Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: Protección de datos personales y redes sociales: cambios en las políticas de privacidad de Facebook tras la implementación del Reglamento General de Protección de Datos de la Unión Europea

Autores (en el caso de tesistas y directores):

Ana Clara Morana

Bernadette Califano, tutora

Fernando Amdan, co-tutor

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2020

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS SOCIALES
CARRERA DE COMUNICACIÓN SOCIAL

Protección de datos personales y redes sociales:

Cambios en las políticas de privacidad de Facebook tras la implementación del Reglamento General de Protección de Datos de la Unión Europea

TESINA DE GRADO

Fecha de entrega: diciembre 2019

Alumna: Ana Clara Morana (anaclaramorana@gmail.com)

Tutora: Bernadette Califano (bernacali@gmail.com)

Cotutor: Fernando Amdan (fernando.amdan@gmail.com)

Índice

1. Introducción

Los acelerados cambios de las Tecnologías de la Información y la Comunicación (TIC) han permitido un aumento exponencial de las capacidades de almacenamiento, procesamiento y análisis de la información. Esta capacidad técnica ha facilitado el éxito de la monetización de las plataformas online de redes sociales, a través de sus herramientas de publicidad y elaboración de perfiles.

Nuestro trabajo se propone indagar sobre las tensiones vinculadas a la protección de datos personales de los usuarios de redes sociales, considerando particularmente el funcionamiento de la red social Facebook. Para esto, nos interesa estudiar sus condiciones de uso y políticas de privacidad en relación a la normativa vigente en la Unión Europea (UE) a partir del 2018 y en Argentina desde el año 2000.

La venta de espacios publicitarios en línea combinada con sofisticadas técnicas de segmentación de las audiencias ha permitido a las plataformas online de redes sociales construir su modelo de negocios. Particularmente Facebook, que comenzó a funcionar en el año 2004 como una red social restringida al uso dentro de la Universidad de Harvard, en el año 2006 amplió su registro por fuera del ámbito académico y llegó a alcanzar, ese mismo año, 12 millones de usuarios activos. Según el último informe de resultados publicado por la empresa, a fines de septiembre de 2019 contaba con 2450 millones de usuarios activos por mes[1], es decir, un 54% del total de los 4500 millones de usuarios totales de Internet en el mundo[2]. En cuanto a su actividad publicitaria, la empresa recaudó durante el año 2019 un total de 48 919 millones de dólares de ingresos por publicidad[3].

La actividad en línea deja huellas que retroalimentan el funcionamiento de las plataformas, moldeando las experiencias de los usuarios a medida. La información se ha convertido en un valioso capital: las grandes empresas de tecnología como Google y Facebook lograron monetizar sus plataformas de anuncios publicitarios valiéndose de las técnicas de elaboración de perfiles y publicidad dirigida y personalizada. En este contexto, surgen tensiones vinculadas a la protección de los datos personales de los usuarios disponibles en Internet, dentro de los cuales cabe distinguir: los datos cedidos de manera voluntaria a partir de un consentimiento expreso, los datos que surgen de una posterior tarea de procesamiento y

[1] Facebook Investor Relations (2019, 30 de octubre). *Facebook Reports Third Quarter 2019 Results.* Recuperado de https://s21.q4cdn.com/399680738/files/doc_financials/2019/q3/FB-Q3-2019-Earnings-Release.pdf

[2] Internet World Stats (2019). *WORLD INTERNET USAGE AND POPULATION STATISTICS 2019 Mid-Year Estimate.* Recuperado de https://www.internetworldstats.com/stats.htm

[3] Facebook Investor Relations (2019). *Quarterly Earnings.* Recuperado de https://investor.fb.com/financials/default.aspx

análisis de los anteriores y el entrecruzamiento con otras bases de datos, y los datos recopilados sin consentimiento expreso e informado por parte del titular.

De la distinta naturaleza de los datos y la multiplicidad de operaciones de tratamiento, surgen posibles conflictos sobre la finalidad por la cual fueron recogidos y el uso que finalmente se les da, sobre el nivel de conocimiento que el usuario tiene sobre estos mecanismos y su capacidad de brindar un consentimiento expreso e informado para ello y sobre las posibilidades efectivas de acceso y rectificación a su información personal en caso de ser necesario.

Las plataformas online de redes sociales promueven de manera constante la participación del usuario, a través de la generación de contenido y las múltiples posibilidades de interacción con otros. Esto se traduce en grandes volúmenes de información personal y datos de comportamiento que los usuarios comparten a diario. Facebook, la red social seleccionada para abordar los objetivos de este trabajo, ha construido sus estrategias de comercialización en base al aprovechamiento de estos grandes volúmenes de datos para perfeccionar el funcionamiento de su plataforma de venta de espacios publicitarios, lo cual le ha permitido alcanzar los 5 millones de anunciantes activos[4].

