe agregar en su “biografía” que se trata de una cuenta “no oficial” para no configurar un delito.

Uno de los temas centrales en cuanto a los riesgos que se pueden llegar a correr es que en los términos deben definirse con precisión los alcances de los datos que se brindan y la **finalidad**, el para que se van a utilizar. Con respecto a los alcances, Monastersky manifiesta: “A veces te piden datos porque lo que quieren es generar contactos de personas para poder venderles algo, para sumarlos a un envío masivo de información. Y con eso hay que tener cuidado”.

Existe un concepto que tiene que quedar claro desde el vamos por parte de las plataformas, y es el de “**la finalidad del dato personal**”, Giorgelli propone un ejemplo: si un medio de comunicación ante un delito entra al perfil del delincuente, la foto debe ser mostrada en el medio de manera que no sea claramente visible el rostro del implicado, debe estar blurreada o difuminada. Si en algún momento se sube una foto propia a una red social, esa foto no puede ser utilizada con otro fin.

Insistimos en este concepto porque en general cuando uno consiente el uso de los datos al aceptar los términos de una app, se asume que se están utilizando para fines publicitarios y no para que los vendan o se usen para otras cosas, ya que allí habría una ilegalidad.

Bárbara Peñaloza adhiere a este concepto de finalidad que aborda Monastersky, ya que en esta intrusión en la privacidad de las personas, hay que distinguir varias cosas: de que app se trata, quien está detrás, como van a tratar los datos y de que formas. Estos datos que pueden terminar en manos de terceros pueden llevar al usuario a ser víctima de actos de discriminación –laboral y/o social- y de ciberdelitos –económicos. Según la abogada durante la pandemia han proliferado aplicaciones con el afán de luchar contra esta situación, sin embargo, manifiesta que puede llegar a ser contraproducente:

“Surgieron iniciativas públicas, estatales, de apps donde uno vuelca datos sensibles, cuestiones relativas a mi salud y mi ubicación. El desconocimiento de quien va a usar esos datos o tratar y como, es un riesgo. Si se desconoce la finalidad, puede llegar a hacerme víctima de una fuga de datos –ceder datos a alguien que el usuario desconoce-”.

La privacidad muchas veces se ve vulnerada y casos resonantes en Argentina tienen que ver directamente con una invasión a la privacidad. Según Giorgelli, han existido casos como por ejemplo el del Blogspot “Cazador Legal”, donde una persona anónima sube fotos de colas de mujeres. Se han iniciado acciones para que se dé la baja de ese contenido, pero Google –ya que Blogspot pertenece a Google- informa que no procede porque según los términos y condiciones de sus plataformas, eso puede afectar a la “libertad de expresión”, por lo tanto no se puede suprimir esa información personal.

Los riesgos son amplios y grandes. Más allá de la venta a terceros, otro problema importante es el cómo se van a tratar esos datos, cómo los juntan, que redes de relaciones pueden llegar a generar, dónde paran, si van a hacer inteligencia sobre estos. Es complejo y según Nocera es un gran negocio turbio el que hay detrás de los datos.

El **marco legislativo** que rige en Argentina está apoyada sobre la Ley de Protección de Datos Personales (Ley 25.326), que argumenta que cualquier base de datos perteneciente a alguna persona, debe estar registrado en el registro de protección de datos personales y manifestar en dicho registro que tipo de datos posee: sensibles -por ejemplo una enfermedad, movimientos bancarios, etc.- o no sensibles -nombre y apellido, fecha de nacimiento-. Asimismo, surge de esta Ley de Protección, los denominados "Derechos ARCO" (Acceso,

Rectificación, Cancelación y Oposición), cumple estas cuatro funciones en relación de los datos personales, Monastersky dice: “donde sea que estén haciendo un tratamiento de tus datos, puedes acceder, rectificar, suprimir u oponerte si algún dato está incorrecto”.

Una característica importante a tener en cuenta con respecto a la Ley de Protección de Datos Personales es que desde el año en la que se dictó (año 2000), no hubo ninguna reforma. Con el avance de Internet durante todos estos años, la Ley está obsoleta en muchos sentidos, por ejemplo, la Ley no habla de perfiles de consumidor, como por ejemplo si lo hace la normativa europea, que entró en vigor en el año 2018.

La actualización en esta materia es más que fundamental, te deja afuera de muchas cuestiones y sin posibilidades. Según Monastersky “ninguna empresa sería va a querer que nosotros desde Argentina tratemos datos de personas del primer mundo, cuando ni nosotros mismos los cuidamos o nuestra normativa no está actualizada”. Con respecto a este punto Monastersky argumenta:

“La Ley Argentina no habla de cookies o de un montón de cuestiones que hoy son fundamentales, tampoco habla del Derecho al Olvido (es el derecho que tenemos como usuarios, titulares de datos, que internet elimine contenido que no es pertinente por el paso del tiempo, o contenido falso, etc.) en Argentina no está reglamentado.”

La Ley Argentina necesita *aggiornarse*, según manifiesta Peñaloza, se necesita reformar considerando todas las nuevas herramientas que nos ha traído la tecnología estos últimos años: la recopilación de datos, el tratamiento. Se hace necesaria una reformulación acorde a los tiempos nuevos que corren y uno de los puntos importantes tiene que ver con el comercio electrónico, deben redactarse reformas que hagan a esta comercialización una actividad segura para así poder evitar daños.

Esta normativa protege a los usuarios tanto en metodologías analógicas como digitales. En el caso de que existan datos incorrectos sobre una persona en internet, la misma puede pedir que se elimine o se rectifique esa información, en el caso de que haya un dato falso y se pueda demostrar que lo es, se puede pedir que el mismo sea dado de baja.

Según dicha Ley, el tratamiento de los datos será ilícito en el caso de que el titular de los mismos no hubiera prestado consentimiento libre. Este permiso otorgado por el dueño de los datos, deberá constar por escrito u otro medio que lo verifique, por ejemplo aceptando términos y condiciones. En el caso de que estos datos se obtengan gracias a fuentes públicas, no hará falta tal consentimiento.

Para la normativa argentina y también para el reglamento europeo, el consentimiento se tiene que hacer de una forma determinada, que este delimitado en algún lado quien va a ser quien utilice los datos, si se hace de forma indeterminada, se trata de un tratamiento ilícito de datos. Monastersky nos da un ejemplo:

“Si en los términos dice que los datos serán utilizados por Carrefour y sus ‘socios comerciales’, es indeterminado, porque no enumera ni detalla quienes son los socios comerciales, es decir, incumple las normativas de protección de datos”.

Mucho hablamos de la poca fuerza que posee esta Ley de Protección, pero también hay que tener en cuenta a las entidades que regulan la protección de datos personales. Bárbara Peñaloza manifiesta que es necesario reforzar a las mismas:

“Es necesario fortalecer ciertas instituciones, por ejemplo la Agencia de Protección de Datos Personales en nuestro país es una entidad que no tiene mayor injerencia como en otros lugares. También es importante fortalecer al poder judicial y que tenga herramientas adecuadas”.

Herramientas como el Código Procesal deben estar actualizadas, tienen que, según Peñaloza, permitirle a los operadores del derecho poder encausar, o mejor dicho poder acceder a la justicia ante un caso del entorno digital y reclamar la protección, autorizando a los abogados a acceder a pruebas digitales en tiempo y forma.

Uno de los problemas más importantes con la regulación a nivel nacional e internacional es que depende mucho de los tratados internacionales que haya firmado cada país, no existe un conductual común que rijan de la misma manera para todos porque depende de cada país y cada organización internacional -OEA y ONU en nuestro caso-.

Existen muchas zonas grises dentro de las normativas y dentro del marco regulatorio. Por ejemplo, la Ley de Protección de Datos en Argentina expresa que cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara. Estos términos y condiciones que nosotros aceptamos habitualmente tienen un vocabulario complicado, difícil de comprender, por lo tanto no cumple con la pauta de claridad que la Ley exige. No obstante, la información está expresada en estos contratos.

Uno de los casos más resonantes del 2021 es el de la actualización de las políticas de privacidad de WhatsApp, que obligaba a los usuarios a aceptar los términos que proponían si se quería seguir utilizando el servicio. En Argentina, según Monastersky, se presentó en la Secretaría de Defensa de la Competencia, un documento alegando que un servicio no puede cambiar los términos y condiciones negándote la posibilidad de seguir usando el servicio por el simple hecho de cambiar algunas cláusulas.

“Internet se maneja con la denominada **Gobernanza en Internet**, funciona como un conductual común a nivel mundial, también son acuerdos que hacen distintos miembros del mundo para que internet funcione. Todas esas reglas no están escritas, solo están habladas y entendidas. Se ha manejado siempre así, se trata de mantener un internet claro prolijo y transparente, por eso no hay muchas cosas escritas.”

Internet no tiene fronteras. Desde un punto de vista jurídico, se puede dictar toda clase de regulación en Argentina, pero si la empresa es de otro país y los términos imponen la jurisdicción para litigar en otro país, no se podría llevar a cabo un juicio contra la empresa en el caso de que se haya perpetrado algún delito contra información personal. Asimismo, si la empresa tiene representación en Argentina -es decir, una oficina en nuestro país- se pueden iniciar acciones legales aunque se haya aceptado los términos de afuera.

La característica de la digitalidad le da a las aplicaciones una ventaja con respecto a las regulaciones. Internet es muy dinámico y está en constante crecimiento y en cuanto a lo legal, en general, las apps buscan cuestiones complejas para que no los afecten tan

directamente. Igualmente, Nocera expresa que no se trata de regularlas, sino que haya una mayor facilidad de acceso a la justicia cuando sucede algo.

Una de las preguntas de importancia realizada a Monastersky para este estudio, es cómo hacer para que el derecho no se convierta en un obstáculo para el desarrollo tecnológico y que al mismo tiempo se pueda regular de forma válida, a lo que respondió:

“Es todo un trabajo que debe hacerse teniendo en cuenta que la normativa tiene que estar y existir, la costumbre va generando un camino y la última etapa se regula normativamente, pero debe analizarse bien porque puede ser una traba para el avance tecnológico”.

