Universidad de San Andrés

Departamento de Ciencias Sociales

Licenciatura en Comunicación

Cambridge Analytica y su Impacto en las Políticas de Privacidad

Alumno: Timoteo Prezzavento

Legajo: 26163

Mentora: Carolina Aguerre

Buenos Aires, Argentina

Índice:

Introducción:

En la actualidad, la actitud de los usuarios en las distintas redes sociales o aplicaciones disponibles en los celulares inteligentes es completamente ingenua y cándida. La forma en la cual las personas vuelcan su información privada, desde nombre, edad, sexo o preferencia política hasta el lugar en donde se ubican en ese momento, muestra un desinterés enorme de las posibles amenazas que les pueden llegar a suceder. Y el listado de las probables consecuencias de esta apatía hacia la información que uno retrata, es cada vez más larga debido a la facilidad con la que uno puede llegar a manipular los datos de otra persona.

A medida que pasa el tiempo, surgen cada vez más plataformas que nos facilitan las distintas tareas que llevamos en nuestra rutina diaria. Por ejemplo, nos dicen cuánta distancia recorrimos, cuántas calorías quemamos, cómo va a estar el clima el día de hoy, nos indican cómo llegar a un determinado lugar o nos permiten pedir la cena de esta noche sin la necesidad de movernos de nuestras casas. La diversidad de estas aplicaciones es gigantesca, al igual que el tiempo que pasamos dentro de ellas.

Ahora bien, para que su uso sea el más cómodo y eficiente, muchas de estas aplicaciones, nos exigen determinados datos personales, con el fin de que la experiencia dentro de la ella sea más fluida. Muchas veces solamente requieren información que nosotros consideramos básica. Por ejemplo, nombre y apellido, edad, número de teléfono, sexo o correo electrónico. Todo lo necesario para que la aplicación nos formule un usuario con una determinada contraseña que usaremos cada vez que entremos a ella para usarla.

Todo este proceso es sumamente genérico a la hora de pensar en cómo nos relacionamos con estas herramientas. Es una acción que ya tenemos asumida y que realizamos sin pensarlo dos veces, debido a que la necesidad de usar la aplicación es mayor que la de poner nuestros datos personales en un servidor que se encuentra en alguna parte del mundo que desconocemos. Y en el que, además, asumimos que se van a quedar en ese determinado lugar y que no van a ser manipulados en un futuro con un fin desconocido.

Pero muchas veces no sólo es esta la información que recopilan las aplicaciones por parte de sus usuarios. La información que desprendemos con los movimientos que llevamos a cabo dentro de las plataformas también son de una gran importancia. Por ejemplo, en el caso de la aplicación que nos ofrece un servicio en el cual podemos pedir un auto que nos lleve a un determinado lugar, el lugar de dónde nos ubicamos, hacia qué lugar vamos, a qué hora realizamos el pedido del servicio, cómo lo abonamos o hasta el recorrido que llevamos a cabo, es recolectado por la aplicación.

Muchas de estas plataformas que describimos tienen algo en común y es que son gratis. No hay necesidad de comprarlas para que sean usadas. Esto nos hace preguntarnos a nosotros mismos cómo hacen para mantenerse en un entorno en donde la competitividad y el surgimiento de nuevas aplicaciones es sumamente fuerte. Con nuestros movimientos dentro de ellas, con los rastros que dejamos, con el tiempo que pasamos dentro de ellas. Y estas plataformas tienen distintas herramientas para lograr esto. Las redes sociales, por ejemplo, logran esto a través de las distintas formas de interacciones que nos ofrecen. Dándole “like” a una publicación o “retuiteando” algo que te pareció interesante. A medida que mayor atención o tiempo pasamos dentro de ella, más movimientos o acciones realizamos, y más información recolectan. El fin de las aplicaciones es, y más que nada en las redes sociales, captar nuestra atención. Constantemente están encontrando nuevas formas en la cual sus usuarios puedan pasar la mayor cantidad de tiempo. Axel Marazzi, en su nota en Revista Anfibia llamada “Cinco Horas Diarias Mirando el Teléfono”, realiza una pequeña explicación de una de las formas en la cual las redes sociales modifican nuestros procesos cognitivos con el fin de pasar más tiempo dentro de ellas. Cuando algún contenido nuestro tiene una respuesta por parte de nuestros seguidores o amigos, un “like” o “retuit”, esto hace que una parte de nuestro cerebro desprenda dopamina, un neurotransmisor que esencialmente motiva al ser humano. Esa necesidad de estar constantemente viendo nuestras notificaciones para ver cuantas interacciones tuvo nuestra publicación se llama “recompensas variables intermitentes”.

Esta actitud inocente hacia las plataformas sociales, en donde depositamos nuestra vida y momentos personales, permitió la atentación hacia

la privacidad y datos personales más grande de los últimos años. En un caso donde más de 50 millones de personas fueron afectadas por el funcionamiento de distintas aplicaciones que, con el objetivo de minar la información de diferentes usuarios, posteriormente fueron utilizados como elementos que facilitaron el accionar de la publicidad dentro de Facebook.

Mediante tus intereses, es decir likes o el contenido de tus publicaciones en conjunto con tus datos personales, Cambridge Analytica era capaz de entender tu personalidad, armar un perfil, clasificarte dentro de un determinado grupo y de esa manera redirigirte hacia determinada publicidad política o simplemente sugerirte que accedas a cierta noticia. Un proceso que también se conoce como "microtargeting". Tom Agan, en su trabajo llamado "Silent Marketing: Microtargeting", describe al proceso como la creación de un mensaje específico y enunciado de determinada forma teniendo conocimiento de ante mano de que el mensaje va hacia una persona o grupo de personas específico. Con este conocimiento previo, es decir hacia qué persona va dirigido, se puede saber que el impacto del mensaje va a ser satisfactorio. El autor también lo define como una "segmentación psicográfica precisa que utiliza un algoritmo patentado para determinar una combinación de rasgos demográficos y actitudinales para asignar individuos a cada segmento específico" (Agan, 2007). Una práctica preocupante debido a que nos encontramos en un contexto donde existen teóricos que sostiene que las redes sociales son el lugar perfecto para formar posiciones cada vez más críticas, ciegas a posturas diferentes a las suyas o radicalizadas, debido a la constante exposición de contenido que uno puede llegar a sufrir dentro de las distintas redes sociales. Robin Thompson sostiene que las redes sociales son una herramienta sumamente efectiva para radicalizar y reclutar miembros para distintas causas (Thompson, 2011). Sostiene que la forma en la cual logran sumar adeptos es porque les prometen "amistad, aceptación e incluso un sentido de propósito". También hay que tener en cuenta que estas plataformas son el lugar perfecto para la distribución de noticias con contenido inexacto o falso, en donde la ausencia de un sujeto que verifique esta información permite la viralización de noticias de este tipo, sumándose como otro factor que ayuda a la manipulación de la orientación política del usuario.

A lo largo de este trabajo nos enfocaremos en describir los distintos elementos que entraron en cuestión en el momento en donde las declaraciones de Christopher Wylie se hicieron públicas. Tomando como eje principal la siguiente pregunta: ¿Hasta qué punto el escándalo entre Facebook y Cambridge Analytica incidió en los cambios de las políticas de privacidad de distintas plataformas sociales?, tendremos distintos objetivos. El primero será describir a Cambridge Analytica y su relacionamiento con Facebook y las personas que fueron involucradas para poder contextualizar las dimensiones de la situación. Luego, hablaremos sobre el concepto de auto regulación y cómo esta idea predomina en el ecosistema en donde pertenece Facebook. El tercer objetivo será hacer una distinción y a su vez describir lo que conocemos como privacidad y datos personales, elementos que usualmente la gente vincula en una misma idea, pero que no en todos los casos suelen ser lo mismo. Y por último, estudiaremos cómo el caso de Cambridge Analytica afectó a las políticas de privacidad y seguridad de las plataformas y redes sociales más populares dentro de Internet.

Hay muchos motivos que fundamenta el análisis de los acontecimientos entre Cambridge Analytica y Facebook. Primeramente, trajo nuevamente a la discusión el rol de estas plataformas con respecto a nuestra privacidad, y a su vez, la capacidad de influencia que tienen sobre sus usuarios. En segundo lugar, fomentó la discusión sobre la auto regulación, mecanismo que adoptan las plataformas generalmente y que a su vez no son fácilmente regulables por parte de los estados de las distintas jurisdicciones donde operan. Este accionar no sólo es ilegal, sino escandaloso por parte de los actores involucrados trajo como consecuencia una fuerte reacomodación interna de las políticas a otras plataformas sociales, como por ejemplo Twitter o Instagram. Nuestra idea es analizar hasta qué punto estas plataformas se vieron obligadas a cambiarse o modificarse, tomando en consideración la privacidad y datos personales de sus usuarios.

Cambridge Analytica: el escándalo con impacto en los procesos electorales

El rol de Christopher Wylie fue fundamental para que el accionar de Cambridge Analytica sea de conocimiento público. En el año 2017, junto con Wylie y otro denunciante, The Guardian y The Observer llevaron a cabo un proceso de un año analizando distintos documentos y entrevistando a determinadas personas con el fin de comprender el funcionamiento de esta entidad y su influencia en el proceso político conocido como Brexit y con las elecciones de los Estados Unidos del 2016. Documentos e información que en la actualidad se encuentran siendo utilizados tanto en la Corte Suprema de los Estados Unidos como también en la Comisión Electoral y la Oficina del Comisionado de Información, ambos pertenecientes al Reino Unido.

La persona que formaba el rol fundamental dentro de Cambridge Analytica se llama Alexander Nix. Previo a su fundación, Nix dirigía SCL Elections. Una rama de SCL Group, una empresa que proveía, como bien dice la descripción en su página oficial, “data, análisis y estrategias para gobiernos y organizaciones militares en todo el mundo”. Wylie, por otra parte, previo a formar parte de Cambridge Analytica, había trabajado para el partido liberal del país en el que nació, Canadá. En el año 2013, luego de haber estudiado derecho en “London School of Economics”, Wylie se encuentra con un “paper” realizado en el centro de psicometría de la Universidad de Cambridge en el cual describía la correlación entre las personalidades de las personas y sus orientaciones políticas. El trabajo se llama “Los juicios de personalidad basados en computadora son más precisos que los hechos por humanos”, realizado por Wu Youyou, Michal Kosinski y David Stillwell. Luego de leerlo, Wylie piensa en el partido liberal y termina realizando una presentación frente a los dirigentes describiendo cómo estos factores son centrales para los partidos políticos a la hora de buscar futuros votantes o penetrar en determinado grupo social o económico. El partido no le dio importancia a la presentación, pero sí un político dentro del partido le presentó a Alexander Nix, que se interesó sobre el contenido de la presentación de Wylie y le ofreció que trabaje dentro de SCL Elections con el fin de aplicar los conocimientos y estrategias que se presentaban en el “paper” de la Universidad de Cambridge.

Este grupo, SCL Group, y específicamente su rama que apuntaba a las elecciones, utilizaba lo que Wylie describe como “operaciones psicológicas” en el cual, mediante la persuasión y la dominación de información, cambiaban las posiciones políticas de las personas. Y las técnicas que utilizaban tienen nombres que hoy en día se utilizan a menudo cuando se habla de los medios masivos de información: la desinformación y la circulación de “fake news” o noticias falsas.