Las operaciones de la red social Facebook sobre los datos de sus usuarios han sido reconocidas públicamente con una mirada crítica. Podemos encontrar en los medios masivos de comunicación varios casos publicados como ejemplos de “manipulación de datos” por parte de la plataforma. Uno de los casos más recientes, de difusión global, ocurrió en 2018 y fue protagonizado por la red social y una consultora política llamada Cambridge Analytica, la cual fue acusada de haber accedido a los datos de 50 millones de usuarios a través de la mencionada red social sin su consentimiento, para la implementación de campañas políticas segmentadas y la difusión de noticias falsas en función de los intereses, ideologías y comportamiento de los usuarios[5]. Facebook también ha sido acusada de haber compartido datos de los usuarios sin consentimiento previo con empresas fabricantes de dispositivos móviles[6], con entidades bancarias[7] y empresas de comercio electrónico[8], entre otros.

---

[4] Facebook llega a 5 millones de anunciantes activos en la plataforma y novedades para pequeños anunciantes. (2017, 10 de abril). *Facebook Newsroom.* Recuperado de https://ltam.newsroom.fb.com/news/2017/04/facebook-llega-a-5-millones-de-anunciantes-activos-en-la-plataforma-y-novedades-para-pequenos-anunciantes/

[5] 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. (2018, 21 de marzo) *BBC.* Recuperado de https://www.bbc.com/mundo/noticias-43472797

[6] Pozzi, S. (2018, 6 de junio). Facebook compartió datos con cuatro fabricantes de móviles chinos. *El País.* Recuperado de https://elpais.com/internacional/2018/06/06/actualidad/1528295615_677947.html

[7] Zuriarrain, J. M. (2018, 7 de agosto). Facebook intercambia información de los usuarios con entidades bancarias en EE UU. *El País.* Recuperado de https://elpais.com/tecnologia/2018/08/07/actualidad/1533649374_513508.html

[8] Facebook, cada vez más complicado: revelan una nueva filtración de datos de usuarios que involucra a Amazon. (2019, 4 de abril). *Clarín.* Recuperado de https://www.clarin.com/tecnologia/facebook-vez-complicado-revelan-nueva-filtracion-datos-usuarios-involucra-amazon_0_8dDqB-WBI.html

Este tipo de controversias relacionadas a la protección de los datos personales de los usuarios de redes sociales han influido en la opinión pública y en la voluntad política hacia una regulación más exigente y actualizada. En este contexto, nos proponemos indagar sobre el modelo de negocios de Facebook y el valor que los datos personales representan en él, las políticas de privacidad y de datos dentro de las cuales enmarca sus actividades y los cambios más recientes que la red social ha implementado en ellas como respuesta a la sanción del Reglamento General de Protección de Datos de la UE y las polémicas generadas en torno a sus actividades.

En mayo de 2018, entró en vigencia el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Con motivo de esta nueva reglamentación, Facebook implementó una serie de cambios en sus condiciones de uso y políticas de privacidad para adecuarse. La mayoría de estos cambios fueron implementados a nivel global, mientras que se reservaron algunas cuestiones específicas para cumplir con las obligaciones que el RGPD impone para la protección de los datos personales de los ciudadanos europeos. En nuestro trabajo analizaremos los cambios implementados en ambas instancias, tanto en el ámbito de la UE como fuera de la región, considerando para este caso las Condiciones de Uso y Política de Datos de la empresa disponibles en Argentina.

A la luz de estas nuevas tendencias regulatorias, en Argentina se presentó, en septiembre de 2018, un proyecto de reforma de la Ley 25.326 de Protección de Datos Personales, vigente desde el año 2000[9]. El Director de la Agencia de Acceso a la Información Pública[10], Eduardo Bertoni, afirma que algunas disposiciones del RGPD que apuntan a facilitar las transferencias de datos internacionales entre los países miembros de la UE y aquellos países que garanticen un nivel de protección adecuado, han promovido la revisión interna de muchas legislaciones nacionales en materia de protección de datos personales, con el objeto de alcanzar la adecuación con el RGPD y garantizar el flujo de datos con países de la UE, lo cual propiciaría entre otras cosas, las operaciones de comercio electrónico[11].

Es por esto que, una vez analizado en profundidad el RGPD, nos proponemos estudiar en el apartado final de nuestro análisis la Ley 25.326 de Protección de Datos Personales, los

[9] Bertoni, E. (2018, 25 de mayo). Europa protege sus datos personales. *La Nación.* Recuperado de https://www.lanacion.com.ar/opinion/europa-protege-sus-datos-personales-nid2137848

[10] La Agencia de Acceso a la Información Pública (AAIP) es el órgano de control de la Ley 27.275 de Derecho de Acceso a la Información Pública, de la Ley 25.326 de Protección de Datos Personales y de la Ley 26.951 de creación del Registro Nacional "No llame". Argentina.gob.ar (2019). *Planificación 2019 de la Agencia de Acceso a la Información Pública.* Recuperado de https://www.argentina.gob.ar/aaip/planificacion2019

[11] Bertoni, E. (2018, 25 de mayo). Europa protege sus datos personales. *La Nación.* Recuperado de https://www.lanacion.com.ar/opinion/europa-protege-sus-datos-personales-nid2137848

cambios propuestos en el proyecto de reforma mencionado y las similitudes y diferencias con lo dispuesto por el Reglamento europeo.