La normativa debe estar actualizada en todo momento. La tecnología avanza a pasos agigantados, los mecanismos existentes deben reforzarse ante cada avance, el derecho no alcanza los pasos enormes que da la digitalidad. Peñaloza aporta que a la hora de reformular la Ley, hay que apoyarse en ciertos principios que están fijados en nuestra constitución y que se plasman en diversas leyes específicas como la defensa de consumidores o defensa de la competencia.

Sociedad argentina, términos de servicio y la generación Millennial

El rango de edad es un factor muy importante en cuanto a la valoración de la seguridad personal dentro de la red. Actualmente, existe mucha gente que cree que internet es un mundo maravilloso y que no hay nada malo en ello, muchos de ellos pertenecen a un grupo etario de edades avanzadas. Por otro lado, están los que aceptan el juego de otorgar información y no le dan la importancia necesaria desconociendo el tema o ignorándolo.

Sin embargo es imposible extraerse de este nuevo mundo digital que propone el siglo XXI. Alejarse del entorno digital es prácticamente imposible, te desconecta del mundo y de la inmediatez. Bárbara Peñaloza adhiere a este concepto: “Hoy en día el entorno digital es prácticamente nuestra normalidad, excluirme de esos entornos o del uso de determinadas plataformas, redes o apps, me excluye del intercambio social, todo transcurre por allí”.

El desconocimiento por parte de los usuarios es una de las preocupaciones que más llaman la atención. Sin embargo Peñaloza nos da una mirada distinta con respecto a esta “falta de conocimiento”:

“En general yo no sé si hay un desconocimiento absoluto. La brecha se está acortando. Está achicándose esa cantidad de personas que desconoce absolutamente el uso de sus datos. Lo que está tomando más relevancia es la indiferencia, aun cuando conozco que posibilidades puede haber, igual se usa la app. Es indiferencia a conocerlo.”

La sociedad argentina no toma consciencia de las consecuencias que puede llegar a presentar la recolección de datos y el desconocimiento de los contratos que aceptamos en los términos y condiciones. La mayoría solamente quiere una asistencia rápida y nada más, y según Luis Nocera, abogado: “Lo que hagan con su información/datos personales a la gente no le importa, ni tampoco lo entiende”.

El desconocimiento va de la mano con el cambio cultural, que no existe, no se miden las consecuencias. Un ejemplo curioso que nos expresa Monastersky es el de una plataforma que incluyó en sus términos y condiciones un premio económico que no ganó nadie, dando la pauta de que prácticamente nadie los lee ni les dan importancia.

Utilizar la red social para entretenerse y divertirse, entre otras cosas, es una de las medidas más importantes a la hora de proteger nuestros datos. Según Nocera lo ideal sería no subir fotos que aludan a la intimidad de las personas: fotos con menores, fotos del jardín donde van los hijos/as, caminos habituales, etc.

La protección de datos personales también corre por cuenta de los usuarios. Una de las problemáticas que nos afectan a nivel social y cultural tiene que ver con la falta de educación que existe en términos de protección de privacidad y datos. No existe la cultura de la privacidad o como menciona Nocera: “*no hay cultura del cuidado del dato*”. El dinamismo propuesto por esta era digital hace que cualquier dato/foto/video que un usuario publique, en un segundo pueda estar en cualquier lado del mundo y en manos de quien sea.

Revalorizar la privacidad y la imagen del usuario es un de las tareas o una de las expectativas a cumplir a nivel sociedad. Todo lo que sucede y hacen las personas en internet queda ahí, según Peñaloza hay que tener como norte la idea de **permanencia**. La autora también plantea que es importante tener conciencia de los peligros que pueden suponer en el entorno digital, que viene dado de esa indiferencia respecto de los datos que se van dejando.

Algunos de los valores que promueve Peñaloza son, por ejemplo, evitar publicaciones riesgosas, ya que son invitaciones a las ciberestafas o publicar datos de los hijos. Asimismo lo de siempre, donde voy a estar o si voy a estar sola/o en mi casa, cuidar la privacidad tiene que ser un valor fuerte y debe transmitirse a niños, niñas y adolescentes.

En Argentina la cultura de datos y la expectativa de privacidad son casi nulas, no existe en los países de la región. Por otro lado, en Europa se da un reglamento de protección de datos muy dura y estricta, según Monastersky: “La normativa europea es tan rigurosa que hay sanciones de hasta más de 20 millones de euros y que en Argentina no pasa, ni tampoco las autoridades de aplicación hace mucho por cambiar esta cultura”. Además el abogado agrega que la cultura de datos debería empezar prácticamente desde el jardín hasta en los hogares.

Una de las soluciones o, mejor dicho, algunas medidas que servirían para ir cambiando la perspectiva con respecto al objeto de estudio de este análisis es el de trabajar directamente en los diseños institucionales, en las autoridades de protección de datos. María Julia Giorgelli propone que se debería trabajar de forma regional, es decir, con normas de carácter regional ya que el problema principal de internet es que no tiene fronteras o cuestiones de jurisdicción.

“Hay q trabajar fuerte en 2 vectores: campañas de concientización y difusión, y cuestiones de educación. Es importante en materia de Ciberseguridad desde el punto de vista más blando, no es solo seguridad informática, sino como cuidamos nuestros datos en el entorno virtual”

A su vez, Giorgelli agrega que hay que trabajar en un sentido blando: la configuración de privacidad que bien puede modificarse en casi todas las páginas web, hay que tener conciencia de que uno pierde el control de esa información que circula. Por otro lado también

hay que trabajar con las empresas de tecnología: “Para que de algún modo también tengan compromisos con cuestiones más de interés público, y no solo sean guiados por la innovación”.

La sociedad impone de cierto modo la vinculación a las plataformas, es imprescindible pensar en ellas en el siglo XXI. Son pocos los usuarios que se detienen a leer los términos y condiciones de uso de los datos personales al crear una cuenta.

Es mayor la voluntad de querer pertenecer al mundo virtual que pocos son conscientes de lo que posteriormente se hace con los datos. Si bien sabemos que se utilizan para su comercialización, los usuarios culpabilizan a las redes sociales cuando ellos a voluntad propia les conceden a terceros la información.

Desde hace ya algunos años podemos observar cómo la tecnología ayudó en el avance de los medios de comunicación, la apertura en su difusión y los nuevos canales. Una generación llamada Millennials creció con dichos avances y formó parte de la evolución. Esta generación la abarcan jóvenes que nacieron a finales del siglo XX y se encuentran completamente influidos por el ámbito digital y los cambios que esto trajo, además de conocer como era el mundo sin internet, creció junto a los grandes avances y formaron parte de esta revolución. La también llamada “Generación Y” posee una gran destreza digital, ya que supo adaptarse a los cambios que la tecnología obligó.

Haciendo referencia a lo dicho anteriormente, se considera muy difícil pensar un mundo en el que los más jóvenes no se involucren, necesitan pertenecer e interactuar, el sentido de pertenencia es importante hoy por hoy. Según Peñaloza no se piensa mucho en las consecuencias que esto podría traer, ella cree que la necesidad de interacción social le gana a la razón.

“Curiosos e inconformistas que no solo buscan y se nutren de la información diaria de los medios de comunicación e Internet, sino que son característicos porque participan de ella. Comparten, opinan, debaten e interactúan a nivel global gracias a las nuevas tecnologías,

creando de esta forma un nuevo paradigma comunicativo que se basa en un modelo circular, en el que cobra más importancia el *feedback*, que el propio mensaje inicial que quiera transmitirse”.

El nuevo paradigma, anteriormente mencionado, produjo cambios en la forma de comunicar. El avance tecnológico colaboró a que el usuario no sólo utilice los medios para informarse sino también que se exprese y comparta su opinión. Este fue el fin de una era en la que el diario llegaba y sólo nos permitía transmitirnos los sucesos de la actualidad.

El uso de datos y la conexión virtual es fundamental en el ámbito laboral, el usuario se ve obligado a formar parte por cuestiones netamente laborales y es ahí donde también se cede de forma involuntaria los datos personales y preferencias. En el área de marketing son imprescindibles, a mayor recolección de datos, mayor difusión puede tener la marca.

Es en este punto donde chocan dos intereses, si el usuario es consciente de la extracción de datos pero es un trabajador del área de marketing, se va a ver obligado a pertenecer, no por el hecho de desear formar parte del círculo virtual sino por cuestiones laborales, mismo Facebook brinda datos de clientes pero debes acceder de tu cuenta personal para loguearte y obtenerlos.

Nick Jones, vicepresidente ejecutivo de innovación y crecimiento en Arc World Wide, hizo unas declaraciones al respecto de todo ello en uno de los principales congresos a nivel mundial sobre innovación y tecnología, que se celebra en Barcelona (Mobile World wide Congress 2016):

"La nueva generación de Millennials e incluso los públicos más jóvenes están cada vez más familiarizados con este tipo de mundo. Donde no hay tanta protección de la privacidad (...) Ven esto como un valor, más que una intromisión en su intimidad".

Jones, afirma que los jóvenes están cada vez más dispuestos a compartir sus datos y preferencias para que las publicidades adapten su contenido a ellos. De esta manera el usuario

no busca la información sino que le llega de acuerdo a sus intereses. La burbuja de Pariser hace hincapié en ese asunto, como fue detallado anteriormente.

Mark Zuckerberg, joven millennial, fue el padre de este cambio. El programador de 37 años supo cambiar por completo el modelo de comunicación con la creación de una de las plataformas más reconocidas mundialmente que forma parte de las Big Five, Facebook. Con sus pros y contras, el joven supo crear una red social que permitía la conexión con otras personas facilitando de esta manera el vínculo y cambiando de forma completa la manera de comunicarse.