Ahora bien, Cambridge Analytica se formó a partir de SCL Group. Encabezado por Wylie, la idea era que esta parte de la empresa se direccione hacia las elecciones, utilizando las herramientas disponibles por parte de SCL y el conocimiento de Wylie. La forma en la cual Cambridge Analytica termina relacionándose con el partido republicano de los Estados Unidos es a través de Steve Bannon, el director y editor de Breitbart, un sitio de noticias que contienen principalmente información orientada a gente de extrema derecha y que a su vez se hizo conocido por la publicación de teorías conspirativas y la viralización de noticias falsas. En ese momento, Bannon encabezaba la campaña electoral del candidato republicano de las elecciones del 2016, Donald Trump. Luego de la victoria de Trump, ocupó el rol de asesor principal de las decisiones presidenciales que se llevaban a cabo hasta agosto del 2017 en donde el presidente le pidió su renuncia. Según las investigaciones de The Guardian, previo a su participación en la campaña electoral de los Estados Unidos, Steve Bannon había ayudado a un político amigo llamado Nigel Farage que lideraba la opinión pública a favor de la separación del Reino Unido y la Unión Europea, más conocido como el Brexit. Wylie describe en unas de las tantas notas que realiza en conjunto con The Guardian, que la relación entre él y Bannon era sumamente fluida, debido a sus mutuos intereses, principalmente la relación entre la cultura y la política, y como estos dos elementos se relacionan entre sí.

Pero lo central de nuestra investigación es describir cómo Cambridge Analytica logró alcanzar y luego utilizar los datos de más de 50 millones de usuarios de Facebook. Para que Wylie pueda llevar a cabo sus ideas y lo que aparentemente Bannon le exigía, él necesitaba datos y en gran cantidad. Una de las formas en la cual uno puede conseguir semejante cantidad de información es comprándola. Dentro de los gastos realizados por Cambridge Analytica que

presentó Wylie a The Guardian, aparece una compra hacia una empresa llamada “Global Science Research”, liderada por Aleksander Kogan. Kogan había desarrollado una aplicación llamada “thisismydigitallife”, en donde mediante respuesta a determinadas preguntas pretendía adivinar una personalidad o forma de ser. Como cualquier aplicación común que hoy en día uno se puede descargar desde cualquier dispositivo, te exigía que le permitas a la aplicación acceder a tu cuenta de Facebook para poder crear así tu cuenta y posteriormente llevar a cabo la determinada prueba. Algo que uno acepta sin detenerse demasiado tiempo en las descripciones o leer las especificaciones sobre el permiso que le estamos dando a la aplicación. Pero, a diferencia del resto, aceptando el permiso de la aplicación, no solo accedía a tus datos personales que contenía tu perfil Facebook, sino que también a los datos personales de los usuarios que uno tenía como amigos. Esto le permitió a Kogan acceder a información de millones de personas en cuestiones de semanas. Wylie confiesa que Facebook se tendría que haber dado cuenta sobre los movimientos que Kogan estaba realizando con la información de las personas, debido al tráfico que estaba generando mediante el proceso de extracción de los datos personales. Pero, aparentemente, una vez que los protocolos de seguridad de la plataforma alarmaron sobre la situación, Facebook se contactó con Kogan, el cual justificó las acciones diciendo que lo que estaba realizando tenía motivos académicos.

Cuando esto se hizo publicó, podríamos decir que desenmascaró dos problemas institucionales de gran relevancia para Facebook. El primero estuvo relacionado con la distribución masiva de noticias falsas por parte de Cambridge Analytica, que llevan a las personas a la desinformación, en donde aparentemente también estuvo involucrado el gobierno de Rusia. Según las investigaciones realizadas, gran parte de los portales o páginas que se encontraban dentro de la plataforma que publicaban de forma masiva noticias con contenido inexacto, estaban financiadas por empresas rusas con vínculos con el gobierno de ese país. Y, por otro lado, problemas estructurales que se relacionan con la privacidad y la seguridad de la plataforma y la información de sus usuarios. Acá es donde entra en juego el accionar por parte de Cambridge Analytica, Christopher Wylie y Alexander Kogan.

En un principio, Facebook defendió la posición de que lo sucedido fue una manipulación a la plataforma. Que ellos en ningún momento facilitaron la extracción de la información a Cambridge Analytica. Una de las tantas soluciones por parte de Facebook al escándalo fue denegar el acceso a las aplicaciones a la información de los usuarios de la plataforma, recién en agosto de este año. Las aplicaciones, para poder tener acceso a dicha información, debían pasar por un proceso de revisión. Si tu aplicación cumplía con los requisitos, te daban este acceso.

A comienzos de este año, la revista “Wired” le hizo una entrevista a Mark Zuckerberg en donde le preguntan qué tipo de regulación le aplicaría a su plataforma teniendo en cuenta que debería proteger a sus usuarios y la sociedad en general. Zuckerberg desvía la respuesta de la pregunta describiéndole al autor sobre un uso específico que le dan a la inteligencia artificial dentro de la red social. Le describe que, mediante el uso de este tipo de inteligencia, es la forma en la cual Facebook controla el contenido que se publica dentro de ella. Y que complementa esta herramienta con el empleo de aproximadamente quince mil personas que también se dedican a la seguridad dentro de la red social. Zuckerberg luego se enfoca sobre el tema de la pregunta inicial en donde agrega que, en realidad, cualquier aparato regulatorio debería enfocarse sobre este último elemento. Incluso sugiere como las entidades regulatorias deberían funcionar a la hora de enfocarse sobre las empresas tecnológicas, que es mediante la creación de un lineamiento o determinados puntos que deberían seguir, en vez de que se les exija que cumplan “procesos específicos”. Hay una clara razón por la cual él responde esto y es debido a que, si estos entes regulatorios le obligan a funcionar de determinada manera, estas empresas deberían cambiar por completo sus estructuras tanto funcionales como económicas. Más adelante describiremos cómo se verían afectadas estas estructuras.

Las consecuencias para Facebook fueron manifestadas a través de distintas vías. Una de ellas fue la sanción por parte de la Comisión Federal de Comercio de los Estados Unidos en la cual establecía una multa de $40.000 dólares por cada usuario que se vio afectado. Además, lanzaron una investigación sobre las prácticas que realizaba la plataforma con los datos. En el

año 2011, Facebook estableció un consenso con la Comisión Federal de Comercio en el cual se sostenía que la plataforma estaba obligada a defender, entre otras cosas, la confidencialidad y privacidad de sus usuarios. Y que, si decidía compartir la información, debía tener el consenso de los usuarios. Luego de que la situación con Cambridge Analytica llegó a la agenda pública de los medios masivos, la comisión se vio obligado a revisar si Facebook violó el consenso que habían establecido. Una de las primeras consecuencias es el pago de la multa que recién mencionamos. El portal Vox, en abril de este año, publicó una nota en el cual detalla todas las formas en la que el aparato gubernamental de Estados Unidos puede regular a Facebook y a su vez a todas las redes sociales que tienen en su poder la información de millones de personas. Una de ellas es a través de un acta llamada "Publicidad Honesta". Impulsada por senadores de ambos partidos en octubre del 2017, se propone esta ley "para mejorar la transparencia y la responsabilidad de los anuncios políticos online", pero la ley nunca logró avanzar. Incluso la Comisión Federal de Comercio propuso dos regulaciones en donde el objetivo es "promulgar una regla que en su texto e interpretación reconozca la importancia primordial de proporcionar al público la más clara revelación del pagador o patrocinador de estas comunicaciones públicas en Internet."[1]

Por parte del lado europeo, la Unión Europea el 25 de mayo estableció una ley llamada Reglamento General de Protección de Datos. Este proyecto tiene distintos puntos, por ejemplo le exige a cualquier empresa o entidad, como por ejemplo una universidad, que a la hora de utilizar la información de cualquier ciudadano europeo se lo tiene que notificar. También, los individuos ahora tienen el derecho de tener acceso a esta información y pueden hacer con ella lo que quieren. Es decir, la pueden modificar o hasta eliminarla. El objetivo de este proyecto es claro, hacer que este tipo de procesos sean más transparente hacia los usuarios y además establecer consecuencias hacia las organizaciones que las incumplen. En su presidencia, Obama también intento avanzar una ley que tenía objetivos similares llamada Declaración de Derechos de Privacidad del Consumidor. Se contemplaba la misma idea de que la persona podía controlar

[1] Federal Election Comission, (26 de marzo, 2018). Proposed Rules, Vol. 83, N. 58. http://sers.fec.gov/fosers/showpdf.htm?docid=373521.

sus datos, pero lamentablemente no logró obtener mayoría dos veces. A diferencia de Estados Unidos, podemos encontrar una posición más agresiva por parte de la Unión Europea que establece claramente lo que se tiene que hacer a la hora de tratar con la información de sus ciudadanos y además delimitando el accionar de la contraparte.

Las sanciones gubernamentales no fueron las únicas consecuencias que sufrió Facebook. Sus acciones cayeron precipitosamente un 18% días después de que sea de conocimiento público sus vínculos con Cambridge Analytica. Pero dos meses después, luego de testificar ante el congreso y pedir disculpas públicamente, las acciones volvieron a su valor anterior. Por otro lado, un movimiento a través de la etiqueta "#DeleteFacebook" logró tomar tracción luego de los eventos, en donde insistía a los usuarios de la plataforma a que eliminen su cuenta como respuesta al accionar de Facebook. Incluso un exdirectivo de la red social y cofundador de WhatsApp, Brian Acton, publicó un tuit[2] en donde les sugería a sus seguidores que era la hora de borrar las cuentas de Facebook.

[2] Acton, B. (20 de marzo, 2018). Publicación en Twitter, https://twitter.com/brianacton/status/976231995846963201

Auto Regulación:

Como bien describimos anteriormente, existen casos en donde los estados o entidades gubernamentales se ven obligados a intervenir sobre determinado campo con el fin de beneficiar o proteger a los ciudadanos que pertenecen dentro de dichos países. Describimos procesos regulatorios como el de Estados Unidos o la Unión Europea que utilizaron diferentes herramientas a su disposición con el fin de regular Facebook, y el resto de las redes sociales, luego del escándalo de Cambridge Analytica con el fin de evitar que se repita una situación de tal escala.

Pero no es mediante la presión externa la única forma en la cual estas plataformas se ven obligadas en cambiar elementos dentro de estructura con el fin de cambiar su funcionamiento. Existen muchas situaciones en la cual, por motivos internos, que estas empresas por decisión propia modifican sus estructuras internas para alcanzar distintos objetivos.

Tomemos el caso de Facebook. Luego de que su relacionamiento con Cambridge Analytica llegara a los portales más importantes, también realizó modificaciones en su plataforma con el fin de mejorar su imagen y que sus usuarios no migren hacia otro lado. A principios de abril del 2018, desde su cuenta personal, Mark Zuckerberg realizó una publicación que detalla dos grandes cambios. El primero es en la rama de las publicidades que uno puede realizar dentro de Facebook. Una de las acusaciones que se le hacía a la plataforma era el libre acceso a organizaciones rusas a comprar pauta publicitaria a artículos o información falsa apuntada específicamente a determinado sector de la sociedad de Estados Unidos con el fin de influir en su voto, lo que se denomina “microtargeting”. Ahora, si una persona pretende publicitar a través de Facebook, deber tener su cuenta verificada y a su vez confirmar su identidad y locación. El segundo elemento que se describe también está enfocado para solucionar el problema mencionado anteriormente. Los usuarios que tienen una gran cantidad de páginas en su poder, ahora se les exige una verificación. A través de esto, Facebook pretende disminuir la cantidad de usuarios con procedencia dudosa que se dedican a viralizar noticias falsas. Como bien podemos ver, ambos cambios se enfocan en revertir lo que Christopher Wylie había declarado ante los medios. Una posición similar sostuvo

Zuckerberg cuando declaró frente a la comisión judicial y de comercio del Senado de Estados Unidos. Sostuvo que Facebook en ese momento estaba llevando a cabo un proceso de revisión a todas las aplicaciones que utilizaron o manipularon una gran cantidad de información en el pasado. Y, además, ahora solamente se les comparte tres elementos de toda tu información a los desarrolladores de dichas aplicaciones: tu nombre, tu correo electrónico y tu imagen de perfil.