1. 2 Objetivos y Metodología

La presente tesina fue realizada en el marco del Grupo de Investigación en Comunicación (GIC) “TIC y cultura digital: políticas y conflictos emergentes”, dirigido por la Dra. Bernadette Califano durante el período 2018 - 2019.

El Objetivo general de este trabajo es analizar las tensiones vinculadas a la protección de datos personales de los usuarios de redes sociales, a partir del estudio de las políticas de privacidad de la red social Facebook y la normativa vigente en la Unión Europea y Argentina.

Para abordar el Objetivo general, proponemos como objetivos específicos:

- Describir el surgimiento de Facebook y el valor de los datos personales para su funcionamiento.
- Estudiar el marco regulatorio europeo y argentino en materia de protección de datos personales.
- Analizar los cambios en las políticas de privacidad de Facebook en relación a las normativas estudiadas.
- Caracterizar las tensiones emergentes vinculadas a la protección de los datos personales de los usuarios de redes sociales.

Desarrollaremos estos objetivos a partir de una investigación cualitativa, enfocándonos en el estudio de caso de la red social Facebook y la protección de los datos personales de sus usuarios. Realizaremos un relevamiento bibliográfico consultando algunas fuentes de referencia y un análisis documental y comparativo sobre los marcos regulatorios seleccionados.

Nuestro trabajo se estructura en seis partes. Comenzaremos desarrollando la bibliografía utilizada como marco conceptual para el análisis del objeto de estudio, identificando algunos planteos centrales a partir de los cuales definimos nuestros objetivos, preguntas de investigación y los conceptos teóricos para abordarlos.

Considerando estos planteos, en la segunda parte nos dedicaremos a estudiar específicamente el caso seleccionado, enfocándonos en dar cuenta de la lógica de funcionamiento de la red social Facebook y del valor de los datos personales para la plataforma.

Luego, estudiaremos la legislación europea vinculada a la protección de los datos personales, realizando un análisis comparativo entre el RGPD y la normativa que reemplaza, la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Una vez desarrollado el marco regulatorio de la UE, indagaremos sobre las tensiones y desafíos emergentes para la protección de los datos personales en relación al uso de las redes sociales y trabajaremos sobre las condiciones de uso y las políticas de privacidad de Facebook para analizar los cambios introducidos en relación a las modificaciones sancionadas por el RGPD.

Por último, estudiaremos los principios y disposiciones de la Ley 25.326 para la protección de datos personales en Argentina y analizaremos su proyecto de reforma, vinculándolo con el trabajo ya realizado sobre los estándares propuestos por el RGPD.

Algunas conclusiones y líneas de investigación posibles se sintetizan en el apartado final de este trabajo.

1.3 Antecedentes de la investigación

Como antecedentes de análisis relacionados con nuestro objeto de estudio, encontramos algunos planteos sobre la protección de la privacidad en Internet en De Gràcia (2013), donde, frente a la lógica de personalización de las plataformas, se presenta la necesidad de preservar el derecho de audiencia, entendido como el derecho de los individuos a tener acceso a todo tipo de contenidos, incluidos aquellos que no coincidan con sus intereses de acuerdo con los perfiles desarrollados automáticamente por las redes sociales. Existen, además, posturas como la de Rodríguez (2013), quien compara la tradición estadounidense en materia de protección a la privacidad con la normativa europea en relación a la protección de los datos personales. También relevamos los planteos de Álvarez Ugarte (2013) sobre las políticas de vigilancia y la necesidad de advertir los riesgos que éstas pueden implicar para la protección de la privacidad y de los datos. Por último, se destaca el análisis de Busaniche (2013) sobre una apropiación desigual de la manipulación de los datos en relación al control que ejercen las plataformas de redes sociales sobre la información personal de los usuarios.

En relación al funcionamiento de Internet y el control de la información, tomamos como referencia el análisis de Cortés (2012) sobre los distintos mecanismos técnicos que permiten realizar monitoreos de contenidos en línea y cómo dan forma a una arquitectura de red que puede representar un riesgo para los derechos fundamentales de los usuarios.

En cuanto a los estudios específicos sobre el uso de la información personal en redes sociales, se vinculan los planteos de Magnani (2014), quien desarrolla la idea de una nueva configuración de Internet basada en la explotación de los contenidos generados de manera colectiva y analiza el caso particular de Facebook desde el funcionamiento de su plataforma de publicidad y sus sofisticadas técnicas de personalización y segmentación en función de los intereses y comportamiento de los usuarios.

En esta misma línea, Gendler (2018) analiza el uso masivo de la información personal de los individuos como un modelo de producción gracias a los avances de las TIC. El autor entiende que las redes sociales imponen una nueva lógica de gubernamentalidad algorítmica, es decir, basada en la explotación, análisis y modulación de estos datos para la personalización de contenidos y modelar la conducta del usuario en ellas.