Políticas de datos de las Big Five

Políticas de privacidad en Facebook:

Facebook, como mencionamos anteriormente, estuvo implicado en el conflicto con Cambridge Analytica. Es por eso que en la actualidad tienen mejor definidas sus políticas respecto a la privacidad de los datos y actividades de los usuarios dentro de la plataforma. En la actualidad, una de las cinco empresas más reconocidas en el mundo virtual, comparte preguntas con sus respuestas al alcance de los usuarios para que se puedan informar.

Dentro de la página responden la pregunta de qué tipo de recopilación hacen, “Recopilamos el contenido, las comunicaciones y otros datos que proporcionas cuando usas nuestros Productos. (...) También puede incluir el contenido que ves a través de las funciones que proporcionamos, como la cámara, para que podamos realizar acciones como sugerirte máscaras y filtros que quizá te gusten, así como darte consejos sobre cómo usar los formatos de cámara” (Facebook, 2021), es decir, que en este caso le informan al usuario que tiene acceso no sólo a sus datos personales sino también a la localización, cámara y contenido.

Ahora bien, ¿Qué se hace posterior a la recopilación de datos? Los datos recopilados se comercializan a terceros o a sus “socios” externos con los que trabajan y de esta manera no sólo obtienen una ganancia sino también la vigilancia de todos los usuarios respecto a la

privacidad y a las preferencias de cada uno. “En su lugar, las empresas y organizaciones nos pagan por mostrarte publicidad sobre sus productos o servicios. Al usar nuestros Productos, aceptas que te mostremos anuncios que consideremos relevantes para ti y tus intereses. Usamos tus datos personales a la hora de determinar qué anuncios te mostramos”. (Facebook, 2021).

A modo de conclusión, Facebook en sus políticas de privacidad describe con transparencia todo lo que hacen con la recopilación de los usuarios. Es decir, está bien explícito pero mantenemos la postura de que muchos de los usuarios no los leen.

Políticas de privacidad en Amazon:

La infraestructura que provee Amazon, también forma parte de las Big Five. En la página web oficial también mencionan qué tipo de información recopilan y que hacen con ella.

En primer lugar mencionan que reciben y almacenan cualquier tipo de información que el usuario proporcione, si se elige no proporcionar información la plataforma indica que el usuario no podrá disfrutar de muchas otras funciones que ellos ofrecen y “Al igual que muchos sitios web, utilizamos "cookies" y otros identificadores únicos, y obtenemos ciertos tipos de información cuando su navegador web o dispositivo accede a Amazon Services y a otro contenido servido por Amazon o en su nombre en otros sitios web” (Amazon, 2021).

Además expresan que la información que recopila la propia plataforma reciben más datos de otras fuentes como de los transportistas, información de entregas de productos, entre otras cosas. Pero, ¿Con qué fines utiliza Amazon los datos que recopila? Utilizan la información personal para “operar, proporcionar, desarrollar y mejorar los productos y servicios que ofrecemos a nuestros clientes”.

Por otro lado, para la compra y entrega de productos y servicios, para brindar soluciones a problemas y otorgar mejoras en Amazon Services, para recomendar funciones, productos y servicios y algo poco reconocido como la utilización de entrada de voz, imágenes

y cámara “utilizamos su entrada de voz, imágenes, vídeos y otra información personal para responder a sus solicitudes, proporcionarle el servicio solicitado y mejorar nuestros servicios“. (Amazon, 2021).

Además el sitio web enuncia que se utilizan los datos para cumplir con obligaciones legales, para mismo comunicarse con el usuario y para publicidad. Esta última es común en las Big Five ya que conectan anunciantes con perfiles que tengan las preferencias acordes a lo que ofrecen. También “Utilizamos información personal para prevenir y detectar fraudes y abusos con el fin de proteger la seguridad de nuestros clientes, Amazon y otros. También podemos utilizar métodos de puntuación para evaluar y gestionar los riesgos crediticios”. (Amazon, 2021)

Políticas de privacidad en Google:

Google es otra de las plataformas que forman parte de las Big Five. Dentro de su página oficial podemos encontrar información general accesible a todos los usuarios.

Desde Google afirman que los datos que recopilan desde la plataforma son para brindarle a los usuarios una mejor experiencia en su recorrido virtual, y para ello, necesitan información básica referida a los datos personales como así también el idioma de origen hasta datos más complejos ya referidos a preferencias para poder hacer que coincidan los anuncios con sus usuarios.

“El tipo de información que recoge Google y cómo se utiliza esa información depende del uso que hagas de nuestros servicios y de cómo administres los controles de privacidad. Si no has iniciado sesión en una cuenta de Google, almacenamos la información que recogemos con identificadores únicos vinculados al navegador, la aplicación o el dispositivo que utilices. Esto nos permite, por ejemplo, mantener tus preferencias de idioma en todas las sesiones de navegación”. (Google, 2021).

Políticas de datos de otras plataformas

Políticas de privacidad en Twitter:

Al completar el formulario de datos personales exigidos para la elaboración de la cuenta en la red social, nos encontramos con la cláusula de aceptación de los términos y condiciones que la página obliga a aceptar, de lo contrario no se podrá llegar a la etapa final en la que se integra a la comunidad de la plataforma como un usuario.

En el caso de Twitter, para leer dichos términos, se debe hacer clic en otro enlace que redirige hacia una página nueva. Allí se encuentran diversas cuestiones que explican a los usuarios el funcionamiento de la red y cuestiones respectivas a la seguridad de los datos, entre otras cosas.

La política de privacidad explica a los usuarios cómo se maneja la información que proporcionan los mismos utilizando la red.

“Comprende que mediante el uso que usted hace de nuestros Servicios, usted consiente a la recopilación y uso (tal y como se recoge en la Política de privacidad) de esta información, incluida su transferencia a los Estados Unidos, Irlanda y/o a otros países para su almacenamiento, procesamiento y uso por parte de Twitter y sus filiales” (Twitter, 2021).

Si bien uno no acepta al comenzar a utilizar la aplicación, posteriormente cuando actualiza la misma, la letra chica explica cambios en los procesos que muy pocos o ninguno llega a leerlos.

Desde Twitter afirman que los datos de todas las cuentas ya sea desde el tipo de dispositivo que se utiliza hasta los mismos datos personales se comercializan a terceros quienes son sus socios. “Estos socios de plataformas publicitarias actúan como controladores de esos datos. Las plataformas con las que actualmente trabajamos en calidad de tal son: Google y Facebook”. (Twitter, 2021).

Políticas de privacidad en TikTok:

La red social del momento, o mayormente utilizada por los más jóvenes, ofrece grabar y editar videos para compartir en el perfil con una duración de 15 a 60 segundos. Si

bien es una de las redes sociales que es tendencia, ¿sabemos cuáles son sus políticas con respecto a los datos que utilizan?

En su página oficial responden a la pregunta planteada anteriormente y agregan aún más información respecto a con quién comparten dicha información que provee el usuario y que a su vez alimenta al crecimiento de la plataforma. Debemos remarcar que Tik Tok en su página plasma incluso detalles que otras plataformas no. Además de la información que recopilan una vez descargada la aplicación y creada la cuenta comentan que también lo hacen sin la creación de la misma. "Recopilamos información sobre usted si descarga la aplicación y usa la Plataforma sin crear una cuenta" (TikTok, 2020). De esta forma no sólo recolectan información siendo usuario sino también no formando parte del mundo tiktokero.

El proceso ya nos suena familiar, es decir, podemos observar que la aplicación utiliza los datos de la misma forma que las grandes plataformas mencionadas con anterioridad. "Nosotros usamos su información para proporcionarle a usted la Plataforma y para mejorarla y administrarla. La usamos para ofrecerle una Plataforma efectiva y dinámica y, en el caso de que hayamos determinado que corresponde a nuestros legítimos intereses, la utilizaremos para mejorar y desarrollar la Plataforma, para impedir las actividades delictivas y para garantizar la seguridad de los usuarios. Siempre que contemos con su consentimiento, también utilizaremos su información personal para mostrarle publicidad personalizada y para promocionar la Plataforma". (TikTok, 2020)

Por otro lado, afirman que la información que aporta el usuario la conservan por tiempo indeterminado mientras tengan utilidad, "en el caso de que no necesitemos su información para prestarle a usted el servicio, la conservaremos únicamente mientras tengamos una finalidad comercial legítima para conservar dichos datos o si estamos sujetos a la obligación legal de conservarlos" (TikTok, 2020).

Políticas de privacidad en Whatsapp:

Si pensamos en la forma más rápida de comunicarnos, automáticamente se piensa en Whatsapp. La aplicación fue comprada por Facebook en 2014 por más de 4.000 millones de dólares y las políticas son similares al integrante de las big five.

En su página oficial declaran los usos posteriores de la información que el usuario proporciona. En primer lugar, con la creación de la cuenta, se brinda el número de celular y recopilan la información básica como el nombre y la foto que acompaña al perfil.

En segundo lugar, los mensajes que se envían a través de la interfaz no son conservados sino que se almacenan en el propio dispositivo pero cuando se realiza el envío del mismo proceden a eliminarlo del servidor, esto no sucede con los mensajes no entregados." Si un mensaje no se puede entregar de inmediato (por ejemplo, si el destinatario no tiene conexión a Internet), lo conservamos de forma cifrada en nuestros servidores durante un plazo máximo de 30 días mientras intentamos entregarlo" (Whatsapp, 2021).

El contenido multimedia funciona de diferente manera que los mensajes, en este caso los mismos son almacenados temporalmente de forma cifrada en los servidores. Las últimas actualizaciones de la aplicación permiten realizar un cifrado de extremo a extremo, esto significa que los mensajes no pueden ser leídos ni por la plataforma ni por terceros.

Por otro lado, Whatsapp manifiesta que utilizan la información para " operar, proporcionar, mejorar, entender, personalizar, respaldar y promocionar nuestros Servicios" (Whatsapp, 2021).