Este tipo de acciones, en donde una entidad cambia por voluntad propia su funcionamiento o estructura, se enmarca dentro de los mecanismos de auto regulación. En estos procesos se contempla la idea de que no es necesario que alguna organización, gobierno o entidad regulatoria les exija determinados funcionamientos, estructuras u objetivos debido a que pueden cambiar en función a estos elementos por voluntad propia. Gunningham y Rees, en su texto "Auto Regulación: Una Perspectiva Institucional", definen al concepto como un "proceso regulatorio mediante el cual una organización a nivel industrial (…) establece reglas y estándares relacionados con la conducta de las empresas en la industria" (Gunningham y Rees, p. 364). Como bien mencionamos anteriormente, en la entrevista que le hace Wired a Zuckerberg días después del conocimiento público del robo masivo de información de sus usuarios, el fundador de la red social sugiere que no es necesario que exista una presión externa por parte de organizamos externos que le obliguen a funcionar de determinada manera. Zuckerberg sostiene que estableciendo un lineamiento determinado es suficiente. Ahora bien, ¿cómo debería ser el contenido de dichos lineamientos? ¿A quién deberían beneficiar, a la sociedad o a la empresa en cuestión? ¿La aplicación de este método evitaría situaciones como las de Cambridge Analytica?

El caso de Estados Unidos y su intento de regular este ecosistema es un claro de ejemplo de falta de conocimiento a la hora de quererle aplicar reglas. Una falta de conocimiento que se refleja como incertidumbre sobre cómo confrontarlos. Las razones de esto pueden ser varias, entre ellas presiones o "lobby" por parte de las compañías que se pueden ver afectadas por dichas regulaciones. Lo que trae como consecuencia esta auto regulación por parte de las plataformas. Pero es una regulación consciente de que, si los caminos que

toman no son los correctos, la cantidad o el flujo de sus usuarios pueden ser afectados (cómo lo ejemplifica el movimiento #DeleteFacebook). Pareciese que este camino autónomo es el que más confianza transmite debido a que refleja una imagen más responsable y a la misma vez le da una oportunidad de ser más flexible con los cambios que la regulación estatal. Gunningham y Rees sostienen que existe una "resistencia de las empresas multinacionales que operan en un mercado cada vez más global, y no es de extrañar por qué, tanto política como económicamente, la regulación gubernamental directa se ha vuelto menos atractiva en los últimos años". (Gunningham y Rees, p. 364)

Cuando se habla de la intervención del aparato estatal dentro de lo que vendría a ser internet, muchas veces se usa como argumento en contra, la posible atentación hacia lo que conocemos como libertad de expresión. Se sostiene que internet es el lugar en donde uno puede encontrar una gran pluralidad de voces debido a los múltiples canales o plataformas en el cual uno puede reflejar su discurso o posición sobre algún determinado tema. El concepto de auto regulación nunca atentaría en contra de este derecho de la libertad de expresión ya que cualquier cambio realizado por la plataforma o red social es tomado por una entidad privada y no por un estado que tiene que garantizar este derecho y además tomar decisiones que más benefician a la sociedad. A su vez, si estas plataformas esperasen a que los gobiernos avancen con sus políticas, nunca pudiesen evolucionar e innovar de forma tan rápida, algo característico de ellos. Como sostiene el artículo de Forbes[3] sobre la auto regulación, generalmente los políticos apuntan a aplicar "políticas globales que cubren toda una industria y establecen los requisitos de cumplimiento más amplios, independientemente de cuán posible sea cumplirlos". Otro argumento que utiliza el autor es que cuando se aplican leyes de determinado tipo, lo realizan considerando el presente, pero nunca teniendo en cuenta el largo plazo.

Por otro lado, si tomamos en consideración lo sucedido con Cambridge Analytica, podríamos sostener que hay un aumento en la desconfianza por parte

[3] Bansal, J. (9 de julio, 2018) The Self-Regulation Window Is Closing for Tech Companies, *Forbes*, https://www.forbes.com/sites/forbestechcouncil/2018/07/09/the-self-regulation-window-is-closing-for-tech-companies/#32accd263ba5

de los usuarios hacia las plataformas debido a la posible manipulación de sus datos. O por lo menos, como retrata la encuesta realizada por Reuters e IPSOS[4], un poco menos de la mitad de los norteamericanos encuestados creen que Facebook obedece las leyes de privacidad establecidas por sus gobiernos. Mientras que una encuesta realizada por una organización alemana llamada Bild am Sonntag, sostiene que el 60% de los alemanes que participaron temen que las plataformas como Facebook afecten negativamente la democracia.

Podemos encontrar otro ejemplo de esta forma de actitud por parte de Facebook en la publicación realizada en su "Newsroom" en marzo de este año[5]. Firmada por el jefe de privacidad, Erin Egan, se describen distintos ajustes a su interfaz. Uno de ellos es la posibilidad de acceder a los ajustes de tus datos de forma más fácil, en donde uno puede acceder a las configuraciones desde un lugar. El segundo elemento que modificaron fue el menú relacionado a su privacidad. "Los nuevos atajos de privacidad son un menú donde puedes controlar tus datos en solo unos pocos toques, con explicaciones claras de cómo funcionan nuestros controles". A partir de este cambio, uno puede modificar el nivel de seguridad de su cuenta, controlar su información personal y hasta decidir cuantos anuncios puedes ver en la página de inicio. Por último, también facilitaron la eliminación de tus datos en la plataforma, dándote la posibilidad de incluso descargarla. La razón por la cual nos detenemos en esta publicación es debido al discurso que optaron las personas en cuestión. Volviendo a lo que mencionamos anteriormente, la auto regulación es una forma para que las empresas puedan renovar su imagen hacia sus usuarios, convenciéndolos de que continúen utilizando su plataforma. A lo largo de la publicación, se utilizan distintas frases que transmiten esta idea. Una de ellas es la siguiente: "También es nuestra responsabilidad decirle cómo recopilamos y usamos sus datos en un leguaje detallado, pero también fácil de entender".

Ahora bien, Facebook en realidad es una empresa de publicidad, vende nuestra atención. El 98% de su margen del año 2017 vino de la publicidad que

[4] Ingram D. and Auchard, E. (25 de marzo, 2018) Americans less likely to trust Facebook than rivals on personal data, *Reuters,* https://www.reuters.com/article/us-facebook-cambridge-analytica-apology/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-idUSKBN1H10AF

[5] Egan, E. and Beringer, A. (28 de marzo, 2018) It's Time to Make Our Privacy Tools Easier to Find, *Facebook Newsroom*, https://newsroom.fb.com/news/2018/03/privacy-shortcuts/.

vende dentro de ella. El valor de mercado de Facebook en abril de 2018 es de medio trillón de dólares.

La forma en la cual funciona este mecanismo central dentro de la red social es la siguiente. Nosotros, por decisión propia proveemos de información a Facebook: dónde trabajamos y nos educamos, lugares donde hemos vivido o nos encontramos actualmente, información básica sobre nosotros, familiares y relaciones personales, detalles sobre nosotros, eventos importantes en nuestras vidas. Eso es solo lo que se encuentra en nuestro perfil. Facebook, además, junta toda lo que clickeamos, posteamos o comentamos, y a través de esta información presume o infiere quién es el usuario, como por ejemplo tu orientación política o estado familiar. Luego de formular tu perfil en base a la recolección de estos datos, determinadas publicidades aparecen cuándo se ingresa a la red social.

Uno al crear una página dentro de Facebook puede hacer que las publicaciones de estas páginas lleguen a un público más grande pagando una determinada cantidad de dinero. Unas de las herramientas que ofrece el servicio de publicidad de esta red social es la elección de una audiencia determinada. Según tus intereses, como explicamos en el párrafo anterior, y al público que se apunta, se puede determinar a qué personas llegarán las publicaciones como publicidad en base a su información[6].

Esto crea una máquina de publicidad sumamente efectiva ya que les facilita a las páginas impactar de forma directa a partir de los atributos de los usuarios, haciendo que el mensaje les llegue a las personas que muy probablemente tengan una determinada interacción con la publicación. Dentro de estos atributos podemos encontrar subsecciones relacionados con lo demográfico, con sus intereses y hasta con las conductas que reflejan. Según el público al cual nosotros pretendemos apuntar, podemos seleccionar determinados atributos para que la audiencia sea aún más limitada.

[6] Por ejemplo, tenemos una determinada página que vende teléfonos importados. Entonces, a través de esta herramienta de la elección de audiencia, podemos hacer que nuestra página les aparezca a usuarios que tengan como “likes” páginas de marcas de teléfonos o que recientemente hayan visitado perfiles relacionados a la tecnología. Además, podemos limitar que nuestra publicidad solamente impacte a usuarios que vivan en determinado país, provincia, o incluso en un radio de un kilómetro.

La razón por la cual nos detenemos a analizar y describir esta parte de la plataforma es debido al artículo que realizó Vox en relación con el modelo de negocio de Facebook y este concepto de la auto regulación. En plena tormenta para la red social en donde todos los sitios de noticias hablaban sobre ella, Vox le realiza una entrevista a una experta en leyes sobre empresas tecnológicas y aplicación antimonopolio llamada Sally Hubbard[7]. Una de las declaraciones que realiza es sobre el modelo económico de la red social. Ella sostiene que el modelo de Facebook es completamente basado sobre la ganancia que realizan a través de la publicidad, y que es por eso por lo que la idea de la protección de la información del usuario va en contra de este modelo. Ellos precisan de esta información para poder seguir aplicando el modelo, es la razón por la cual la gente invierte en publicitar ahí, debido a la capacidad y efectividad de hacerle llegar tu mensaje a quien quieras. El periodista luego le pregunta si los usuarios y la sociedad puede confiar en que Facebook puede auto regularizarse a lo que Hubbard responde que no. Esto es debido a que si realmente quisieran enfocarse en proteger la información de sus usuarios deberían cambiar por completo como es su estructura económica ya que "depende del acceso y distribución de datos personales privados".

El tema de su modelo de negocios incluso fue mencionado en uno de los días en el cual congreso de los Estados Unidos llamó a Mark Zuckerberg a declarar. Anna Eshoo, que representa uno de los distritos dentro del estado de California, le preguntó si él estaba dispuesto a cambiar el modelo de negocio de la plataforma con el "interés de proteger los derechos de privacidad de los individuos." En la misma sesión, Jan Schakowsky, otra representante dentro del congreso, le remarca todas las disculpas públicas que realizó él en nombre de la plataforma, comenzando en la que realizó en el año 2003 ante Harvard. Schakowsky termina sosteniendo que la auto regulación, por parte de las plataformas sociales, "simplemente no funciona".

Nuestro objetivo de investigación no es discutir la eficacidad de este tipo de posición, sino describirlo como una forma en la cual las compañías se

[7] Illing, S. (18 de julio, 2018) Why "fake news" is an antitrust problem, *Vox*, https://www.vox.com/technology/2017/9/22/16330008/eu-fines-google-amazon-monopoly-antitrust-regulation

posicionan contemplando a sus usuarios. Encontramos que es una herramienta que les permite a las empresas establecer algún mecanismo de rendición de cuentas y de transparencia, aunque no siempre reflejen exactamente cómo lo hacen. Como bien sostiene la nota de Forbes sobre esta situación entre la auto regulación y los movimientos que realizó Facebook ante el escándalo: “Cuándo se trata de generar confianza entre los usuarios y el público en general, la gente necesita saber que los motivos de la compañía están en línea con sus valores personales”.

Privacidad vs. Datos Personales:

A la hora de hablar sobre estos dos conceptos, muy probablemente encontremos puntos que los relacionan entre sí. La razón por la cual sostenemos está posición es debido a que dentro de nuestra privacidad se contemplan nuestros datos personales o también que nuestros datos personales pertenecen a nuestra privacidad. Pero a pesar de este relacionamiento, existen distintos elementos que distinguen a un concepto del otro.