Se desarrollaron, además, tesinas de grado de la Carrera de Ciencias de la Comunicación de la Universidad de Buenos Aires que abordan ciertos aspectos relacionados con nuestro objeto de estudio. En la tesina *Tensiones y desafíos en la protección de los datos personales. El caso del Sistema Único de Boleto Electrónico (SUBE) en la Argentina* (Migliorini, 2018), se aborda la problemática del tratamiento de datos personales a cargo de los organismos del Estado. Este trabajo permite profundizar en la distinción del derecho a la protección de los datos personales respecto al derecho a la privacidad y, si bien difiere de los objetivos de la presente tesina, ya que no está orientado al análisis del tratamiento de datos personales por parte de una empresa privada, el análisis del caso SUBE sirve como referencia para el estudio de las operaciones de tratamiento y las implicancias de estas actividades sobre los derechos de los usuarios.

Otra tesina de grado elaborada en el marco de la Carrera, realiza un estudio del marco regulatorio sobre la protección de datos personales en Argentina y a nivel internacional en relación al desarrollo de las web 2.0, titulada *Protección de Datos Personales en redes sociales y webs 2.*0 (Passeron, 2012). Respecto al estudio de caso sobre las operaciones de tratamiento de datos personales ejercidas por una empresa privada, la tesina *Google adsense y la protección de datos personales. El conflicto del modelo de la publicidad digital dentro de la normativa argentina* (Lezcano, 2012) analiza las tensiones entre la protección de los datos personales y la lógica de funcionamiento de Google como plataforma digital de publicidad. Este trabajo representa también una valiosa referencia para nuestro estudio, el cual se distingue por la elección del caso, la incorporación de la normativa europea al análisis y el trabajo en profundidad sobre las políticas de privacidad de Facebook.

2. Marco conceptual

El análisis de nuestro objeto de estudio se desarrolla en el marco de lo que Manuel Castells (1995) definió como revolución tecnológica, fundada sobre el rol preponderante de la información y la creciente capacidad del procesamiento de los datos. Castells (1995) caracteriza este fenómeno como el surgimiento de "un nuevo modelo de organización sociotécnica" (p.1) que denomina modo de desarrollo informacional, ya que toma forma sobre los avances e innovación en el ámbito de las tecnologías de la información. Como todo modo de desarrollo, se asienta sobre un elemento clave para potenciar la productividad del modo de producción. En este caso, se trata de la aplicación del conocimiento científico para la generación de nuevos conocimientos: "Es la búsqueda y acumulación de conocimiento en sí mismo lo que determina la función tecnológica bajo el informacionalismo" (Castells, 1995, p.7).

Este nuevo modelo de organización ha coincidido con otro fenómeno histórico en el plano de la organización de nuestra sociedad: una etapa de reestructuración del sistema capitalista. Según Castells (1995), ambos fenómenos han dado lugar a la creación de un nuevo paradigma tecnológico, facilitado por las tecnologías de la información y su potencial capacidad de recolección, procesamiento y análisis de la información. Si bien la reestructuración del sistema capitalista podría haber ocurrido independientemente de estos cambios tecnológicos, las tecnologías de la información cumplieron un rol fundamental en su reinvención para superar las propias contradicciones del sistema, gracias al aumento de la productividad, a su capacidad para descentralizar y automatizar ciertos procesos de producción, a la promoción de un régimen económico internacional y a su flexibilidad inherente, que consolida la posición dominante del capital sobre el trabajo.

Estos cambios atraviesan todas las esferas de la vida humana, entre ellas, las actividades de consumo. Es un período caracterizado por el surgimiento de los mercados de masas, la estandarización de la producción y la internacionalización de la economía. En este contexto, los avances en el procesamiento de la información y la velocidad con la que son difundidos y aplicados se vuelven cruciales para acercar a las grandes empresas a sus consumidores:

> (...) la constitución de mercados de masas y la distancia cada vez mayor entre compradores y vendedores han creado la necesidad de un marketing específico y una distribución efectiva por parte de las empresas, disparando de este modo la creación de una cantidad de sistemas de acumulación de la información y flujos de distribución de la información, a fin de establecer la conexión entre los dos extremos del mercado. (Castells, 1995, p.14)

El sistema capitalista, cuya meta estructural responde al principio de la maximización del beneficio, afianza el cumplimiento de sus objetivos sobre el poder de la información y la generación de nuevos conocimientos a partir de su procesamiento. Esto genera crecientes redes descentralizadas de acumulación de datos para enriquecer los procesos de producción, consumo y organización de la sociedad, combinados con la innovación tecnológica y la acumulación de conocimiento científico.