Políticas de privacidad en Instagram:

La utilidad que provee Instagram es compartir con el círculo virtual fotos y videos, además recientemente se agregó la opción de realizar compras u ofrecer productos para su comercialización en la misma. Esta red social forma parte de Facebook desde el 2012 y la recolección de datos funciona de la misma manera que WhatsApp y Facebook.

Toda la información que el usuario proporcione en la aplicación será utilizada para la recopilación. Es decir, cuando el usuario se integra al ecosistema virtual comparte de forma indirecta (con la plataforma) el contenido, ubicación, imágenes, la cámara cuando se la utiliza y las personas que rodean al usuario, entre otras cosas. "Recopilamos información sobre las personas, las páginas, las cuentas, los hashtags y los grupos a los que estás conectado y cómo interactúas con ellos a través de nuestros Productos, como las personas con las que más te comunicas o los grupos de los que formas parte". (Instagram, 2021).

¿Qué hacen con toda esta información recopilada? la aplicación utiliza la información a favor de sus funciones y para que su algoritmo funcione con mayor precisión. "Usamos la información que tenemos para proporcionar nuestros Productos, así como para personalizar las funciones y el contenido (incluidos la sección de noticias, el feed de Instagram, Instagram Stories y los anuncios) y hacerte sugerencias (como grupos o eventos que pueden interesarte o temas que quizás quieras seguir) tanto dentro como fuera de nuestros Productos". (Instagram, 2021). Whatsapp declara también sus fines comerciales, "colaborando" con socios externos como anunciantes, socios de medición, socios que ofrecen bienes y servicios en sus productos, entre otros.

Políticas de privacidad en Netflix:

El boom de Netflix surge en el 2015 cuando comienza a quebrantar las fronteras y expandirse internacionalmente. Esta plataforma ofrece películas y series a usuarios suscriptos que abonen mensualmente el servicio. Durante los últimos años, la plataforma supo crecer en relación a su servicio integrando series y películas producidas por la marca.

¿Qué sucede con los datos en esta plataforma? La información que recopila incluye el nombre del usuario, mail, dirección, formas de pago y número de teléfono además de la actividad realizada por los suscriptores en Netflix como las preferencias de películas, series, búsquedas y el id del dispositivo que se utilice.

La página declara que " la información recopilada a través del uso de cookies, contadores de visitas a la web y otras tecnologías, incluidos los datos de publicidad (por

ejemplo, información sobre la disponibilidad y entrega de anuncios, el URL del sitio, así como la fecha y la hora)" (Netflix, 2021).

Tipo de investigación

Como desarrolla el autor, Hernández Sampieri, las investigaciones se clasifican según la intención o finalidad que persiguen, en relación al tema el tipo de investigación será correlacional.

En esta investigación analizaremos cómo se vinculan las diferentes variables, más precisamente: cómo a más usuarios aceptando los términos y condiciones, sin saber los riesgos que implica el clic, más empresas o plataformas comercializarán datos personales.

Otra de las variables a analizar será la del desconocimiento por parte de los usuarios a la hora de aceptar estos términos y condiciones. Desconocimiento en términos de la comercialización de datos, la finalidad de los datos que ellos mismos otorgan, de manera consciente o inconsciente.

Marco metodológico

El marco metodológico nos permitirá identificar y comparar las diferencias en cláusulas de las plataformas infraestructurales. La perspectiva que se llevará a cabo corresponderá a un **método cualitativo**, ya que se busca otorgar profundidad en los datos y la lógica de recolección de los mismos.

Este método es subjetivo y múltiple ya que el investigador/es, como mencionamos anteriormente, está inmerso en el contexto de interacción que se desea investigar y asumimos que los valores van a formar parte del proceso de conocimiento.

En la investigación el muestreo que se utilizará para luego recopilar datos y será **no probabilístico por cuotas** debido a que nosotros como investigadores determinaremos cuáles serán los criterios para la selección de la muestra. Como por ejemplo, la clase social, marcos legales de las diferentes plataformas, variables en las cláusulas, entre otras.

Emplearemos una única **técnica de recolección** de datos y será la **entrevista**. La característica principal de esta es que será abierta, creemos que es conveniente que los entrevistados puedan desarrollar sus respuestas permitiéndonos observarlos como actores sociales. De esta manera no sólo serán útiles sus respuestas sino también su perspectiva y conocer cómo interpretan sus experiencias.

Las palabras del protagonista nos brindarán mayor información ya que este tiene un papel fundamental y al estar frente a frente serán más los aspectos involucrados que ayudarán en la recolección de datos.

Posibles preguntas:

1. ¿Cuáles son las plataformas que mayormente utilizas?
2. ¿Para qué las utilizas?
3. ¿Tomas algún recaudo a la hora de poner tus datos personales?
4. ¿Qué aspectos te hacen confiar en una plataforma? ¿Por qué?
5. ¿Por qué quieres formar parte del ecosistema virtual?
6. ¿Por qué crees que necesitan tus datos personales y preferencias?
7. ¿Cómo crees que ganan dinero las plataformas?
8. ¿Conoces el destino final o la finalidad de estos datos? ¿Qué te imaginas que hacen con los datos?
9. Cuando aceptas los términos y condiciones/ servicios ¿ lees todas las cláusulas? ¿Te parece importante leerlas?

Muestreo

La muestra de tipo no probabilística se compuso por treinta y dos participantes de un rango etario de 10 a 65 años residentes de Capital Federal y Gran Buenos Aires de ambos sexos (Mujeres= 41% / Hombres= 59%). En la elección de la muestra se consideró que sean

personas activas en el mundo virtual de al menos una plataforma o red social y edad de entre 10 a 65 años mencionadas anteriormente.

Para poder tener una buena segmentación de la muestra, se decidió separar a los participantes por el rango etario. El primer rango es de 10 a 17 años, en el que se contempla el punto de vista que tienen los pre-adolescentes y adolescentes, dueños de la nueva generación que se aproxima y una de las más provistas por las nuevas tecnologías de los últimos años.

El segundo rango de edad corresponde a la pubescencia y juventud conformada por personas de 18 a 25 años. El tercer rango etario corresponde las edades de gente de 26 a 35 años, gracias a los jóvenes adultos pudimos obtener mayor profundidad en sus respuestas, contemplando el paso del tiempo y madurez. Más adelante estaremos citando algunas respuestas que nos parecieron más nutritivas.

Por último nos enfocamos en los rangos etarios más avanzados, que van de 36 a 50 años y por último de 51 a 60 años.

Instrumentos

Se utilizó el método de entrevista para la recolección de datos dando lugar a preguntas que puedan desarrollar aún más cada respuesta favoreciendo a obtener una información completa. Se indagó acerca de qué tipos de plataformas utilizan, qué datos completan a la hora de la creación de la cuenta, los aspectos que dan confianza de la misma, la pertenencia al mundo virtual, la necesidad de obtener datos personales por parte de la plataforma, la finalidad de los mismos y la lectura y aceptación de los términos y condiciones.

Procedimiento

Proceso de recolección de datos

El proceso de recolección de datos fue mediante la entrevista personal o vía Zoom en dónde se le informó al entrevistado la finalidad del uso de la información obtenida al finalizar

las preguntas obteniendo el consentimiento de los mismos en el uso de sus datos personales como nombre, apellido y edad en el trabajo de investigación final.

Proceso de análisis de datos

Los resultados obtenidos al finalizar la entrevista se volcaron en una desgrabación con el formato de cuestionario dando lugar a la pregunta y luego la respuesta por parte de los entrevistados (ver anexo). Para lograr una integración en la información brindada por los mismos se elaboró una tabla en dónde tuvimos en cuenta las respuestas, el rango etario y la lectura de los términos y condiciones para luego basarnos en las conclusiones finales.

Análisis

El presente estudio tuvo como objetivo principal investigar qué riesgos asume un usuario en relación a la privacidad de sus datos cuando acepta los términos y condiciones que impone cada plataforma durante la última década. En lo que concierne al primer objetivo planteado se pudo determinar el grado de conocimiento por parte de los usuarios cuando aceptan dichos términos y condiciones o servicios a través de la respuesta en la encuesta realizada.

En segundo lugar, se realizó una encuesta específica para los profesionales de la cibernética y se pudo identificar descriptivamente los usos posteriores que las empresas le dan a los datos personales de los usuarios pertenecientes al mundo virtual vendiéndoles a terceros la información, mismo ellos comentándolo en sus políticas (un tanto ocultas).

En relación a cuáles son los factores principales que llevan a un usuario a aceptar los términos y condiciones o servicios mencionados anteriormente, se analizó la voluntad de cada uno en cuanto al pertenecer al mundo virtual. Con la información brindada por los entrevistados se puede afirmar que el deseo de integrar la virtualidad consiste en no quedarse afuera de las novedades ni de la vida de sus conocidos.

Todas las entrevistas comenzaron con preguntas que luego dieron lugar a la profundización de las mismas. Las entrevistas fueron presenciales y vía Zoom, se inició con

una presentación personal del entrevistado y posteriormente se consultó si forma parte del mundo virtual al menos con la utilización de una plataforma y sobre el tipo de redes o plataformas que utiliza a diario o eventualmente.

La red social más utilizada entre los pre-adolescentes y adolescentes es Instagram y Youtube, para este sector entrevistado la única preocupación es el paso del tiempo y así su único objetivo: el entretenimiento. Se pudo identificar que el público más joven es el más arriesgado a la hora de probar nuevas herramientas que proveen las aplicaciones y eso sucedió con TikTok, la red social que más euforia causó en los más chicos por su funcionalidad innovadora y disruptiva.

En relación al rango etario de 18 a 25 años, se puede observar el principal uso de la red social Instagram, una aplicación que está siendo actualizada constantemente. En segundo lugar, Twitter siendo el espacio elegido para obtener información de todo tipo.