Nissenbaum sostiene una definición de la idea de datos personales a partir de una directiva de la Unión Europea: "datos personales significa cualquier información relacionada con una persona física identificada o identificable…" (Nissenbaum, p. 4). Pero a pesar de que este concepto tenga una definición en particular, el autor encuentra que existe una gran ambigüedad a la hora de definirlo debido a la contextualización que se le da. Dependiendo en donde se esté aplicando la idea, su definición se va a alternando. En relación con la privacidad, Nissenbaum encuentra que los teóricos se confunden a la hora de querer definirla debido a la ausencia de la distinción entre la concepción neutral del concepto y la concepción normativa. La concepción neutral contempla la idea de que la privacidad debe gran valor y que además merece tener protección legal. Por otra parte, la concepción normativa describe a la privacidad como un elemento valorable y que definitivamente merece ser protegida. Más adelante trata de definir a la privacidad y lo hace apoyándose en Ruth Gavinson: "la privacidad es una condición que es medida en términos del grado de acceso que otros tienen para usted a través de la información, la atención y la proximidad." (Nissenbaum, p. 70). Al igual que el concepto de datos personales, dependiendo en donde se contextualiza la idea de privacidad, su significado también se altera. Por ejemplo, en el ámbito legal, la privacidad se lo define como "la reclamación de individuos, grupos o instituciones para determinar por sí mismos cuando, como y hasta qué punto la información sobre ellos se comunica con los demás." (Nissenbaum, p. 71).

La IAPP, que sus siglas en español significan Asociación Internacional de Profesionales de Privacidad, categorizan los distintos tipos de datos personales bajo la idea de que se pueden dividir a partir de si se relacionan con su vida

privada, profesional o pública[8]. Las categorías son seis: datos internos, externos, históricos, financieros, sociales y de rastreo. La primera categoría contempla información que uno tiene para uno mismo y que no la refleja a primera vista. Es decir, información sobre el conocimiento de la persona y sus creencias, intereses y preferencias personales e información utilizada para autenticar al individuo con algo que ellos saben. La segunda categoría abarca más información superficial como por ejemplo su etnicidad, sexualidad, identitarios o características físicas. La tercera categoría simplemente es sobre la información sobre la historia personal del individuo. La categoría financiera contiene información sobre las transacciones, créditos, propiedades y cuentas de la persona en cuestión. La quinta categoría, la social, describe datos que reflejamos en la comunidad o sociedad en donde nos encontramos. Por ejemplo, información sobre la familia en la cual vivimos o la relación, el estatus social al que pertenecemos, educación que recibimos o carrera profesional y hasta antecedentes penales. Por último, la categoría de rastreo abarca información sobre los dispositivos electrónicos que utilizamos, información que nos permite contactarnos con nosotros y la información sobre el lugar en donde nos encontramos o vivimos.

En consecuencia de la comparación que realizamos nos vemos obligados a retratar un último concepto que entrelaza a los dos anteriores, el de la protección de datos. Según la IAPP, se describe como el manejo de dicha información personal. Que a su vez su definición se modifica según el contexto, como por ejemplo si se habla de seguridad se define como la implementación de distintos medios que protegen a los datos de posibles modificaciones, divulgaciones, usurpaciones o destrucciones no autorizadas.

Retomando la discusión del comienzo, en el caso de Cambridge Analytica lo que se manipuló fueron distintos tipos de datos según las categorías de la IAPP. La razón por la cual sucedió esto es debido al tipo de información que uno puede plasmar dentro de su perfil de Facebook. Son cuatro los tipos de categorías: datos internos, externos, sociales y de rastreo. A pesar de esto, Facebook no le obliga a sus usuarios que completen todos estos tipos de datos.

[8] International Association of Privacy Policy, *Categories of Personal Information*, https://iapp.org/media/pdf/resource_center/Categories-of-personal-information.pdf

El accionar que llevó a cabo esta entidad tiene un término específico que es la violación de datos personales. El parlamente europeo en el año 1996 lanzó un artículo llamado “Artículo 29” en el cual, junto a representantes de la comisión y supervisores europeos de la protección de datos, establecieron distintos puntos sobre la protección de datos. Dentro de este documento se define a la idea de violación de datos personales como “una violación en la seguridad que conlleva a la destrucción, alteración, pérdida, divulgación no autorizada o acceso no autorizado o accidental de los datos personales transmitidos, almacenados o procesados de otra manera”[9]. Este artículo actualmente forma parte de una ley previamente mencionada, el Reglamento General de Protección de Datos de la Unión Europea. A su vez, otra entidad europea también sostiene una posición similar. La Agencia de la Unión Europea para los Derechos Fundamentales sostiene un artículo en el cual se discute sobre la protección de datos personales. En su carta de derechos fundamentales, el artículo 8 presenta tres puntos sobre este derecho, de los cuales solo describiremos a los dos primeros. El primero sostiene que toda persona perteneciente a la Unión Europea tiene derecho a la protección de los datos personales que le conciernen. El segundo punto describe que si estos datos llegan a ser usados con algún fin, primero tiene que haber consentimiento por a la persona en cuestión o por alguna ley. Además, defiende la idea de que todos tienen el derecho de acceso a sus datos y derecho a que se rectifique.

En contraste, por Estados Unidos no existe lo que se conoce como “el derecho a la protección de datos” como bien describimos anteriormente con la Unión Europea. “Estados Unidos utiliza un enfoque sectorial de la privacidad que se basa en una combinación de legislación, regulación y autor regulación, y carece de un marco integral de datos personales como el proporcionado por la directiva de la Unión Europea” (Esteve, p. 37). Esteve, en el artículo, enumera las distintas regulaciones, protecciones constitucionales o tratados que regulan la privacidad en dicho país. Pero a pesar de esto encuentra que “el marco legislativo estadounidense sobre privacidad y datos personales es más complejo y difícil de entender…” (Esteve, p. 41). El autor incluso menciona una entidad

[9] European Union (1996), Article 29: Data Protection Working Party, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

que nosotros ya trajimos a la discusión, la Comisión Federal de Comercio. El autor describe en su publicación que entre todos los roles que lleva a cabo esta comisión en relación con la privacidad, una de ellas es exigirles a las distintas compañías que si llevaron a cabo una modificación en sus políticas de privacidad, están obligados a notificar a los usuarios que llevaron a cabo estos tipos de cambios. Esto lo notamos cuando la aplicación o plataforma nos notifica sobre cambios en sus términos y condiciones.

Uno de los puntos que destacamos de las entidades regulatorias europeas era la posibilidad que le daban a los usuarios poder acceder y controlar sus datos personales. Por ejemplo, esto se establecía a través del Reglamento General de Protección de Datos o también a través de los artículos 12 y 14 de la Directiva de la Unión Europea[10]. Ahora bien, en Estados Unidos no existen regulaciones que contemplen esta idea que mencionamos. Si algún usuario exige estos tipos de derechos, nuevamente entra en cuestión la Comisión Federal de Comercio ya que es la encargada de regular las plataformas sociales en cuestión.

No es el eje central de nuestra discusión denotar cómo las distintas entidades legales abordan esta temática sobre la privacidad y nuestros datos que se encuentran depositados en estas plataformas. Pero es de gran importancia este caso que se llevó a cabo a partir de las revelaciones realizadas por Edward Snowden en el año 2013. Dentro de la denuncia de Snowden, se sostenía que el servicio de inteligencia del Reino Unido, también conocido como el GCHQ, estaba "secretamente interceptando, procesando y almacenando datos de millones de personas a partir de comunicaciones privadas", como bien describe el artículo de The Guardian[11]. La razón por la cual nos tomamos el tiempo en este caso es con relación a como la Corte Europea de los Derechos Humanos falló en contra de este organismo gubernamental, sosteniendo que los métodos utilizados por el GCHQ violaron la privacidad de las personas

[10] Data Protection Commission, Chapter 2: General Rules on The Lawfulness of the Procession of Personal Data, *EU Directive*, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm

[11] Bowcott, O. (12 de septiembre, 2018). GCHQ data collection regime violated human rights, court rules, *The Guardian*, https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules

afectadas. Es importante destacar que acciones legales son posibles en contra de las personas y organizaciones que atentan contra estos derechos.

En la actualidad existe una gran discusión sobre cómo la privacidad atraviesa de distintas maneras sobre el individuo. Graham Greenleaf expuso en el año 2017 un análisis sobre las leyes de privacidad de 120 países y como cada país abarcaba las distintas temáticas. Dentro de la investigación, se encuentran unos cuadros donde se señala el país, organización internacional a la que pertenece, el año en el cual salió la ley, el año de la última enmienda y si el proyecto contempla el sector público, el privado o ambos. La razón por la cual traemos en discusión a este autor y su trabajo es para ejemplificar uno de los aspectos donde la privacidad afecta al individuo, en este caso las democracias. Es decir, en los países más democráticos es donde más se encuentran proyectos legales que contemplan y protegen la privacidad, mientras que en los países con gobiernos más autoritarios sucede lo contrario. Por ejemplo, tomando en cuenta los países de esta última característica como Corea del Norte o China, naciones que según el índice realizado por The Economist[12] no se encuentran dentro del análisis de Greenleaf debido a la ausencia de proyectos con el fin de proteger la privacidad de sus ciudadanos. Del otro lado, Australia tienen un proyecto relacionado a esta temática desde 1988 que contempla tanto el sector privado como el sector público y forma parte de dos acuerdos internacionales. Otro ejemplo similar es Canadá que tiene dos leyes distintas, una que contempla el sector público y otro el sector privado, ambos desde el año 1983. Al igual que el ejemplo anterior también forma parte de acuerdos internacionales, en este caso tres.

[12] The Economist, *The Economist Intelligence Unit's Democracy Index*. https://infographics.economist.com/2018/DemocracyIndex

Cambios en las Políticas de Privacidad:

En esta última sección de nuestra investigación abordaremos los tres puntos que describimos hasta el momento, Cambridge Analytica, auto regulación y privacidad versus datos personales, y cómo al mismo tiempo se entrelazan para poder abordar el último punto en cuestión: los cambios en las políticas de privacidad.

En un primer paso, definiremos qué son las políticas de privacidad. Podríamos considerarlo como un documento que describe cómo determinada organización hace público las acciones qué realiza con la información de los involucrados en dicha organización. Utilizando como ejemplo la organización central en nuestra investigación, las políticas de privacidad describen que realiza Facebook con la información de sus usuarios. Estas acciones que lleva a cabo pueden variar dependiendo que dicen las políticas, desde guardarlas, manipularlas o hasta modificarlas. Pero al mismo tiempo, deben describir detalladamente que es lo que realizan. Al igual que cuando realizan estos cambios en su estructuración por voluntad propia, elemento que describimos anteriormente como auto regulación. Lo que detallan a través de las políticas de privacidad es una gran oportunidad para las organizaciones para mostrar transparencia y seguridad hacia las personas que les pertenece.

Al mismo tiempo, este argumento de que esta acción es para crear una buena imagen de la organización no es el único por la cual existe las políticas de privacidad. Las organizaciones además tienen que respetar determinadas reglas establecidas por las entidades legales, como por ejemplo las que establecen el Reglamento General de Protección de Datos o la Comisión Federal del Comercio.

A continuación analizaremos el impacto que tuvo lo sucedido con Cambridge Analytica en las redes sociales más usadas o con más usuarios. Según el artículo del Foro Económico Mundial[13] la plataforma más popular es, obviamente, Facebook. De 149 países censados, toma el primer puesto en 119.

[13] Hutt. R. (20 de marzo, 2017). The world's most popular social networks, mapped, *World Economic Forum*, https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/.

La red social que le sigue es Instagram, siendo la segunda preferencia para los usuarios de 37 países (que además es de Facebook). Mientras tanto, Twitter es la segunda preferencia en Estados Unidos y gran parte de la Unión Europea, y Reddit la segunda preferencia en países como Australia, Canadá o Dinamarca.