Es en este contexto que nos proponemos estudiar el nivel de protección de la información personal de los usuarios en un producto particular de la mencionada revolución tecnológica: las plataformas de redes sociales. Nuestro trabajo se nutrirá del análisis que José Van Dijck (2016) propone acerca de una historia crítica de las redes sociales, distinguiendo el funcionamiento de las plataformas digitales de uso masivo a partir de seis elementos clave: Propiedad, Gobierno, Modelo de Negocios, Tecnología, Usuarios y Contenido. Este esquema de análisis surge de la combinación de dos abordajes: la teoría del actor-red (desarrollada por Bruno Latour, Michael Callon y John Law) y la economía política, dimensiones necesarias según Van Dijck para estudiar en profundidad la evolución del ecosistema digital, no sólo en el nivel de la tecnología y de la experiencia del usuario, sino también considerando su impacto en las dimensiones políticas, económicas, sociales y culturales.

La teoría del actor-red permite un análisis pormenorizado de cada plataforma digital o microsistema por separado, entendiéndolas como constructos tecnoculturales, mientras que la economía política las concibe como estructuras socioeconómicas organizadas, lo cual permite estudiar el ecosistema de plataformas digitales en su conjunto y advertir las leyes y normas que configuran su lógica particular de funcionamiento (Van Dijck, 2016). Para este enfoque, la infraestructura política y el régimen político y legal son fundamentales para explicar la evolución y éxito de este ecosistema de medios. Como referente de esta postura, la autora retoma los ya mencionados estudios de Castells sobre el contexto político económico que ha inaugurado una nueva etapa del sistema capitalista y ha permitido un crecimiento sostenido de los medios de autocomunicación de masas: el capitalismo informacional. Sus postulados advierten las relaciones de poder subyacentes a cada plataforma y permiten ahondar en el entramado de propietarios/desarrolladores/controladores y responsables del tratamiento de datos frente a los usuarios/productores de contenido/sujeto titular de datos.

Mientras que la economía política permite analizar las relaciones de poder desde una perspectiva institucional, la teoría del actor-red es útil para analizar cómo opera el poder en los dispositivos tecnológicos. La primera permite enfocarse en los regímenes de propiedad, gobierno y modelos de negocios, mientras que la segunda hace hincapié en los niveles de la

tecnología, los usuarios y el contenido. A continuación, describiremos brevemente cada uno de los elementos sobre los que Van Dijck construye su análisis:

- **Propiedad**: estudiar el régimen de propiedad de cada plataforma permite distinguir los objetivos de los propietarios, si se trata de una organización sin fines de lucro o de propiedad colectiva cuyo funcionamiento está centrado en el usuario, o si se trata de una empresa o corporación comercial y responde a los intereses económicos de sus accionistas.
- **Gobierno**: la estructura de gobierno refiere a los mecanismos bajo los que cada plataforma gestiona su funcionamiento, compuestos por protocolos técnicos (relacionados a las restricciones del código o la arquitectura de la red) y por protocolos sociales, es decir, normas explícitas e implícitas que definen el campo de acción de los usuarios de la red social. Las normas explícitas suelen asentarse en políticas de privacidad o condiciones de servicio que cada usuario debe reconocer haber leído y aceptado para ser partícipe de la red social. Éstas no adquieren fuerza de ley, pero aseguran restricciones, obligaciones y sanciones a la conducta dentro de la plataforma. Es importante señalar que Van Dijck admite la ignorancia y/o indiferencia de los usuarios frente a este tipo de contratos, los cuales por ser en su mayoría extensos, ambiguos y/o poco claros son aceptados sin ser leídos con detenimiento para acceder rápidamente a las plataformas.
- **Modelo de Negocios:** permite analizar las estrategias de monetización de las redes sociales como plataformas de anuncios publicitarios. Para Van Dijck, las plataformas deben dedicar especial cuidado en ponerlas en práctica de la manera más sutil y menos invasiva posible, de modo tal que no interfieran con la actividad de los usuarios en la red social ni consuma el ideal de gratuidad con el cual se promocionan este tipo de servicios en línea:

> Las estrategias de publicidad convencional dirigidas a las audiencias de masas dejan de ser válidas para un mundo dominado por el contenido generado por los usuarios y la red social; en un entorno social online poblado de “amigos”, los usuarios no esperan ni toleran la aparición de actividades comerciales. (Van Dijck, 2016, p.43)

- **Tecnología:** En esta dimensión se destacan las configuraciones del código por default y los cambios que operan en la interfaz no visible para el usuario, además de las restricciones inherentes a la interfaz visible que guían y condicionan su comportamiento en la red social. Desde este punto de vista, la plataforma es considerada como una instancia mediadora entre la actividad social del usuario y los algoritmos que codifican estos datos y traducen la información en un entorno digital

específico. Entendemos por algoritmo un conjunto de instrucciones técnicas que permiten el procesamiento de grandes volúmenes de información: “Es una lista finita de instrucciones definidas para calcular una función, una directiva paso a paso que permite un procesamiento o razonamiento automático que ordena a la máquina producir cierto *output* a partir de determinado *input*” (Van Dijck, 2016, p.35). En este caso, los datos de comportamiento y la información personal funcionan como insumo para el procesamiento y análisis algorítmico, mediante el cual se interpreta la información en función de los objetivos que fueran establecidos en su diseño. El valor agregado de Facebook como instancia mediadora reside en la capacidad de transformación de estos grandes volúmenes de información en un conjunto de datos consolidado de acuerdo a sus objetivos comerciales y los intereses de sus propietarios. Como veremos más adelante, este modelo de creación de valor es central para el funcionamiento de la plataforma y el éxito de sus estrategias de monetización.