La red social del pajarito azul es una de las más utilizadas a la hora de elegir informarse, no sólo por su acotada información sino también por la inmediatez que ofrece. "Utilizo Twitter principalmente para estar actualizada de las noticias y también para descargarme", afirma la entrevistada de 25 años.

Por otro lado Facebook, a pesar de tener menor relevancia en los más jóvenes, es la red social más utilizada y elegida en adultos de entre 26 a 60 años. Cabe destacar que tanto Instagram como Twitter siguen vigentes, la principal elección se da en una de las plataformas que conforman las Big Five: Facebook. En dicha plataforma comentan los entrevistados que obtienen todo lo que buscan en un mismo lugar: relaciones, información de actualidad y un market, entre otras cosas.

En el último tiempo, por cuestiones de la pandemia y público conocimiento, este rango etario se vio afectado económicamente, los emprendedores comentaron que gracias al market tanto de Facebook como Instagram pudieron utilizar el espacio que ambas plataformas ofrecen para obtener mayor visibilidad y para generar mayores ventas. "Instagram es fundamental para promocionar mi emprendimiento".

Con el fin de poder determinar la valoración que hacen de su propia seguridad, se consultó a los participantes qué tipo de cuidados o aspectos tienen en cuenta al crear una cuenta nueva en las plataformas.

Los más jóvenes demostraron tener mayores cuidados en relación a la seguridad de sus datos, no así el resto de los entrevistados quienes admiten que es importante cuidar de los mismos pero la plataforma te obliga a completar ciertos requerimientos para poder concluir con la creación del usuario. “Uno de los recaudos que tomo es leer las pautas y políticas de privacidad antes de escribir mis datos”, detalla Ignacio de 14 años. Por otro lado, Lucas, de 15 años, afirma: “tomo algunos recaudos. Algunas páginas que no son de confiar no los pongo”.

A pesar de haber una diversidad en las respuestas, todos los entrevistados confirman el deseo de poder tomar mayores recaudos a la hora de completar el formulario que provee la plataforma. Por un lado se pueden identificar usuarios a los cuales no les afecta o interesa la finalidad que tiene la plataforma con sus datos pero por el otro lado hay quienes intentan ser cautelosos con su privacidad y los cuidados que toman son en relación a información básica como domicilios. “Trato de leer las condiciones para que mis datos no anden circulando” (Gonzalo, 21 años).

Los recaudos que toman los de 26 a 35 años a la hora de completar el formulario para avanzar con la creación del usuario en la plataforma es completar únicamente los datos obligatorios: “No dejo datos importantes como tarjeta de crédito o cuestiones que sean muy personales”.

Otro usuario detalla que únicamente completa los campos requeridos para pasar a la siguiente etapa de la elaboración de la cuenta. “Generalmente pongo solo la información realmente necesaria como mail, fecha de cumpleaños y nombre completo. Intento no poner dirección de mi casa o mi número de celular”.

Algunos de los recaudos que emplean son en el contenido compartido en la red social, este cuidado surge una vez dentro del círculo virtual. “Trato de tener todo en privado para que

gente que no conozco no pueda verlos y no acepto desconocidos. Además publico muy poco sobre mi vida privada”.

En las edades más avanzadas se puede identificar que la mayoría no toma ningún recaudo, simplemente en los datos básicos. Exceptuando respuestas de participantes que sí los toman, pero que son minoría. Pocas personas conocen la finalidad de los datos, Daniel de 28 años afirma que siempre trata de tomar todos los recaudos posibles y que "desconfía mucho de algunas plataformas".

Cabe destacar que a pesar de ser una minoría, es importante remarcar que los usuarios comiencen a hacerse eco de hacia dónde van sus datos ya que pocos leen las políticas de privacidad compartidas en cada plataforma. “Trato de cambiar las claves cada tanto, que no se filtren datos de no cargar cuestiones familiares. Me preocupa mucho el tema de protección de datos y me parece que es un tema a tratar” (Alfredo, 57 años).

Uno de los objetivos principales de las preguntas fue determinar el grado de confianza que tienen los usuarios para con las plataformas o redes sociales que utilizan habitualmente. Se pudo hallar un mayor porcentaje de participantes que confían en las plataformas por la cantidad de usuarios que integran el ecosistema, es decir, aumenta la confianza en relación a la cantidad de usuarios que forman parte del mundo virtual, "que la use todo el mundo".

Por otro lado, las actualizaciones permanentes que ofrecen nuevos cambios son fundamentales para alimentar la confianza de las personas: “Si las plataformas son muy conocidas, me da seguridad. Además si WhatsApp tiene el respaldo de Facebook me da seguridad porque ya tienen mis datos”, Matías de 26 años.

Otro usuario define que lo que mayor confianza le brinda es la masividad y "el tipo de corporaciones que están detrás que imagino que cumplen regulaciones, normativas, etc.”, Juan, 36 años. Otra respuesta a destacar fue la de Valentina, joven de 21 años, “que no exponga tanto mi perfil y que tenga actualizaciones me hace confiar, cuando actualizan constantemente es una señal de seguridad”.

Otra de los aspectos los cuales ayudan a generar mayor confianza es que la aplicación esta verificada, es decir, que cumpla con ciertos requisitos. “Las verificaciones que te hacen para utilizarla me llevan a confiar”. Sasha, 25 años.

Por otro lado, se pudo delimitar también la existencia de cierto grado de desconfianza en usuarios que se sienten obligados a formar parte del mundo virtual por el acceso a ciertas cuestiones como trámites bancarios ya que en ocasiones la atención personalizada quedo nula. "No elegí formar parte. Me obligó la sociedad, al no tener atenciones personalizadas", dejando en claro su postura. (Guillermo de 64 años).

Si bien muchos desconocen para qué las plataformas necesitan de los datos personales, la otra parte no. Actualmente las plataformas buscan cierto grado de transparencia compartiendo sus políticas de privacidad, debemos destacar que se encuentran en las páginas oficiales de cada una pero que los usuarios optan por no leerlas por su complejo vocabulario empleado, la extensión y la letra chica. Todos los entrevistados afirman la importancia de su lectura pero pocos de ellos intentan realizarla.

En cuanto al conocimiento con el que cuentan los participantes del rango etario más bajo sobre por qué las plataformas requieren de la recolección de los datos personales y preferencias, se pudo determinar casi en su totalidad que estos desconocen la necesidad de las redes de poseer los datos de sus usuarios. Una entrevistada de 17 años afirmó su desconocimiento y supuso: “No sé, para verificar mis datos o por seguridad”.

Sin embargo, esta pregunta dio lugar a un par de excepciones, donde se pudo determinar cierto grado de conocimiento pero casi por debajo de la media, y en función de suposiciones: “No lo sé, supongo que para registrar o ver las cosas que me muestran o para ver que videos me pueden llegar a gustar”. La otra excepción se dio con un participante de 17 años, que mostró tener una idea de para que podrían llegar a necesitar los datos y preferencias estas plataformas: “No tengo idea, pero supongo que para crear un perfil tuyo y mandarte publicidad”.

Dentro de esta pregunta pudimos encontrar un cierto patrón: a medida que la edad va subiendo, el grado de conocimiento aumenta. El segundo rango etario entrevistado correspondiente a las edades que van de los 18 a los 25 años, mostró un mayor conocimiento de porque las plataformas se hacen de los datos y preferencias. Un alto porcentaje de los participantes respondieron que estos datos se vinculan y son necesarios para poder mandar publicidad dirigida a los perfiles de cada uno. “Los datos para enviarte información por mail por ejemplo, y preferencias para saber qué tipo de contenido traerte”. (Macarena, 25 años)

Un usuario adolescente dijo "Creo que necesitan de tus datos para mostrarte lo que te gusta y mantenerte constantemente interesado". (Josefina, 18 años). Más allá del desconocimiento y de la suposición sobre cómo avanzan las plataformas en relación a esta problemática, hay otros tipos de delitos cibernéticos que fueron detallados con anterioridad: Phishing, Spam, Suplantación de identidad y Cookies.

Es importante que tanto los más pequeños como los adultos tengan herramientas para que la delincuencia cibernética disminuya y para esto deben bajar la cantidad de datos exigidos por las plataformas. “Creo que los datos los utilizan por la información, podrían usarse para comportamiento del consumidor o para el marketing incluso, para poder llegar mejor a un target específico”. (Eugenia, 25 años)

Por otro lado, también se pudo delimitar cierto grado de conocimiento por parte de los participantes en cuanto a otros aspectos –no los principales, como los anteriores- de por qué se necesitan los datos de los usuarios. Las plataformas necesitan los datos para saber que el usuario es una persona real y no “un bot”, como afirma un participante de 21 años. A su vez, una entrevistada de 19 años asegura: “Los necesitan para saber que sos vos en realidad, una persona real y si no estás sacando datos de otra persona”. Es decir, que también los datos son requeridos, en cierto punto, para verificar la existencia de la persona física.

Otro de los aspectos importantes en los cuales se determinó que existe un cierto conocimiento es en cuanto a la generación de bases de datos por parte de las plataformas,

nutridas de los datos de los usuarios y se puede ver reflejada en esta respuesta: “Algunos datos asumo que los utilizan para poder almacenarlos en la base de datos y diferenciar a un usuario de otro”. Otros creen que las bases de datos son personalizadas y separadas por usuario: “No sé para que los necesitan, pero supongo que forman una base de datos tuya”.

Entrado en edades más avanzadas pudimos identificar casi en su totalidad el conocimiento por parte de estos ante la necesidad de las plataformas por los datos y preferencias. Se puede vislumbrar en esta respuesta de una chica de 29 años que además de necesitar los gustos de los usuarios y sus datos para generar publicidad dirigida, también existe un entendimiento sobre la venta de datos: “Para venderte cosas, pero también tengo la duda de que puedan vender esos datos”.