El artículo del Foro Económico Mundial utiliza como fuente una página llamada Vincos que, basándose en páginas que miden el tráfico dentro de internet, realiza un mapa con las redes sociales más usadas en todo el mundo. Como expresamos anteriormente, Facebook logra ser la que mayor tráfico genera. Pero este primer puesto se diferencia en dos países: Rusia y China. El país ruso tiene dos plataformas principales en la que se concentran gran parte de sus usuarios, VKontakte y Odnoklassniki. Mientras que en el país asiático, la mayoría de sus ciudadanos utilizan Qzone. Es importante destacar que en China, Facebook se encuentra completamente bloqueado desde el año 2009. Existen varias razones por la cual uno no puede ingresar a la plataforma. Una de ellas es debido a que, según el gobierno chino, Facebook no cumple las regulaciones y leyes establecidas por el gobierno. Esas declaraciones fueron realizadas en el año 2014, mientras que la plataforma está bloqueada, como mencionamos arriba, desde el 2009, el mismo año en el cual se realizaron protestas en una región del país que fueron organizadas a través de Facebook. [14]

Continuando con la enumeración de las redes sociales más populares, Vincos da una lista de 14 plataformas[15]. De esta lista tomaremos las siguientes: Facebook, Youtube, Twitter, Qzone, Snapchat y VKontakte. Gran parte de ellas son plataformas que fueron creadas en Estados Unidos, como Facebook, Twitter, Youtube o Snapchat. Mientras que el resto de las que consideraremos fueron fundadas en otros países. La razón por la cual optamos por plataformas con un origen distinto que el de la mayoría es debido a que pretendemos analizar hasta qué punto este escándalo influyo en otras. Es decir, debido a que gran parte de sus usuarios no forman parte de los Estados Unidos o Europa, donde más consecuencias trajo el conflicto con Cambridge Analytica, estas redes

[14] Kan, M. (30 de octubre, 2014). China: Facebook not banned, but must follow rules, *PC World*, https://www.pcworld.com/article/2841252/china-facebook-not-banned-but-must-follow-the-rules.html

[15] Vincos Blog. (5 de febrero, 2018). El mapa de las redes sociales en el mundo 2018, *Vincos*, http://vincos.it/2018/02/05/la-mappa-dei-social-network-nel-mondo-gennaio-2018

sociales no se vieron obligadas a tener que cambiar sus políticas de privacidad. Al mismo tiempo, si esta hipótesis no se logra comprobar, también consideramos relevante estudiar qué tipos de mecanismos o cambios realizaron Qzone y VKontakte y por cuales motivos. Otra similitud para considerar es que todas son plataformas sociales. En todos los casos es necesario crearte un usuario para poder ingresar o registrarte. Uno debe depositar dentro de ella información personal para poder así comenzar a utilizarlo. A su vez, en todas las plataformas uno puede conectarse con otras personas, comunicarse con ellas y hasta incluso publicar contenido de distintas formas, cada una de forma particular o a través de distintos formatos.

Los cambios realizados por Facebook ya los mencionamos en los capítulos anteriores. Uno de sus cambios centrales, realizado el 4 de abril, fue la forma en la cual las personas adquirían publicidad dentro de la plataforma, una de las críticas centrales que se le hizo dentro del caso de Cambridge Analytica en relación con la capacidad de publicitar contenido inexacto o "fake news". Tener la cuenta verificada, confirmación de identidad y locación son los nuevos requisitos fundamentales que te exige Facebook si uno pretende publicitar dentro de ella. El segundo cambio que realizaron fue la posibilidad de eliminar con mayor facilidad la información que uno tienen en su perfil. Y el tercer cambio fue una modificación en el menú de privacidad que tiene la plataforma, haciéndolo más sencillo y fácil de comprender. Todos estos cambios realizados, fueron anunciados a través de la misma plataforma. El acceso de las aplicaciones dentro de Facebook a la información de los usuarios también fue atacado por los cambios en las políticas de privacidad, que a su vez también fue otra de las críticas centrales del escándalo. A través de un posteo en Facebook[16], el jefe de tecnología llamado Mike Schroepfer, describe los cambios realizados en relación con el funcionamiento de las aplicaciones dentro de la red social. Distingue distintos puntos sobre estas modificaciones que resume diciendo: "Ya no permitiremos que las aplicaciones soliciten acceso a información personal (…), estado y detalles de las relaciones, lista de amigos, historial de educación y trabajo...". A su vez, también eliminarán la información que tenga una aplicación

[16] Schroepfer, M. (4 de abril, 2018). An Update on Our Plans to Restric Data Access on Facebook, *Facebook Newsroom,* https://newsroom.fb.com/news/2018/04/restricting-data-access

sobre el usuario una vez que se hayan cumplido tres meses de inactividad. Es decir, si una aplicación tiene información sobre un usuario y si ese usuario no usa la aplicación en tres meses, ya no tendrá disponible esa información. Otro cambio que realizaron, anunciado el 28 de marzo, fue el cierre de las "Partner Categories"[17], relacionado a la publicidad dentro de Facebook. Lo que esta herramienta permite es que "los proveedores de datos de terceros, ofrecer su orientación directamente en Facebook". Facilitaba la refinación de las categorías de las personas a quien uno puede apuntar su publicidad, ya que complementaba la información que tenía el usuario dentro de la plataforma con la información que proveían estos terceros, como por ejemplo información demográfica. Por último se encuentra una iniciativa llevada a cabo por Facebook mismo en relación con el impacto que la plataforma misma tiene sobre las elecciones que transcurren en países. Anunciado también a través de una publicación de Facebook[18], lo que sostiene este proyecto es la idea de "ayuda a proporcionar una investigación independiente y creíble sobre el papel de las redes sociales en las elecciones, así como la democracia en general". A través de distintas organizaciones orientadas a los procesos democráticos y sus mejoras, como por ejemplo el "Democracy Fund", Facebook trabajará en conjunto con ellas y proveerles información sobre el accionar de las redes sociales y su utilización durante los periodos electorales.

La segunda plataforma que abordaremos será Twitter. Al igual que Facebook, esta red social también tuvo acusaciones de distintas partes en relación con el uso inapropiado de la misma en distintos aspectos. En las mismas elecciones presidenciales en la que Facebook se vio involucrado, las del año 2016 en Estados Unidos, a Twitter se lo acusó de influenciar de la misma forma. Se lo culpó de no llevar a cabo acciones suficientes en contra de cuentas falsas que se encargaban en difundir información falsa o cerrar cuentas que lo único que hacían era llevar a cabo distintos discursos de odios, entre otros.[19] Incluso

[17] Facebook. (28 de marzo, 2018). Shutting Down Partner Categories, *Facebook Newsroom*, https://newsroom.fb.com/news/h/shutting-down-partner-categories/

[18] Schrage, E. (9 de abril, 2018). Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections, *Facebook Newsroom*, https://newsroom.fb.com/news/2018/04/new-elections-initiative/.

[19] Kimer, J. (21 de marzo, 2018). Big Tech is Failing the Self-Regulation Test, *Corporate Foreign Policy*, https://corporateforeignpolicy.com/big-tech-is-failing-the-self-regulation-test-23674f93a590

el mismo Twitter realizó una publicación que analizaba la participación e influencia que tuvo la plataforma en las elecciones, en la que sostiene que aproximadamente cincuenta mil cuentas fueron creadas con el fin de difundir contenido inexacto sobre la elección. [20]

Retomando nuestro eje de análisis, Twitter a su vez también realizó distintos cambios en sus políticas de privacidad. La publicación que introduce los dichos cambios comienza sosteniendo "...que siempre se debe saber qué datos recopilamos de usted y cómo los usamos, y que debe tener un control significativo para ambos". [21] Más adelante, se denotan los cuatro puntos centrales de las modificaciones que se aplicaron a partir del 25 de mayo. El primero es sobre la posibilidad de controlar de forma más sencilla tu información personal dentro de la plataforma, mejorando las distintas herramientas que logran esto. Los siguientes puntos se enfocan en una misma idea, la forma en la que ellos manipulan tus datos. El segundo punto sostiene que se van a enfocar más en como ellos comparten su información al público o a las aplicaciones que requieren tu información. El tercer punto habla de mayor transparencia y control de la relación que llevan a cabo ellos, es decir Twitter, con terceros que utilizan tu información para la implementación de publicidad. Por último, la plataforma social sostiene que van a hacer todo lo que puedan para poder cumplir las distintas reglas que se le exige con el fin de prever posibles consecuencias negativas hacia sus usuarios, tratando de hacer de Twitter un lugar seguro y para el interés general de su público. Como podemos ver, gran parte de sus cambios están orientados hacia lo que vendrían a ser los datos que tienen ellos de sus usuarios y dejar en claro que hacen ellos con esta información. Y al mismo tiempo, le da la posibilidad de poder controlar aún más y con más detalle los datos que uno deposita en él. Dentro de estas posibilidades se encuentra poder decidir el nivel de seguridad de tu cuenta, las aplicaciones que pueden acceder a ella o incluso preferencias en relación con que tipo y que cantidad de publicidad el usuario quiere ver en su "timeline".

[20] Twitter, (Mayo, 2018). Updated to our Terms of Service and Privacy Policy. https://help.twitter.com/en/rules-and-policies/update-privacy-policy
[21] Twitter, Privacy Policy, https://twitter.com/en/privacy#update

Snapchat será nuestra tercera plataforma. Conocida por la idea de que el contenido que uno publica o comparte directamente con otro usuario se borra en el lapso de un día o al enviarla. Esto no significa que la plataforma en sí no recolecte cierto tipo de información a pesar de que su contenido sea efímero. En una entrevista realizada al medio inglés Daily Mail, el fundador de Snapchat Evan Spiegel sostiene que a diferencia de Facebook, su plataforma no está hecha para que los mensajes privados de sus usuarios y al mismo tiempo no muestran públicamente una línea de tiempo de todo lo que el usuario publicó.[22] Sus cambios en las políticas de privacidad reflejan de cierta manera las declaraciones de su dueño. Antes de comenzar a analizar dichos cambios, es importante destacar la forma en la cual la sección de políticas de privacidad está reflejada en la página de la plataforma. Sin la necesidad de tener que cambiar o redireccionarte a otra página, Snapchat presenta lo que ellos llaman "Centro de Privacidad". Dentro de aquí la plataforma te da la posibilidad de acceder a distintas secciones, como por ejemplo sus políticas de privacidad, sus principios de privacidad, la privacidad del servicio que ofrecen e inclusive una sección nombrada "Cómo Usamos tu Privacidad". Esto que acabamos de describir es uno de los cambios que realizó en sí Snapchat, la posibilidad de que el usuario pueda acceder de forma más sencilla a este tipo de información.

Uno de los principales cambios que realizó Snapchat, cercana a la fecha del 25 de mayo, es la de poder acceder de forma más sencilla a las configuraciones personales de tu usuario con la idea de modificar o borrar tu información dentro de ella. Dándote la posibilidad de incluso descargar que tipo de información uno depositó dentro de ella. En relación con la breve descripción que dimos al comenzar a hablar sobre Snapchat, en la que mencionamos que se categorizaba por la idea de que el contenido uno publicaba era efímero, lo mismo no sucede del lado de la plataforma. En las modificaciones realizadas en sus políticas de privacidad, ahora denotan específicamente que tipo de contenido recolectando. Dentro de acá se encuentran qué tipo de filtros que se utilizan en las publicaciones, las búsquedas realizada y las páginas que uno

[22] Pettit, H. (30 de mayo, 2018). Snapchat's Evan Spiegel says he would "appreciate it if Facebook copied our data practices" as he pokes fun at Mark Zuckerberg's long history of stealing his ideas, *Daily Mail – Mail Online*, https://www.dailymail.co.uk/sciencetech/article-5787083/Snapchat-CEO-Evan-Spiegel-encourages-Mark-Zuckerberg-copy-data-protection-practices-also.html

visita luego de utilizar la plataforma. Esto no quiere decir que anteriormente Snapchat no realizaba este tipo de prácticas, sino que simplemente ahora lo aclara en sus políticas de privacidad. Por último, también realizaron cambios que no son importantes para nuestro análisis como la creación de un término de acuerdo que aparece al cerrar la cuenta o nuevas políticas relacionadas a las "cookies". Esto se aplicó con la idea de poder tener un registro de la cantidad de gente que se elimina del sistema.