- **Usuarios y hábito:** aquí se distingue la participación implícita del usuario, que tiene que ver con las configuraciones por defecto que mencionábamos en el ítem anterior, de la participación explícita, que alude al uso e interacción que el usuario establece con la red social, más allá de las limitaciones del código. Esta distinción permite a la autora centrarse en el análisis de las reacciones que han manifestado los usuarios frente a los cambios en el código o condiciones de servicio de las distintas plataformas, desde críticas aisladas hasta movimientos de una marcada organización con capacidad de acción sobre las decisiones unilaterales de las plataformas. En este sentido, Van Dijck advierte las posibilidades del usuario para ejercer un mayor poder sobre el funcionamiento de la red social, considerando un uso más consciente y participativo en ella.
- **Contenido:** esta dimensión suscita profundos debates en torno a cuestiones de propiedad intelectual, inabarcables en este estudio dados los objetivos planteados, pero cabe mencionar las tensiones que surgen entre los usuarios como productores de contenido que circula en la plataforma y los desarrolladores de las plataformas, qué tipo de información y formato es considerado contenido, quién es su propietario y quién lo controla.

Centrándonos en el funcionamiento de la red social que motiva este trabajo, debemos considerar que Van Dijck sostiene que Facebook necesitó afianzar un sentido más amplio de la palabra “compartir”. Se dio un proceso de cambio a nivel cultural y simbólico que generó grados aceptables del compartir, del mostrarse y del ser visto. La autora hace un particular hincapié en el rol que opera lo simbólico y lo cultural detrás de los mecanismos legales, económicos y operativos necesarios para un funcionamiento rentable para la red social: a

partir de estos cambios graduales enfocados en la acción del “compartir” reservada para los sujetos, allanaron el camino para cambiar gradualmente los grados aceptables de privacidad y monetización.

La autora realiza una fuerte crítica a estas empresas que defienden una “retórica de la transparencia y la apertura” (Van Dijck, 2016, p.19) en relación a la información de los usuarios y los contenidos producidos por ellos, pero mantienen una absoluta reserva sobre los procesos de monetización que sostienen sus plataformas: de qué manera operan, qué información es compartida con terceros y bajo qué términos y condiciones. En este sentido, es valioso retomar la distinción que propone entre los términos “conexión” y “conectividad” para dar cuenta de cómo opera este discurso de la transparencia frente a las políticas de la empresa: la conexión está dada entre usuarios y genera capital social, mientras que la conectividad está relacionada con la acción de compartir los datos de los usuarios con terceros y genera y se sustenta sobre la producción de valor en los metadatos. Esta distinción es útil para dar cuenta del control de la información.

En síntesis, este esquema permite desarrollar de qué manera operan la socialidad y la técnica en un mercado oligopólico, dominado por un reducido número de empresas que sostienen una retórica de la apertura y la transparencia en cuanto a la información y contenidos producidos por los usuarios pero mantienen una absoluta discreción sobre el control y manipulación que ejercen sobre estos datos (Van Dijck, 2016).

En relación a estos planteos, encontramos en el trabajo de Fumagalli, Lucarelli, Musolino, & Rocchi (2018) las herramientas necesarias para profundizar el análisis del modelo de negocios de Facebook, centrado en la creación de valor a partir del uso de la información personal de los usuarios. Los autores consideran particularmente el caso Facebook para dar cuenta del funcionamiento del capitalismo de plataformas - concepto que retoman del trabajo desarrollado por Nick Srnicek en su libro *Platform Capitalism* (Fumagalli et al., 2018, p.15) -, como un nuevo modelo de explotación y acumulación del capital centrado en las crecientes posibilidades de recolección y análisis de grandes volúmenes de información. Estos avances en las técnicas de procesamiento de la información fueron facilitados por el desarrollo de “algoritmos de segunda generación”, llamados así porque poseen una mayor capacidad de auto-aprendizaje, permitiendo un nivel de automatización mucho mayor: “De hecho, después de la primera etapa de implementación y creación, debida a la actividad humana, están en condiciones de operar de modo casi totalmente automatizado mediante el aprendizaje automático (*machine learning*)” (Fumagalli et. al., p.14).