Además de afirmar que se necesitan los datos para publicidad o para que envíen contenido que vaya dirigido al *user*, una chica de 32 años asegura que se necesitan “por cuestiones de marketing, publicidad y propaganda política”. Podemos vincular esta respuesta directamente a lo sucedido años atrás con Facebook y Cambridge.

Otro aspecto que se pudo identificar es que ya en estas edades existe una cierta desconfianza de porque pueden llegar a necesitar tus datos y preferencias, tanto en la respuesta anterior como en esta: “Para ubicar publicidad dirigida o para hacerte algo raro, por eso no confío mucho”.

En los encuestados de edad de 26 años a 35, podemos encontrar términos importantes dentro de este estudio que participante más jóvenes no utilizaron, como cookies o algoritmos, términos propios de la virtualidad: “Por publicidad y por las cookies, para brindar un mejor servicio también. Por ejemplo cuando ves una película en Netflix, después la plataforma te ofrece películas del mismo estilo gracias a los algoritmos”.

Con respecto a los participantes más grandes del rango encuestado, se determinó que el 100% de los mismos están provistos de conocimiento sobre esta personalización que proponen las plataformas de sus usuarios. Remarcan que los gustos y preferencias son

utilizados directamente para cuestiones que tienen que ver con la publicidad. Asimismo los participantes también identificaron aspectos positivos de esta publicidad dirigida: “Entras a Google, Mercado Libre y ya saben que estás buscando o lo que quieres. Te ofrecen todo, pero a la larga te facilita la vida porque llegas a lugares que no hubieses llegado”.

Para poder dar una muestra del conocimiento sobre materia de datos de los participantes pertenecientes a este rango de edad, elegimos la respuesta de un entrevistado de 36 años que transmite una cierta profundidad: “Los datos los necesitan por un lado para que nos identifiquemos, y otros nos puedan identificar. Pero entiendo que principalmente son datos que utilizan luego para vender sus productos/publicidad, investigar acerca de patrones de consumo, comportamiento, etc.”

En relación a la desconfianza que brindan las plataformas y redes los usuarios comentaron que admiten estar inseguros generando una "paranoia" que es lógicamente alimentada por la sugestión de algunos otros usuarios en dónde aparecen dichos populares como que el celular o dispositivo "nos escucha". “Los datos y preferencias se utilizan continuamente. De hecho esta la paranoia de estar hablando sobre algo en tu casa y al rato te aparece alguna oferta justo de lo que estabas hablando, algo de eso hay”.

El rango más adulto de las entrevistas realizadas adhiere a lo que creen todos los entrevistados mayores. Estos participantes afirman que las redes de esta forma marcan una tendencia y así mismo es cómo funcionan los algoritmos, buscar algo en particular los lleva directamente a publicidades del mismo estilo o del mismo producto que se ha realizado en la búsqueda.

Cabe destacar que aún permanece la desconfianza sobre este tipo de plataformas debido a que se ha demostrado fehacientemente la venta de datos: “Pienso que ellos comercializan nuestros datos, por ejemplo Facebook, es una buena plataforma para estar conectado pero es muy dañina”.

“Por ejemplo por descarga o cuando un usuario abona el servicio Premium” (Joaquín, 17 años). Esta respuesta se relaciona con uno de los objetivos planteados en la investigación, se comprueba que cuantos más usuarios tenga la plataforma, la misma será propietaria de una mayor cantidad de datos que luego venderán a terceros, tal como figura en sus políticas de privacidad. “Cuanto más gente la use, más dinero tendrán” (Martina, 17 años)

Dentro de este rango etario se mostró un conocimiento parcial sobre cómo se reeditúan las redes, sin embargo, ninguno respondió con total certeza. La mayoría de las respuestas tuvieron que ver con las publicidades pero también con las descargas que se efectúan de estas aplicaciones, siendo estas solamente una parte de la obtención de dinero.

El segundo rango etario perteneciente a las edades de 18 a 25 mostró mayor precisión en cuanto a cómo se obtienen dinero las aplicaciones. La publicidad y la venta de espacios publicitarios por parte de las redes a usuarios que quieren tener visibilidad en sus emprendimientos o negocios sigue siendo la respuesta principal. Sin embargo, muchos de estos participantes afirmaron que si no es de esta forma, desconocen de qué manera lo hacen: “Creo que ganan plata con las propagandas pero si la gente no las paga realmente no sé cómo ganan dinero”.

La publicidad fue una de las respuestas que resonaba en la mayoría. Las aplicaciones siempre van a depender de la publicidad para obtener ganancias y esto se hace exitoso cuando recolectar más cantidad de datos para luego perfilar al usuario y ofrecer la publicidad que mayor compatibilidad tenga con el mismo. “Supongo que por publicidad, pero hay ciertas aplicaciones que uno no sabe cómo ganan” (Gianna, 24 años).

Una minoría de participantes añadió otro aspecto sobre esta materia, siendo este uno de los aspectos principales en este estudio: la venta de datos. Podemos afirmar entonces que una hay un conocimiento en materia a esta problemática, afirman que estos datos se venden a otros lugares –empresas- para poder seguir generando “consumismo”. “Proporcionando los datos que yo les doy, a partir de eso, sugiriendo a empresas que quieren hacer publicidad” (Valentina, 21 años).

Vinculado a la venta de datos se encuentra la constante generación de información – que se convierten en datos cuantificables gracias a herramientas como la Big Data- a través de la navegación del usuario dentro de la plataforma. Una participante asevera que generan dinero con las “mismas acciones que provee la plataforma” y que puede ser a través de los clics, *views*, conversiones y diferentes tipos de interacciones. Todo esto sumado a la venta de publicidad.

Otro de los aspectos que surgen dentro de las respuestas de estos jóvenes de entre 18 y 25 años y que está directamente asociada a una de las funciones principales de las aplicaciones que se pueden descargar gratuitamente, es la de suscribirse a las funciones Premium de algunas plataformas como Spotify, Tinder, Happn entre otras. Una participante de 25 años afirma que las plataformas se reditúan gracias a “la cantidad de suscriptores que tienen”.

La venta de espacio publicitario para personas que le compran a las plataformas es la respuesta con mayor popularidad dentro de las entrevistas realizadas. Se sigue confirmando el conocimiento parcial por parte de los participantes. Sin embargo una minoría también es consciente de que la venta de información existe. “Hacen bases de datos y después los venden a esos datos” (Alan, 32 años).

La interacción con la aplicación y la generación de información también se encuentra presente en este rango etario. Debemos diferenciar dos aspectos en relación a los datos. En primer lugar, los datos que brinda un usuario cuando genera la cuenta y en segundo, los datos que son generados cuando el usuario navega en la plataforma. Ambos tipos de datos son los que recolectan las aplicaciones. “Estimo que ganan dinero con las interacciones de las personas o usuarios que utilizan las plataformas” afirma una de las participantes de 28 años de edad.

Hay aplicaciones que cuentan con suscripciones, de esta manera los usuarios abonan el servicio de streaming para ver películas y series sin la intervención de publicidad. Esta es otra

de las formas en las que las plataformas obtienen ganancias. Es el caso de Spotify que tienen usuarios que abonan la suscripción para poder escuchar la música sin la aparición de avisos publicitarios.

Por otro lado, con respecto a las plataformas que brindan el servicio de delivery o de mensajería, los usuarios sólo consideran que las ganancias que obtienen son a través del pago del servicio. “Netflix y Disney Plus ganan dinero porque los usuarios la abonan. También por publicidad. Sin embargo Whatsapp no tengo entendido de que forma obtienen las ganancias”.

Entrando en los rangos de edades más avanzadas, el hecho de que las plataformas recaudan dinero a partir de venta de espacios publicitarios a marcas sigue siendo la respuesta fácil y popular por cada uno de los integrantes de las entrevistas realizadas.

Además de la publicidad, varios entrevistados aseguran que “no les sorprendería” que obtengan ingresos por la venta de datos de las personas. “Depende de la plataforma. Instagram gracias a la publicidad y me imagino que también deben vender los datos hacia otras compañías” (Sebastián, 37 años).

Los participantes más grandes se muestran decididos con respecto a la venta de datos. Además adhieren a que toda esa información que averiguan son vendidas a empresas que necesitan los datos para poder dirigir publicidad. En este sentido, la venta de datos puede darse tanto a empresas que destinan esos perfiles para fines comerciales, pero también con la finalidad de generar propaganda política:

“Usan tus datos para vender, comercializar, lo harán bajo cualquier aspecto, ya sea vendérselo a una empresa, un partido político, a cualquiera que le reditúe dinero” (Juan, 59 años).

Luego de recopilar y analizar toda esta información provista por los entrevistados, llegamos a un punto de inflexión dentro del cuestionario y dentro de esta investigación. Con el objetivo de identificar el grado de conocimiento por parte de los usuarios, se consultó sobre la finalidad de los datos y qué se imaginan que hacen las plataformas con la información de las personas que se registren.

El aspecto más abordado por parte de los entrevistados más jóvenes tiene que ver con que las redes necesitan los datos simplemente para registrarlos. Para estos participantes la finalidad de la recopilación de datos es la de archivarlos en ciertos lugares y además afirman “no creo que una red social los utilice para algo muy importante”.

Otro aspecto a destacar que expresaron los entrevistados de este rango etario tiene que ver con el objetivo de las redes de recabar los datos. Comentan que tiene que ver con poder identificar al usuario como una persona real y que no sea un “bot”. Sin embargo agregan que “los revisan y se los guardan”. Asimismo añaden, a base de suposiciones, que quedan en la base de datos –refiriéndose a Internet- y que quedan para todo el mundo.

Los participantes que utilizan plataformas de streaming o con el objetivo de ver videos –Youtube- afirman que “los guardan y verán ahí que hacen, además de revisar la información para mostrar videos que pueden llegar a gustarle a uno”.

Debemos remarcar también la no importancia que algunos le brindan a estas cuestiones. “No me lo puse a pensar, no tengo idea. Supongo que para que te conozcan por el nombre que tenes en las redes” (Lucas, 15 años).