La cuarta plataforma que analizaremos será Youtube. A diferencia de las anteriores, esta se caracteriza por su orientación hacia creadores de contenidos en formato de video. En conjunto con Facebook, según el mapa creado por Veico, son la plataforma con mayor cantidad de usuario activos por mes. Y además, también se caracteriza por ser una gran plataforma que te permite anunciar. Comparten ciertas características, como por ejemplo ambos te permiten direccionar tu publicidad hacia determinado usuario. Al comienzo mencionamos que esta actividad es conocida como "microtargeting", ya que le permite al anunciante seleccionar que características debe tener la persona que consume esa publicidad. Pero a diferencia de Facebook, Youtube también te permite seleccionar en qué tipo de categoría uno quiere publicitar. Como dijimos anteriormente, esta plataforma está orientada hacia usuarios que crean videos. Una vez creado el contenido, para publicarlo, Youtube te exige que lo categorices de determinada forma, como por ejemplo videojuegos. Esta categorización le da la posibilidad al anunciante de que su anuncio se aplique a todos los videos que se encuentran dentro de esta categoría.

La razón por la cual elegimos considerar esta plataforma ya fue mencionada. Principalmente por la cantidad de usuario activos que tiene. Luego también porque se caracteriza por ser una plataforma con contenido en formato de video, a pesar de que Facebook también permite este tipo. Pero el detalle es que solamente te permite ese formato. Y en consecuencia es importante destacar la diferencia en el consumo de la publicidad que tiene el usuario. Como explicamos anteriormente, Facebook te permite publicitar una publicación, sin importar su formato, que se comparte a las personas que cumplan ciertos requisitos que determina el anunciante. Esta parte se cumple en Youtube, pero la diferencia es que la publicidad está integrada dentro de lo que lo usuario

consume. Es decir, si uno quiere ver un video de esta plataforma, muy probablemente tenga anuncio. Este anuncio puede aparecer al comienzo, a la mitad del video o al final. Pero uno está obligado a consumir sus primero cinco segundos y después te da la opción de poder saltearlo y continuar con el video que uno pretendía ver. Existen cinco segundos que uno está obligado del anuncio mientras que en Facebook es más fácil ignorarlo ya que solamente continúas navegando las noticias que uno encuentra al entrar a ella.

Una de las modificaciones realizada que más nos llama la atención está vinculada con la compra de publicidad por terceros. Es decir, Youtube ahora solamente permitirá a empresas que utilizan DoubleClick para pasar su publicidad. DoubleClick es una plataforma que cualquier marca se puede asociar para poder aplicar campañas comerciales por internet. Un detalle que no es menor es que Google es dueño de tanto DoubleClick como Youtube. Este nuevo requerimiento de Youtube en relación con la exigencia de tener una asociación con DoubleClick, le evita a Google de que cualquier entidad publicite en su plataforma. Principalmente, esto solamente se aplicaría en el continente europeo debido a las nuevas regularidades por parte del Reglamente General de Protección de Datos establecidas el 25 de mayo. El segundo cambio realizado por Youtube está relacionado con una práctica de rastreo. Este método, conocido como “píxel tracking”[23], es una forma en la cual una página obtiene información sobre la actividad que tiene el usuario dentro de su página. La finalidad de este método es que a partir de esa recolección de información sobre el usuario se utilicen para saber qué tipo de publicidad pasarle una vez que vuelva la misma página. También se utilizan para hacer analizar cómo se mueven las personas dentro de tu página. Youtube aplicaba este método de recolección que luego utilizaba para saber que publicidad pasarle al usuario antes de ver el contenido.

Como dijimos anteriormente, Youtube pertenece a Google. Si uno pretende entrar a las políticas de privacidad de Youtube, directamente se redirecciona hacia una página de Google. Es por eso por lo que también tomaremos en consideración algunos cambios realizados por Google que de

[23] RYTE Wiki, Tracking Pixel, https://en.ryte.com/wiki/Tracking_Pixel

cierta manera afectan a Youtube. En una publicación[24] realizada el 11 de mayo por el director relacionado a la privacidad y legalidad de Google, William Malcolm, se señalan distintos puntos. El primero de ellos es una modificación en las políticas de privacidad para que sean más fácil de entender en donde se explica de forma más sencilla las acciones realizadas por Google. Como venimos notando, esto es uno de los cambios más significativos. El segundo cambio relevante en nuestro análisis está relacionado a la información que recolectan. Realizaron modificaciones con el fin de que el usuario pueda entender de forma más clara sobre cómo Google recolecta nuestra información y la justificación de esta práctica. Todos esto cambios no solo reflejan los cambios realizados dentro de Youtube sino que a todas las plataformas o servicios que ofrece Google, como por ejemplo su servicio de correo electrónico llamado Gmail.

A continuación, abordaremos las redes sociales que no tienen su mayor volumen de usuarios dentro de América o Europa. Estas son: Qzone y VKontakte. Como describimos anteriormente, decidimos considerar estas plataformas dentro de nuestro análisis debido a la importancia de ver si sus estructuras internas fueron modificadas o no a pesar de no formar parte de la Unión Europea o tener que cumplir con las regulaciones del estado norteamericano.

Como ya hemos mencionado, Qzone tiene su origen en China. Este país tiene unas regularidades muy particulares sobre las redes sociales, principalmente el bloqueo completo sobre plataformas que el gobierno del país no puede controlar, como por ejemplo Facebook o WhatsApp. Todas estas plataformas que ofrecen una forma de comunicación ya necesaria para las rutinas de las personas fueron reemplazadas por plataformas desarrolladas por compañías de ese país: WeChat por WhatsApp, Weibo por Twitter o Youku por Youtube. A la hora de investigar sobre las políticas de la red social en cuestión, no se encuentran un sitio específico que las describa. Al entrar a la página principal de Qzone, de todos los enlaces que se encuentran ninguno te redirecciona a un sitio de dichas características. Pero si encontramos referencia

[24] Malcolm, W. (11 de mayo, 2018). Our Preparation for Europe's new data protection law, *Google Blog*, https://www.blog.google/outreach-initiatives/public-policy/our-preparations-europes-new-data-protection-law/

a las políticas de privacidad dentro del sitio de Tencent. Esta empresa multinacional es conocida dentro de China por proveer distintos servicios relacionados a internet y uno de ellos es Qzone. Fueron los fundadores de dicha red social en el año 2005 en el cual también constituyeron otras plataformas que ya hemos mencionado, como es el caso de WeChat. Utilizando como ejemplo a Youtube y Google, Tencent en este caso vendría a ser Google.

En relación con las políticas de privacidad, Tencent deja muy en claro las acciones que realiza en la materia de datos de sus usuarios en su sitio oficial[25]. Ya en el primer párrafo explicita que su posición: “al utilizar nuestros servicios, usted acepta que podemos recopilar, usar y compartir su información de acuerdo con esta política de privacidad, según sea revisada de vez en cuando.” También especifican los tipos de datos que recolectan como por ejemplo la información que especifica tu cuenta, desde tu nombre, número de teléfono, correo electrónico hasta tu número de tarjeta de crédito. La información que recolectan las plataformas también se especifica en esta lista: las publicaciones que compartís o creas, con quien las compartís, de donde las realizas, desde que proveedor de internet lo realizas, que búsquedas realizaste, con que personas te comunicaste y que tipo de mensaje realizaste. Justifican estos métodos diciendo que la recolección de datos se realiza para mejorar sus servicios, para entender cómo acceden sus usuarios a las plataformas e incluso para proveerte con publicidad y mejorarla. Existe una sección determinada sobre la publicidad en donde distinguen que ellos no comparten información personal con los distintos anunciantes o terceros sin que el usuario lo especifique pero que sí comparten información no personal, como por ejemplo información que directa o indirectamente te identifica.

Existe un apartado importante de destacar relacionado sobre a quiénes comparten tu información en donde se destaca la siguiente frase: “El usuario acepta que Tencent o alguna de las compañías afiliadas pueden requerir retener, preservar u ocultar tu información personal por distintos motivos”. Dentro de los distintos motivos que se enumeran, hay uno que dice que pueden realizar esto por requerimiento por una autoridad del gobierno, una fuerza de la ley o debido

[25] Tencent (14 de mayo, 2018) Privacy Policy

a que la empresa se vea obligada a realizarlo debido a leyes o regulaciones. Este punto describe perfectamente lo que mencionamos anteriormente sobre la actitud invasiva y controladora por parte del gobierno chino por sobre las redes sociales.

Ahora bien, particularmente no encontramos ninguna modificación relacionado con Cambridge Analytica o que refleje una actitud particular de la red social vinculado a sus políticas de privacidad. El caso de Qzone es todo lo contrario a lo que venimos analizando, debido a que el tipo de prácticas tomadas por la organización de Wylie son muy similar a las que realiza la plataforma. Como bien presenta el artículo de Wharton[26], de la escuela de negocios de la Universidad de Pennsylvania, "…las preocupaciones sobre la privacidad de los datos tienen una resonancia pública mucho menor en China que en los Estados Unidos, al menos en parte debido a preocupaciones más amplias sobre la capacidad del gobierno chino de usar la tecnología para monitorear más de cerca el comportamiento de sus ciudadanos."

El caso de la plataforma rusa no se aleja demasiado de Qzone, ya que el gobierno de Rusia comparte prácticas similares al gobierno chino. VKontakte tiene una reputación de hacerle llegar información al gobierno ruso sobre publicaciones de sus usuarios criticando o burlándose de las autoridades. Como es el caso de un usuario que compartió un meme criticando a la religión oficial del país[27], práctica que es ilegal según el Código Criminal Ruso, o cuándo encarcelaron a activistas del grupo Fundación Anti-Corrupción por publicar tuits que supuestamente incentivaban a que la gente se manifiesta en contra del gobierno[28]. A pesar de que la vigilancia estatal no nos compete en nuestra investigación, los hechos que reflejamos sí desenmascaran manipulación de datos personales. El Director General de VKontakte, Andrei Rogozov, se expresó

[26] Garrett, G. (4 de mayo, 2018). The Politics of Data Privacy in a Post-Cambridge Analytica World, *Universidad de Pensilvania – Knowledge at Wharton*, http://knowledge.wharton.upenn.edu/article/the-politics-of-data-privacy-in-a-post-cambridge-analytica-world/

[27] Moldes, C. (9 de agosto, 2018). Russians are facing criminal prosecution for sharing memes online, thanks to anti-extremism laws, *Global Voices*, https://globalvoices.org/2018/08/09/russians-are-facing-criminal-prosecution-for-sharing-memes-online-thanks-to-anti-extremism-laws/

[28] Echo, R. (25 de mayo, 2018). Russian anti-corruption activist are jailed for "inciting riots" based on their tweets and retweets, *Global Voices*, https://globalvoices.org/2018/05/25/russian-anti-corruption-activists-are-jailed-for-inciting-riots-based-on-their-tweets-and-retweets/.

en dos publicaciones distintas sobre estos eventos que sucedieron anunciando ciertos cambios en la plataforma. En la primera publicación[29] destaca ciertos cambios previos realizados por VK, como por ejemplo la opción de poner en modo privado los álbumes de fotos. Pero lo que más habla es sobre la posición que tiene la plataforma en situaciones como estas diciendo que "está obligada a cumplir con las leyes rusas y facilitar la búsqueda de delincuentes reales, pero nos oponemos firmemente a la persecución irrazonable por publicar en Internet". En la segunda publicación es donde se entra más en detalle sobre las modificaciones[30]. Por ejemplo, ahora el usuario tiene la posibilidad de poner en privado su perfil o también de restringir quien puede visualizar tus publicaciones. En esta publicación a su vez menciona el tema de los datos personales. En relación con esto, Rogozov sostiene que quiere que "…este proceso se lo más transparente posible…". Es por eso por lo que armaron una sección dentro de su plataforma donde se detalla sobre qué tipo de información almacenan, por cuanto tiempo o sus motivos de uso. A pesar de que sí encontramos cambios en su estructura, VKontakte no cambió por motivos relacionados a Cambridge Analytica sino que por motivos similares, ya que el accionar de la plataforma en relación con el uso de información personal de sus usuarios llegó a ser noticia.