Los autores caracterizan a Facebook como una plataforma “de anuncios publicitarios” (Fumagalli et al., 2018, p.26) y realizan una descripción detallada de los mecanismos de oferta

y demanda de espacios publicitarios sobre los que la red social asienta su modelo de valorización. Si bien Facebook fue concebida en sus orígenes para un uso exclusivamente académico (Fumagalli et al., 2018), el crecimiento exponencial de usuarios activos le permitió acumular grandes volúmenes de información personal y datos de comportamiento de las 2450 millones de personas que forman parte de la plataforma y generar espacios de comunicación y publicidad dentro de su entorno y fuera de él para su comercialización. La monetización de sus propios espacios publicitarios y la posibilidad de ofrecer espacios en sitios web y aplicaciones de terceros a través de la herramienta *Facebook Audience Network*[12], le permitió convertirse en "la plataforma de publicidad más efectiva" (Fumagalli et al., 2018, p.20). Este éxito se asienta sobre los volúmenes de información y datos que la red social recopila a partir de la actividad de sus usuarios y sus sofisticadas técnicas de análisis e integración de los mismos, lo cual le permite ofrecer un refinado servicio de personalización y direccionamiento de las campañas publicitarias, asegurando que cada mensaje llegue a un público interesado en él con altas probabilidades de ejecutar la acción para la cual es interpelado (sea una operación de compra, de registro, de click o de visualización de video, entre otras).

Este modelo de creación de valor se basa, según los autores, en la explotación del *free labour* (Fumagalli et al., 2018, p.33) o "trabajo gratuito"[13] en español realizado por los 2450 millones de usuarios que interactúan en la red social, generando relaciones con su comunidad, realizando operaciones de compra y venta y generando y visualizando contenido. Facebook ha conseguido explotar esta multiplicidad de expresiones sociales, culturales y lingüísticas y transformarlas en valor de cambio. Es por esto que podemos hablar de "prosumidores" (Fumagalli et al., 2018, p.29) para referirnos a este fenómeno en particular en el que el usuario de redes sociales se desempeña tanto como espectador o consumidor como productor de contenido e información relevante. Este rol es ejercido, desde la mirada de los autores, como un trabajo gratuito, que paulatinamente fue erosionando los límites entre el "tiempo de trabajo" y el "tiempo de vida" (Fumagalli et al., 2018, p.32) gracias a las posibilidades tecnológicas de las plataformas de redes sociales. La estrategia de monetización de Facebook se cimenta sobre la explotación de este trabajo gratuito, expropiando la información generada por los usuarios y transformándola en valiosos insumos para su negocio de publicidad online:

> (...) la compañía estadounidense de servicios de redes sociales y medios sociales en línea lanzada por Mark Zuckerberg representa un ejemplo de una plataforma publicitaria en la

[12] Facebook for Business (2019). Información de Audience Network. Recuperado de https://www.facebook.com/business/help/788333711222886?id=571563249872422

[13] En la traducción original al español recuperada de la Revista Hipertextos, Vol. 6, N° 9, el concepto de *free labour* es traducido como "trabajo libre" en lugar de "trabajo gratuito". Al traducir la palabra *free* al español ambas expresiones son admisibles, pero considerando que la investigación se plantea desde el estudio del capitalismo de plataformas, sus modelos de negocios y las nuevas formas de trabajo digital, en el presente trabajo se optó por el término "gratuito" para hacer referencia a este tipo de prácticas no asalariadas.

> que el valor se basa esencialmente en un proceso de expropiación de las destrezas vitales de las personas. (Fumagalli et. al, 2018, p.15)

Esta actividad se nutre, además, de la asociación que la plataforma ha establecido con proveedores de datos de terceros, a partir de lo cual puede realizar un entrecruzamiento de datos con información del comportamiento de los usuarios en el mundo físico u *offline* (fuera de línea): “Facebook se ha asociado con proveedores de datos de terceros, esto es, con los intermediarios de datos Axciom, Epilson, Experian, Datalogix, Oracle, and Quantium para tener acceso a las personas en función de lo que compran y hacen fuera de línea” (Fumagalli et. al, 2018, p. 18).

Estas reflexiones permiten a los autores desarrollar el concepto de “labor digital” (Fumagalli et al., 2018, p. 32) para dar cuenta de las nuevas prácticas de producción en el capitalismo de plataformas: un tipo de trabajo no asalariado, que atraviesa todos los espacios de interacción social y borra las fronteras del ocio y el trabajo, gracias a la presencia constante e ininterrumpida de la figura del prosumidor. Para los autores, este concepto es útil para caracterizar las nuevas fuentes de valorización basadas en la captación de la información personal, mientras que reservan el concepto de “trabajo digital” para aquellas formas de trabajo asalariadas que utilizan las plataformas digitales para ofrecer servicios de manera independiente en un marco de reducción de derechos para el trabajador (Fumagalli et al., 2018, p.31).