Dentro del rango etario de 18 a 25 años, se pudieron identificar diversas respuestas. En su mayoría se manifestó un desconocimiento por parte de los entrevistados. En este sentido, también adhieren que no creen que hagan “cosas graves” con los datos, justificando que el fin de las redes pasa por el lado del consumo de productos y servicios, y que hacer cosas “indebidas” con los datos sería contraproducente para las plataformas. “No las conozco –las finalidades-, supongo que no hacen nada”.

En muchos casos se identificaron respuestas que tienen que ver con que la meta es “guardarlos para respaldarse en caso de tener algún inconveniente”, dejando en claro en un futuro -¿cercano?- puede llegar a haber un problema. Otras respuestas expresaron como una suposición que “la finalidad es llevarlos a publicidad”.

A su vez, otro aspecto abordado por un joven de 18 años tiene que ver con que el objetivo es simplemente “que sepan que es mi cuenta”, pero agrega que a pesar de que tengan control sobre sus datos personales, de esta forma le aseguran al usuario que no cualquiera entre a su cuenta o se creen perfiles falsos.

Sin embargo fue la minoría que distinguió que una de las finalidades de esos datos es para la venta, además agregaron que es por ese motivo que después aparecen publicidades en la navegación por distintos sitios: “Estimo que los recopilan en una base de datos, donde se aplican filtros y los venden”.

En estos términos, el rango etario de 26 a 35 años fue el que mayoritariamente identificó que una de las metas más importantes a la hora de recabar datos personales de usuarios es para la venta de los mismos.

El otro aspecto importante que abordaron estos entrevistados tiene que ver con la formación de una base de datos. Base de datos que luego es analizada gracias a la compilación de información diversa, ya sea edad, intereses, género, navegación, entre otras cosas. En este sentido, los participantes añadieron que gracias a este análisis y recopilación de datos, se perfila y se segmenta; “cuestiones estadísticas”. “Para mí esos datos son ingresados en una base de datos y con eso sacan estadísticas, preferencias. Hacer un estudio de mercado con la información que proporcionas”.

También se encontraron respuestas vinculadas a una mirada positiva de la recopilación de datos, amparada en que en las actualizaciones se expresa todo lo que se hacen con esos datos. Y agregan que no creen que sea riesgoso para los usuarios: “Así como el mismo estado tiene los datos de todos los ciudadanos, no considero peligroso el hecho de que las plataformas puedan tenerlos. Imagino que los utilizan para su propio beneficio como para el de los usuarios también ya que en reiteradas ocasiones mencionan en la actualización que es para brindar un mejor servicio”. (Martín, 26 años).

En cuanto al rango etario adulto, la mayoría tienen ciertas dudas de cuál es el objetivo o la finalidad de la recopilación de datos. Casi todos respondieron con base en suposiciones, algunos tomaron el camino de que la meta final es generar una base de datos, pero expresada con mayor profundidad, tocando y nombrando conceptos que son cruciales dentro de este estudio:

“No tengo en claro que hacen, pero asumo que arman una base de datos gracias a la inteligencia artificial avanzada que va adaptándose a tus necesidades. Antes las modas o tendencias se imponían desde otro lugar, ahora salen todas de las redes sociales”.

Diversos puntos de vista fueron mencionados dentro de las respuestas brindadas por este rango de edad, por un lado los entrevistados expresaron que “se imaginan” que los utilizan para ver la tendencia de usuarios y/o consumidores, a su vez también creen que los datos son vendidos a otras empresas que se valen de ellos para hacer negocios, demostrando así que los adultos están provistos de conocimiento sobre materia de venta de datos.

Otros manifestaron que no conocen la finalidad pero que creen que intentan saber que les gusta a las personas para poder ofrecerles productos que puedan llegar a consumir, siempre con una lógica que va en torno a la publicidad y el marketing: “Imagino que se venden a empresas, en vez de hacer un estudio de mercado directamente dicen: ‘mira, una persona de 18 a 33 años buscó esto y esto’. De esta forma se ahorran mucho dinero y tiempo en tener que hacer, por ejemplo, un *meeting* con gente y preguntar cosas para recabar información”.

Conclusión

A lo largo de esta investigación se pudo comprobar las hipótesis establecidas al comienzo mediante un trabajo exhaustivo.

La hipótesis principal "La aceptación de los términos y condiciones de las redes sociales aumenta la comercialización de los datos personales vulnerando el derecho a la privacidad" se pudo verificar de forma parcial ya que si bien la aceptación de los términos y condiciones aumenta la comercialización de los datos vulnerando la privacidad, las plataformas en sus políticas de privacidad proveen la información sobre cómo se utilizan dichos datos. Si bien existe una ley de protección, las plataformas se encargan de establecer cierto contrato con los usuarios exigiendo la aceptación.

María Julia Giorgelli, experta en el asunto afirma que: "No existe una norma en nuestro país que regule lo que son las plataformas. Lo que hay es un paradigma relacionado a lo que tiene que ver con la "autorregulación", cada plataforma establece sus términos y condiciones o políticas de uso de esos servicios, sean aplicaciones o plataformas. Frente a eso como usuarios del entorno digital, las opciones que tenemos es "subirnos y adherirnos" a ese contrato de adhesión". Y agrega: "La ley de datos de Argentina establece un criterio de consentimiento rígido, debe ser libre, expreso, informado y contar por escrito. Si uno accede a usar alguna plataforma, Twitter, Facebook, uno acepta términos y condiciones que suelen ser largos, pero uno no tiene grandes chances de cambiar o hacer algo a eso, es unirse o no unirse".

La creación de cuentas aumenta la violación al derecho de la privacidad por cláusulas impuestas por las plataformas. Si nos detenemos en el derecho de privacidad, las cláusulas informan sobre la utilización de datos tratando de obtener cierta transparencia pero las mismas dificultan ese proceso y es ahí en donde el usuario determina no leer las mismas ya sea por el complejo vocabulario legal, la extensión y la letra chica.

En relación a las hipótesis específicas que se desprenden de la hipótesis principal de esta investigación se puede comprobar fehacientemente que a mayor cantidad de usuarios nuevos que se asocian a la plataforma, más cantidad de datos para ser comercializados.

Se puede afirmar que los datos son vendidos a terceros, los cuales son entre ellos anunciantes que a posteriori utilizan el perfil mediante las preferencias eligiendo el que mejor se adapte a su mercado para así utilizar el espacio para publicitar. En el mundo del marketing esto colabora a encontrar al público más específico posible, por ejemplo.

Nocera afirma que existen riesgos y que a pesar de que la aplicación sea gratuita el usuario paga de forma indirecta agregando sus datos. "La pérdida de una supuesta privacidad o confidencialidad. En ningún momento vos estas en un ámbito privado cuando usas aplicaciones, subís una foto y cuando la subís es de la red social, no es más tuya. Si la subiste pertenece a ella. Son los riesgos de utilizar, el producto es gratis pero vos sos el que paga el producto".

A mayor desconocimiento en las redes sociales por parte de los usuarios, mayor es la frecuencia de extracción de los datos personales. Con respecto a esta hipótesis se evidenció que las plataformas extraen datos frecuentemente y esto no tiene que ver con un mayor o menor desconocimiento por parte de los usuarios, es decir, si el usuario desconoce o no los usos posteriores de sus datos igualmente aceptará las cláusulas que proponen tanto las redes sociales como las plataformas que utilice, tenga o no conocimiento

La plataforma no distingue las capacidades intelectuales de los usuarios que forman parte de la red, sino que extrae todos los datos de forma equitativa. "En general yo no sé si hay un desconocimiento absoluto, sigue habiendo pero se va acortando esa cantidad de personas en la población que desconoce absolutamente el uso de sus datos. Lo que está tomando más relevancia es la indiferencia, aun cuando conozco que posibilidades puede haber, igual se usa la aplicación o indiferencia a conocerlo" detalla Bárbara Peñaloza.

En cuanto a los datos más valiosos e importantes a la hora de perfilar a un usuario, se pudo comprobar que no solamente la edad, la geolocalización y los intereses son los datos de mayor valor, sino que la actividad del usuario dentro de la plataforma, sean *likes*, *retweets*, tiempo dentro de la plataforma, también cuentan a la hora de formar perfiles de usuarios para luego intercambiar intereses con empresas a las que venderán estos datos.

En este estudio nos propusimos a indagar cuales son los principales factores que llevan a un usuario a aceptar términos y condiciones que proponen estas plataformas, se pudo determinar que uno de los principales factores es la inmediatez que requieren los usuarios hoy por hoy, otro factor es el de la necesidad de pertenecer si o si al mundo virtual, caso contrario “quedas fuera”. En estos términos, la valoración que le dan los usuarios a su propia seguridad en las redes queda supeditado al conocimiento que posean sobre los riesgos que existen una vez dentro del ecosistema, quienes posean mayor conocimiento tomarán medidas más apropiadas para su seguridad, quienes desconozcan –o sean indiferentes- harán vida normal, sin tomar las medidas ya manifestadas en el estudio.

Por otro lado, cabe destacar que los términos y condiciones que desarrollan las plataformas en sus páginas oficiales se establece como un contrato cuando el *user* inicia la creación de su cuenta y para finalizar el proceso debe aceptar el documento que impone cada ecosistema virtual. "Los términos y condiciones son un documento que lo que hace es definir los derechos y obligaciones que van a existir entre las partes. Una vez que se empieza a utilizar la aplicación o el servicio que se brinde. En la práctica los términos y condiciones no son tan vinculantes como uno creería porque puede haber cláusulas *leoninas* (impuesta por una de las partes sin darte la posibilidad de negarte al aceptar esa cláusula) o que pueden llegar a ser nulas". concluye Daniel Monastersky.