Luego del análisis que acabamos de realizar, podemos encontrar determinados similitudes o patrones. En el anexo podemos encontrar un cuadro que retrata las distintas plataformas con los determinados cambios que realizaron. Uno de ellos es la cercanía de las modificaciones realizadas por Youtube, Facebook, Snapchat y Twitter. Todas estas plataformas llevaron a cabo sus cambios cercana a la fecha en la que el Reglamento General de Protección de Datos empezaba a aplicar sanciones a las plataformas que no cumplían sus requisitos, el 25 de mayo. Es por eso por lo que también hay similitud en las modificaciones que implementaron en sus plataformas, como por ejemplo la claridad en las políticas de privacidad, la posibilidad de modificar tu información o ser más explícitos con las acciones que realizadas con la información personal de sus usuarios. Dentro de los requerimientos nuevos podemos encontrarnos

[29] Rogozov, A. (13 de agosto, 2018). Publicación en su muro, *VKontakte*, https://vk.com/wall6492_7183

[30] Rogozov, A. (31 de agosto, 2018). Publicación en su muro, *VKontakte*, https://vk.com/wall6492_7418

con el derecho de ser olvidado, obligando a las plataformas a dar la posibilidad de poder eliminar su cuenta e información de los servidores, el derecho al acceso a tu propia información si el usuario lo pretende o el consenso en relación con las políticas de privacidad, exigencia que se ve reflejada en la nueva facilidad a la hora de leer estas políticas[31].

Otra similitud que encontramos es en relación con el tipo de información que recolectan todas estas empresas. Entre ellas se encuentran tu nombre, edad, sexo, correo electrónico e incluso los movimientos que realizas dentro de la plataforma. En el capítulo de "Privacidad vs Datos Personales", señalamos que la Asociación Internacional de Profesionales de Privacidad (IAPP) diferencia distintas categorías en relación con los datos personales. Particularmente, los datos que recolectan las redes sociales entran en tres de estas categorías que determina la asociación: datos internos, datos externos y datos de rastreo.

Por otro lado, el caso de Facebook y Twitter es muy particular debido a las fuertes acusaciones que tenían previamente. Gran parte de sus cambios fueron orientada sobre eso. Como por ejemplo los nuevos requisitos que el usuario debe cumplir si pretende publicitar dentro de la plataforma o cambios orientados a la eliminación de perfiles falsos que divulgan información falsa.

Es interesante denotar el rol fundamental que el Reglamento General de Protección de Datos está cumpliendo. Como dijimos anteriormente, gran parte de estos cambios se realizaron gracias a que las nuevas regulaciones establecidas por esta entidad se iban a comenzar a aplicar a fines del mes de mayo. Un dato no menor es que en abril del año 2016 recién la Unión Europea comenzó a optar por estas nuevas medidas pero tuvieron que pasar por lo menos dos años más para que se empiecen a aplicar. Y además, que solo en el continente europeo es donde estas nuevas exigencias se necesitan cumplir. A pesar de esto Facebook, Twitter, Youtube y Snapchat realizaron cambios que se aplicaban indistintamente de donde el usuario se encontraba. Es decir, no necesariamente el usuario debía entrar a la plataforma en Europa para que pueda de gozar de estas modificaciones.

[31] GDPR, *GDRP Key Changes,* https://eugdpr.org/the-regulation/

Conclusión:

Al comienzo de este trabajo, nos propusimos cuatro objetivos: analizar el caso de Cambridge Analytica y su relacionamiento con Facebook, con el fin de contextualizar la magnitud y las personas involucradas, estudiar el concepto de auto regulación y cómo es implementado hoy en día por las plataformas sociales, enumerar las similitudes y distinciones entre privacidad y datos personales, al igual que describirlos individualmente, y por último estudiar plataformas en particular que modificaron sus políticas de privacidad. Todos estos objetivos considerados a partir de la pregunta central: ¿Hasta qué punto el escándalo entre Facebook y Cambridge Analytica incidió en los cambios de las políticas de privacidad de distintas plataformas sociales?

Como bien describimos en nuestro último capítulo, encontramos que solamente cuatro de las seis aplicaciones realizaron modificaciones en sus políticas: Facebook, Twitter, Snapchat y Youtube. Plataformas que se caracterizan por ser las que más tráfico generan y más usuarios activos tienen. Mientras que las otras dos aplicaciones, VKontakte y Qzone, o no realizaron modificaciones o realizaron modificaciones por cuestiones ajenas a Cambridge Analytica. Ahora bien, tomando en consideración estas cuatro aplicaciones que sí modificaron sus políticas, la cuestión es estudiar si realmente realizaron sus cambios por la presión de Cambridge Analytica o si fueron otros los motivos.

La situación entre Cambridge Analytica y Facebook logró tener relevancia mediática a mitad de marzo con las declaraciones públicas de Christopher Wylie a través de The New York Times y The Guardian. Mientras que las aplicaciones en cuestión realizaron sus cambios a fines de mayo. Facebook fue la única que llevó a cabo cambios antes debido a que era la plataforma que se veía afectada directamente por el escándalo y que rápidamente debía cambiar su imagen hacia el público. Logró esto gracias a la posibilidad de auto regularse y por voluntad propia de llevar a cabo cambios que modifican su estructura sin la necesidad de esperar por organizaciones o entes regulatorios. Por otra parte, la razón por la cual las otras tres aplicaciones realizaron sus cambios cerca de fin de mayo fue debido al Reglamento General de Protección de Datos que se aplicaba partir del 25 de ese mes.

Una de las ideas que podemos desprender de esto es que Cambridge Analytica, al tener consideración mediática por parte del público y los países, indirectamente presionó a que el Reglamento General de Protección de Datos entre en vigencia. Pero cómo bien sostuvimos al final del capítulo anterior y como bien describe la página del Reglamento apenas uno ingresa, este proyecto entró en vigor en abril del 2016 pero se aplicó recién este año. Entonces podemos sostener que el proyecto iba a entrar en vigencia e implementarse si hubiera sucedido o no lo de Cambridge Analytica. La única plataforma a la cual esta idea no acompaña es a Facebook debido a que se auto reguló para rápidamente cambiar la percepción del público y sus usuarios.

En uno de los capítulos tomamos en consideración el concepto de auto regulación con el fin de poder describir una forma en la cual las empresas transmiten sus posiciones, valores e ideas a sus usuarios. De las cuatro plataformas en cuestión, las cuatro llevaron a cabo procesos regulatorios por voluntad propia. Cómo dijimos anteriormente, Facebook debido a la presión pública de las declaraciones públicas de Christopher Wylie y Youtube, Snapchat y Twitter para cumplir con el Reglamento General de Protección de Datos. Una futura investigación podría ser estudiar la efectividad de este recurso y sus diferentes formas de aplicación. Ahora bien, el New York Times lanzó una publicación[32] a principios de abril de este año en donde resalta que, a pesar de que la temática sobre la privacidad y las políticas de privacidad aplicadas por las redes sociales llegaron a la agenda de los distintos medios, muchos profesionales sostienen que posiblemente los verdaderos cambios nunca lleguen. Cuando nos referimos a verdaderos cambios, nos referimos a modificaciones en las políticas de privacidad que realmente protejan a sus usuarios. El ejemplo perfecto es el ataque que sufrió Facebook el día 28 de septiembre en donde un problema en la seguridad afectó a más de 50 millones de usuarios imposibilitándoles acceder a su cuenta y robándoles los datos de ingreso a la cuenta[33]. Podríamos sostener la idea de que este tipo de

[32] Bowles, N. (12 de abril, 2018). After Cambridge Analytica, Privacy Experts Get to Say “I Told You So”, *The New York Times*, https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html

[33] Rosen, G. (28 de septiembre, 2018). Security Update, *Facebook Newsroom*. https://newsroom.fb.com/news/2018/09/security-update/.

organizaciones o empresas están tomando ventaja de los que conocemos cómo auto regulación ya que, a pesar de que proveen información sobre lo que hacen, muchas veces es confuso, difícil de entender o incluso no realizan los cambios que prometen realizar.

Ahora bien, una solución que se nos ocurre ante este problema es la participación más activa por parte de los entes regulatorios. Cómo si fuesen los únicos capaces de defender a los usuarios. Uno de los autores que mencionamos anteriormente, Esteve, sostiene una posición contraria a esta hipotética solución. El autor encuentra que este tipo de proyectos en los que los objetivos restringen cómo los datos personales son usados, resultan ser sumamente inefectivos debido a que en la actualidad nos encontramos en un mundo hiperconectado. Continúa diciendo que esto puede afectar a cómo se llevan a cabo distintas innovaciones o desarrollos de nuevas técnicas de comunicación.

A pesar de esta idea, el estudio sobre cómo las políticas afectan o no el avance de las técnicas comunicativas no fue el eje central de nuestra investigación. Nosotros pretendíamos responder la pregunta de qué si el caso de Cambridge Analytica provocó cambios en las políticas de privacidad de distintas plataformas sociales. Lo que encontramos es que esto no sucedió, solamente en el caso de Facebook ya que era la plataforma que es veía afectada por la situación.

Anexo:

Red Social	Cambios Realizados
Facebook	• Exigencia en tener la cuenta verificada si pretende publicitar. • Usuarios con gran cantidad de páginas en su poder deben tener verificación. • Facilidad para acceder a los ajustes de tus datos. • Modificación del menú de privacidad dejándolo más claro y fácil para los usuarios. • Facilidad a la hora de querer eliminar datos de cuenta y la posibilidad de descargarlos.
Twitter	• Cambios en la forma de control de la información personal, haciéndolo más sencillo e intuitivo. • Transparencia en relación con el manejo de la plataforma con la información del usuario, tomando en cuenta las aplicaciones. • Mayor control sobre como terceros utilizan la información de los usuarios de la plataforma en relación con la publicidad. • Promesa de cumplir todas las exigencias que se le hagan por parte de los entes regulatorios.
Snapchat	• Acceso más sencillo a las configuraciones personales del usuario. • Posibilidad de modificar, borrar o la información del usuario. • Listado específico de que tipo de información recolectan.
Youtube	• Empresas que pretenden publicitar dentro de la plataforma, solamente lo pueden hacer a través de DoubleClick. • Terminación del “píxel tracking”.

	• Explicación más sencilla sobre las políticas de privacidad y el accionar de la plataforma en relación con los datos del usuario. • Claridad sobre que tipo de información recolectan y cuál es el fin de ella.
Qzone	• No realizaron cambios.
VKontakte	• Realizaron cambios pero ajenos a lo sucedido con Cambridge Analytica.

Bibliografía:

Marazzi, A. Cinco Horas Diarias Mirando el Teléfono, *Revista Anfibia*, http://www.revistaanfibia.com/cronica/cinco-horas-diarias-mirando-telefono/. Retirado el 21 de agosto de 2018.

Center for Humane Technology, http://humanetech.com/problem/. Retirado el 21 de agosto de 2018.

SCL Group, https://sclgroup.cc/home. Retirado el 6 de septiembre de 2018.

Cadwalladr, C. (18 de marzo, 2018). "I made Steve Bannon's psychological warfare tool": meet the data war whistle blower, *The Guardian*, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. Retirado el 10 de septiembre de 2018.

Statt, N. (31 de julio, 2018). Facebook shuts off Access to user data for hundreds of thousands of apps, *The Verge,* https://www.theverge.com/2018/7/31/17637244/facebook-apps-api-access-shut-off-missed-review-deadline. Retirado el 10 de septiembre de 2018.

Thompson, N. (21 de marzo, 2018). Mark Zuckerberg talks to Wired about Facebook's privacy problems, *Wired*, https://www.wired.com/story/mark-zuckerberg-talks-to-wired-about-facebooks-privacy-problem/. Retirado el 11 de septiembre de 2018.

Federal Election Comission, (26 de marzo, 2018). Proposed Rules, Vol. 83, N. 58. http://sers.fec.gov/fosers/showpdf.htm?docid=373521. Retirado el 12 de septiembre de 2018.

Stewart, E. (24 de mayo, 2018). Why you're getting so many emails about privacy policies, *Vox*, https://www.vox.com/policy-and-politics/2018/4/5/17199754/what-is-gdpr-europe-data-privacy-facebook. Retirado el 12 de septiembre de 2018.

Stewart, E. (10 de abril, 2018). What the government could actually do about Facebook, *Vox*, https://www.vox.com/policy-and-politics/2018/4/10/17208322/facebook-mark-zuckerberg-congress-testimony-regulation. Retirado el 12 de septiembre de 2018

Zuckerberg, M. (6 de abril, 2018). *Facebook*, https://www.facebook.com/zuck/posts/10104784125525891. Retirado el 13 de septiembre de 2018.

Illing, S. (11 de abril, 2018). "It's pretty much the Wild West": why we can't trust Facebook to police itself, *Vox,* https://www.vox.com/2018/3/21/17146674/zuckerberg-hearing-facebook-cambridge-analytica. Retirado el 13 de septiembre de 2018.

Bhardawj, P. (11 de mayo, 2018). Eight weeks after the Cambridge Analytica scandal, Facebook's stock price bounces back to where it was before the controversy, *Business Insider*, https://www.businessinsider.com/facebooks-stock-back-up-cambridge-analytica-charts-2018-5. Retirado el 13 de septiembre de 2018.

Acton, B. (20 de marzo, 2018). Publicación en Twitter, https://twitter.com/brianacton/status/976231995846963201. Retirado el 13 de septiembre de 2018.

Thompson, R. L. (2012). Radicalization and the Use of Social Media, *Journal of Strategic Security* 4, 4(4) (167 – 190), scholarcommons.usf.edu/jss/vol4/iss4/9. Retirado el 19 de septiembre de 2018.

Agan, T. (2007). Micro-targeting, *Penn, Schoen & Berland White Paper.* https://adage.com/images/random/microtarget031207.pdf. Retirado el 19 de septiembre de 2018.

Honest Ad Act 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1989/text. Retirado el 20 de septiembre de 2018.

Ingram D. and Auchard, E. (25 de marzo, 2018) Americans less likely to trust Facebook than rivals on personal data, *Reuters,* https://www.reuters.com/article/us-facebook-cambridge-analytica-apology/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-idUSKBN1H10AF. Retirado el 20 de septiembre de 2018.

Bansal, J. (9 de julio, 2018) The Self-Regulation Window Is Closing For Tech Companies, *Forbes*, https://www.forbes.com/sites/forbestechcouncil/2018/07/09/the-self-regulation-window-is-closing-for-tech-companies/#32accd263ba5. Retirado el 20 de septiembre de 2018.

Illing, S. (18 de julio, 2018) Why "fake news" is an antitrust problem, *Vox*, https://www.vox.com/technology/2017/9/22/16330008/eu-fines-google-amazon-monopoly-antitrust-regulation. Retirado el 20 de septiembre de 2018.

Egan, E. and Beringer, A. (28 de marzo, 2018) It's Time to Make Our Privacy Tools Easier to Find, *Facebook Newsroom*, https://newsroom.fb.com/news/2018/03/privacy-shortcuts/. Retirado el 21 de septiembre de 2018.

International Association of Privacy Policy, *Categories of Personal Information*, https://iapp.org/media/pdf/resource_center/Categories-of-personal-information.pdf. Retirado el 26 de septiembre de 2018.

Hibbard, E. A. (2015). Privacy vs. Data Protection, *Data Storage Innovation Conference*, https://www.snia.org/sites/default/files/Hibbard_DSI_2015_Privacy-vs-Data-Protection-v2-revision.pdf. Retirado el 27 de septiembre de 2018.

European Union Agency for Fundamental Right (2000), *Article 8 – Protection of Personal Data,* http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data. Retirado el 1 de octubre de 2018.

European Union (1996), Article 29: Data Protection Working Party, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Retirado el 1 de octubre de 2018.

Asunción, E. (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA, *International Data Privacy Law*, Volume 7, 1(1), (36 – 47), https://doi.org/10.1093/idpl/ipw026. Retirado el 1 de octubre de 2018.

Data Protection Commission, Chapter 2: General Rules on The Lawfulness of the Procession of Personal Data, *EU Directive*, https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-2/93.htm. Retirado el 1 de octubre de 2018.

Nissenbaum, H. (2010) Privacy in Context: Technology,Policy and the Integrity of Social Life. Cap. 4. Stanford Law Books.

Bowcott, O. (12 de septiembre, 2018). GCHQ data collection regime violated human rights, court rules, *The Guardian*, https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules. Retirado el 3 de octubre de 2018.

Hutt. R. (20 de marzo, 2017). The world's most popular social networks, mapped, *World Economic Forum*, https://www.weforum.org/agenda/2017/03/most-popular-social-networks-mapped/. Retirado el 11 de octubre de 2018.

Kan, M. (30 de octubre, 2014). China: Facebook not banned, but must follow rules, *PC World*, https://www.pcworld.com/article/2841252/china-facebook-not-banned-but-must-follow-the-rules.html. Retirado el 11 de octubre de 2018.

Vincos Blog. (5 de febrero, 2018). El mapa de las redes sociales en el mundo 2018, *Vincos*, http://vincos.it/2018/02/05/la-mappa-dei-social-network-nel-mondo-gennaio-2018/. Retirado el 11 de octubre de 2018.

Schroepfer, M. (4 de abril, 2018). An Update on Our Plans to Restric Data Access on Facebook, *Facebook Newsroom,* https://newsroom.fb.com/news/2018/04/restricting-data-access/. Retirado el 14 de octubre de 2018.

Facebook. (28 de marzo, 2018). Shutting Down Partner Categories, *Facebook Newsroom*, https://newsroom.fb.com/news/h/shutting-down-partner-categories/. Retirado el 14 de octubre de 2018.

Schrage, E. (9 de abril, 2018). Facebook Launches New Initiative to Help Scholars Assess Social Media's Impact on Elections, *Facebook Newsroom*,

https://newsroom.fb.com/news/2018/04/new-elections-initiative/. Retirado el 14 de octubre de 2018.

Ivanova, I. (10 de abril, 2018). 8 promises from Facebook after Cambridge Analytica, *CBS News – Moneywatch*, https://www.cbsnews.com/news/facebooks-promises-for-protecting-your-information-after-data-breach-scandal/. Retirado el 14 de octubre de 2018.

Kimer, J. (21 de marzo, 2018). Big Tech is Failing the Self-Regulation Test, *Corporate Foreign Policy*, https://corporateforeignpolicy.com/big-tech-is-failing-the-self-regulation-test-23674f93a590. Retirado el 17 de octubre de 2018.

Twitter, (Mayo, 2018). Updated to our Terms of Service and Privacy Policy. https://help.twitter.com/en/rules-and-policies/update-privacy-policy. Retirado el 17 de octubre de 2018.

Twitter, Privacy Policy, https://twitter.com/en/privacy#update. Retirado el 17 de octubre de 2018.

Snapchat, Privacy Policy, https://www.snap.com/en-US/privacy/privacy-policy/. Retirado el 17 de octubre de 2018.

Pettit, H. (30 de mayo, 2018). Snapchat's Evan Spiegel says he would "appreciate it if Facebook copied our data practices" as he pokes fun at Mark Zuckerberg's long history of stealing his ideas, *Daily Mail – Mail Online*, https://www.dailymail.co.uk/sciencetech/article-5787083/Snapchat-CEO-Evan-Spiegel-encourages-Mark-Zuckerberg-copy-data-protection-practices-also.html. Retirado el 17 de octubre de 2018.

Irwin, L. (24 de mayo, 2018). Snapchat releases details of its GDPR compliance measures, *It Governance*, https://www.itgovernance.eu/blog/en/snapchat-releases-details-of-its-gdpr-compliance-measures. Retirado el 17 de octubre de 2018.

Kurzer, R. (12 de abril, 2018). Youtube to stop supporting third party ad serving in EU in May, citing GDPR, *Marketing Land*, https://marketingland.com/youtube-to-stop-supporting-third-party-ad-serving-in-eu-in-may-citing-gdpr-238012. Retirado el 28 de octubre de 2018.

RYTE Wiki, Tracking Pixel, https://en.ryte.com/wiki/Tracking_Pixel. Retirado el 28 de octubre de 2018.

Malcolm, W. (11 de mayo, 2018). Our Preparation for Europe's new data protection law, *Google Blog*, https://www.blog.google/outreach-initiatives/public-policy/our-preparations-europes-new-data-protection-law/. Retirado el 28 de octubre de 2018.

Tencent (14 de mayo, 2018) Privacy Policy, https://www.tencent.com/en-us/zc/privacypolicy.shtml. Retirado el 31 de octubre de 2018.

Garrett, G. (4 de mayo, 2018). The Politics of Data Privacy in a Post-Cambridge Analytica World, *Universidad de Pensilvania – Knowledge at Wharton*, http://knowledge.wharton.upenn.edu/article/the-politics-of-data-privacy-in-a-post-cambridge-analytica-world/. Retirado el 1 de noviembre de 2018.

Moldes, C. (9 de agosto, 2018). Russians are facing criminal prosecution for sharing memes online, thanks to anti-extremism laws, *Global Voices*, https://globalvoices.org/2018/08/09/russians-are-facing-criminal-prosecution-for-sharing-memes-online-thanks-to-anti-extremism-laws/. Retirado el 1 de noviembre de 2018.

Echo, R. (25 de mayo, 2018). Russian anti-corruption activist are jailed for "inciting riots" based on their tweets and retweets, *Global Voices*, https://globalvoices.org/2018/05/25/russian-anti-corruption-activists-are-jailed-for-inciting-riots-based-on-their-tweets-and-retweets/. Retirado el 1 de noviembre de 2018.

Rogozov, A. (13 de agosto, 2018). Publicación en su muro, *VKontakte*, https://vk.com/wall6492_7183. Retirado el 5 de noviembre, 2018.

Rogozov, A. (31 de agosto, 2018). Publicación en su muro, *VKontakte*, https://vk.com/wall6492_7418. Retirado el 5 de noviembre, 2018.

GDPR, *GDRP Key Changes,* https://eugdpr.org/the-regulation/. Retirado el 5 de noviembre de 2018.

The Economist, *The Economist Intelligence Unit's Democracy Index*. https://infographics.economist.com/2018/DemocracyIndex/. Retirado el 27 de noviembre de 2018.

Greenleaf, G. (2017). Global Tables of Data Privacy Laws and Bills, *Privacy Laws & Business International Report*, 145, (14 – 26). University of New South Wales.

Rosen, G. (28 de septiembre, 2018). Security Update, *Facebook Newsroom*. https://newsroom.fb.com/news/2018/09/security-update/. Retirado el 28 de noviembre, 2018.

Bowles, N. (12 de abril, 2018). After Cambridge Analytica, Privacy Experts Get to Say "I Told You So", *The New York Times*, https://www.nytimes.com/2018/04/12/technology/privacy-researchers-facebook.html. Retirado el 28 de noviembre de 2018.