Bibliografía general:

ANDERSON, Chris. La economía long tail, de los mercados de masas al triunfo de lo minoritario. Barcelona: Ediciones Urano. ISBN 10: 8493464260 Pág.27 a 40 y 73 a 79.

CARR, Nicholas. Atrapados: cómo las máquinas se apoderan de nuestras vidas. –1ra ed. – Buenos Aires: Taurus, 2015 Pág 83 a 106 ISBN 978-987-737-002-7

CASTELLS, Manuel. La Era de la Información. Vol 3. “Fin de Milenio”. Mexico, 1998. Siglo XXI.

FERNÁNDEZ, José Luis. Plataformas mediáticas: elementos de análisis y diseño de nuevas experiencias, 1ra ed. Buenos Aires: Crujía, 2018 ISBN 978-987-4168-10-8 Pág. 7 a 24.

MOROZOV, Evgeny. La locura del solucionismo tecnológico: Los peligros de la mediación algorítmica. España, 2015. Traducido por Nancy Viviana Piñeiro. Editorial Capital Intelectual. ISBN 978-841-5917-199

PARISER, Eli. El filtro burbuja: Como la web decide lo que leemos y lo que pensamos. 1ra ed - España. Penguin Random House Grupo Editorial, 2017. España.

PARKER, Geoffrey; VAN ALSTYNE, Marshall; CHOUDARY, Sangeet Paul. Platform revolution : How networked markets are transforming the economy and how to make them work for you. Nueva York: WW Norton Company : 2016 ISBN 978-0-393-35435-5 Pág. 229 a 260

SRNICEK, Nick. Capitalismo de plataformas. 1ed – Buenos Aires: Caja Negra, 2018 ISBN 978-987- 1622-68-9 Pág. 39 a 87

TIROLE, Jean. La economía del bien común. 1ra ed. Buenos Aires: Taurus. 2017. Pág 405 a 459 ISBN 978-84-306-1861-3

VAN DIJCK, José, La cultura de la conectividad: una historia crítica de las redes sociales. Ira ed. Buenos Aires: Siglo XXI Editores, 2016. Pág. 17 a 46 ISBN 978-987-629-652-6

Papers citados

Blanca Delgado (2018). “*Términos y condiciones de uso en Internet: La normativa es inútil sin la autorregulación del usuario*”. Facultad de Comunicación, Universidad de Sevilla. España.

Javier Puyol Moreno (2014). “Una aproximación a Big Data”. Revista de Derecho UNED, núm 14. Madrid, España.

Nicolas Oxman (2013). “Estafas informáticas a través de Internet: Acerca de la imputación penal del “Phishing” y el “Pharming”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XLI, Chile. (pp. 211-262)

Yasmina Soto. (2017). “*Datos masivos con privacidad y no contra privacidad*”. Revista de Bioética y Derecho. Barcelona, España.

Páginas web

Amazon. (12 de febrero de 2021). Aviso de privacidad de Amazon. <https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ#:~:text=Utilizamos%20informaci%C3%B3n%20personal%20para%20prevenir,y%20gestionar%20los%20riesgos%20crediticios>.

BBC News Mundo. (24 de julio de 2019). *Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios.* <https://www.bbc.com/mundo/noticias-49093124>

Circulaciones. (20 de febrero de 2020). *Argentina digital.* <https://www.circulaciones.com/argentina-digital-2020/#:~:text=Entre%20abril%20de%202019%20y,129%25%20de%20la%20poblaci%C3%B3n%20total>

Facebook. (11 de enero de 2021). *Política de datos.* <https://es-la.facebook.com/policy.php>

Google. (4 de febrero de 2021). *Política de privacidad de Google.* <https://policies.google.com/privacy?hl=es#infocollect>

Instagram (11 de enero de 2021). *Política de datos de Instagram.* <https://es-la.facebook.com/help/instagram/155833707900388>

Netflix (1 de enero de 2021). *Declaración de privacidad.* <https://help.netflix.com/legal/privacy>

TikTok. (Julio de 2020). *Política de privacidad.* <https://www.tiktok.com/legal/privacy-policy?lang=es>

Twitter. (18 de junio de 2020). *Política de Privacidad de Twitter.* https://cdn.cms-twdigitalassets.com/content/dam/legal-twitter/site-assets/privacy-june-18th-2020/Twitter_Privacy_Policy_ES.pdf

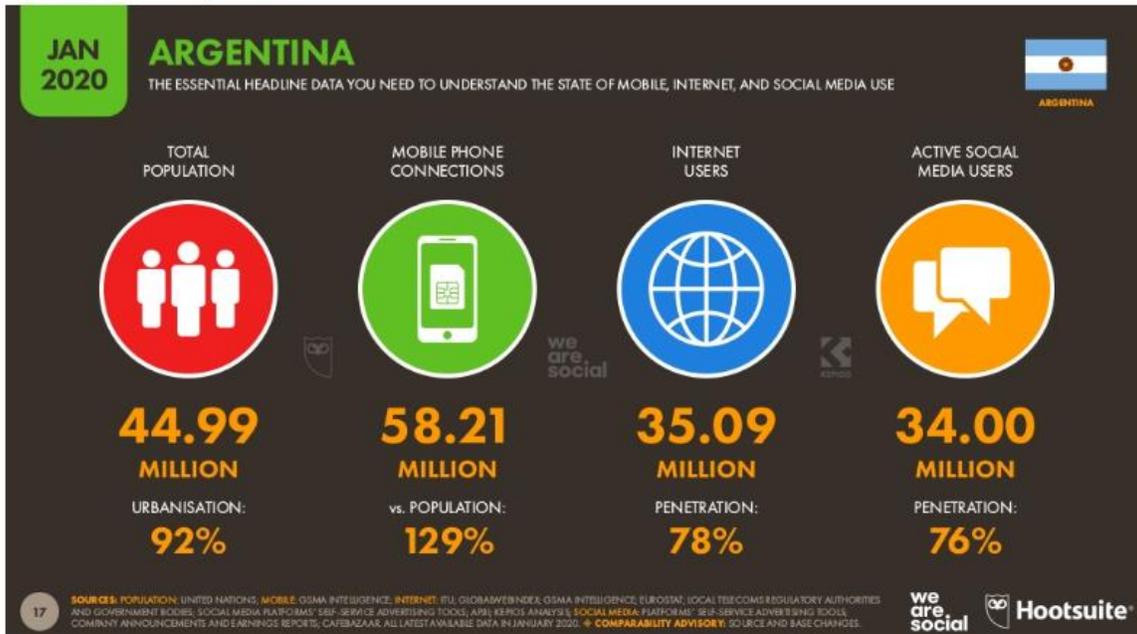
Visual Capitalist. (18 de abril de 2020). *Visualizing the length of the fine print, for 14 popular Apps.* <https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>

WhatsApp. (4 de enero de 2021). *Políticas de privacidad de WhatsApp.* <https://www.whatsapp.com/legal/updates/privacy-policy/?lang=es>

Anexo:

Argentina Digital 2020

Posted on 20 febrero, 2020



Ain't Nobody Got Time for That

The average reading speed of most adults is 200 to 250 words per minute (wpm). College students, probably because they are very studious and not skimming, move that pace up to around 300 words per minute. For the sake of this analysis, we calculated reading times based on 240 wpm.

App/Service	Word Count	How many minutes to read? (240 wpm)
Microsoft	15,260	63.5
Spotify	8,600	35.8
Niantic (Pokemon Go)	8,466	35.2
TikTok	7,459	31.4
Apple (Media Services)	7,314	30.5
Zoom	6,891	28.7
Tinder	6,215	25.9
Slack	5,782	24.1
Uber	5,658	23.6
Twitter	5,633	23.5

Showing 1 to 10 of 21 entries

◀ Previous [Next](#) ▶

Encuesta elaborada para usuarios o personas de 14 a 65 años:

1. ¿Cuáles son las plataformas que mayormente utilizaa?
2. ¿Para qué las utilizas?
3. ¿Tomas algún recaudo a la hora de poner tus datos personales?
4. ¿Qué aspectos te hacen confiar en una plataforma? ¿Por qué?
5. ¿Por qué quieres formar parte del mundo virtual?
6. ¿Por qué crees que necesitan tus datos personales y preferencias?
7. ¿Cómo crees que ganan dinero las plataformas?
8. ¿Conoces el destino final o la finalidad? ¿Qué te imaginas que hacen con los datos?
9. Cuando aceptas los términos y condiciones/ servicios ¿lees todas las cláusulas? ¿Te parece importante leerlas?

Encuesta elaborada para profesionales del ámbito cibernético:

1. ¿Cuando un usuario acepta términos y condiciones de una app esta al mismo tiempo corriendo riesgos? ¿Por qué?
2. ¿Qué riesgos en concreto corre el usuario al entregar sus datos personales?

3. ¿Cuáles son los casos más comunes o los que toman más relevancia en Argentina?
¿Qué usos posteriores le dan a esos datos concretamente, las empresas que los compran?
4. ¿Por qué crees que a pesar de estas consecuencias y manipulación en el uso de los datos personales la gente se involucra igual?
5. ¿El desconocimiento por parte de los usuarios es un factor importante? ¿Por qué?
6. ¿Qué valoración crees que hacen los usuarios de su privacidad? Depende de la edad?
7. ¿Qué valores promover para que sea menos riesgosa la navegación? Sobre todo para los más pequeños, que ahora los niños de 12 13 años ya tienen todo tipo de redes.
8. ¿Cómo hacer para que el derecho no se convierta en un obstáculo para el desarrollo tecnológico, pero que a su vez, pueda regularlo de forma válida?
9. ¿Hay que fortalecer los mecanismos que ya existen? ¿De qué forma podrían fortalecerse?
10. ¿Cómo crees que hacen para evitar a la ley estas plataformas?
11. ¿La Big data puede ser contraproducente ya que cualquier actividad nuestra está siendo grabada o recopilada?
12. ¿Consideras que se viola el derecho a la privacidad? ¿Por qué?