Retomaremos también los planteos de Lawrence Lessig (1998) acerca de los límites y posibilidades de regulación de la conducta en el ciberespacio, para examinar con detenimiento las características particulares de la arquitectura de red de Facebook y las decisiones políticas que la sustentan. Según el autor, es importante considerar que la arquitectura de red o código - es decir, el conjunto de protocolos y reglas que dan forma a un entorno digital particular - no está dada por naturaleza, sólo es una entre otras tantas posibilidades: “(...) el problema es que, evidentemente, la red no tiene naturaleza alguna. No hay una única arquitectura que sea esencial del diseño de la red” (Lessig, 1998, p.6). Detrás de la escritura del código hay un conjunto de valores y principios que constituyen un espacio digital específico, es decir, el código resulta de un conjunto de decisiones políticas que tenderá a valorar en mayor o menor medida las posibilidades de libertad o control a la conducta del usuario. Esta conducta no sólo es regulada por los límites impuestos a través de la arquitectura de red, sino que también es influida y guiada por la ley, las normas sociales y el mercado. La ley no sólo opera directamente sobre la conducta, sino que también puede influir de manera indirecta sobre el resto de las modalidades de restricción. Este elemento es clave para descubrir los caminos posibles hacia una mayor regulación del ciberespacio. En lugar de aceptar el diseño del código como está dado y asumir los límites de su poder

regulatorio, la ley puede trabajar por promover un espacio de mayor regulabilidad, incidiendo en la constitución misma de la arquitectura de red.

Lessig (1998) considera al ciberespacio como un “poder soberano emergente” (p.7), sobre el cual los gobiernos deberían tomar conciencia y trabajar para reponer los límites y protecciones necesarios, como si se tratara de una nación soberana más. El autor considera que es necesario diseñar la arquitectura de red de acuerdo a los valores constitucionales que fundan las naciones soberanas y exigir límites y garantías equivalentes como en cualquier espacio democrático.

Al momento de presentar este ensayo, en el año 1998, el autor advertía sobre la tendencia de Internet en general hacia una mayor capacidad de control y rastreo de las actividades de los usuarios: “Pero en el ciberespacio, a diferencia del espacio real, esta supervisión, este rastreo, este control de la conducta será mucho menos caro. Este control se realizará en segundo plano, de forma eficaz e invisible” (Lessig, 1998, p.12). Según el autor, a un menor costo de las tecnologías de control, el usuario iría perdiendo autonomía y libertad en su capacidad de acción, de una manera casi imperceptible. Este poder, además, terminaría imponiéndose sobre el resto de los poderes soberanos locales, ya que el entorno de la red se volvería central en la vida social y económica. De esta manera, llama a los gobiernos, a los teóricos y políticos a reflexionar sobre el rol preponderante de la arquitectura de la red en la regulación y control de la conducta y la necesidad de investirla de los elementos necesarios para preservar la libertad y derechos fundamentales del usuario.

Una vez desarrollado el análisis de Facebook como red social y plataforma de publicidad en el capítulo 3, daremos cuenta en el siguiente capítulo de la evolución del marco regulatorio europeo en relación a las operaciones de tratamiento de los datos personales. Recurriremos al análisis del Reglamento General de Protección de Datos Personales de la UE para un posterior examen de las políticas de privacidad y condiciones de uso de Facebook: qué cambios se implementaron, qué principios y recomendaciones se adoptaron, de qué manera mutó el funcionamiento de la plataforma y sus prácticas publicitarias.

En relación a las tensiones que surgen al analizar la protección de los datos personales en redes sociales, retomaremos el trabajo de Helen Nissenbaum (2011), en el cual se propone el "marco de la integridad contextual" como un modelo para evaluar aquellos sistemas o tecnologías que provocan un conflicto de interés en relación a los límites de privacidad y la protección de datos personales.

Una idea central de la autora es el concepto de "flujo de información personal", entendiendo que, en cada contexto, el titular de los datos espera cierto tratamiento aceptable de sus datos

personales, lo cual relativiza el alcance de su protección y los límites a su intimidad impuestos, ya que mientras el tratamiento y uso de sus datos se dé en el marco de lo razonablemente esperable dentro de ese contexto, sería aceptado y validado por su titular.

Al introducir la variable de lo "razonablemente esperable" podemos vincular estos postulados con lo desarrollado anteriormente a partir de Van Dijck acerca de la evolución del concepto del "compartir" en el contexto de la red social Facebook. Bajo su mirada, se critica el trabajo discursivo de los representantes de Facebook a la hora de flexibilizar o forzar la amplitud de conceptos como los de "compartir" y "privacidad" para justificar los mecanismos de tratamiento de datos personales de la plataforma, vitales para su modelo de negocios. Resulta interesante poder reflexionar acerca de este punto, ya que, analizando el caso a partir del modelo de integridad contextual, podría validarse o no el funcionamiento y las políticas de privacidad y uso de datos de la red social en caso de enmarcarse dentro de los valores razonablemente esperables de sus usuarios. A estos planteos podría objetarse la complejidad de definir estos valores compartidos, considerando que sólo la plataforma de Facebook cuenta con 2450 millones de usuarios activos por mes[14].

Para Nissenbaum, el desafío radica en encontrar un modelo de análisis que permita dar respuestas a los reclamos sobre la privacidad y protección de datos sin obturar las capacidades de conexión y comunicación de Internet, pero no deja de reconocer el derecho a la privacidad como elemento fundamental de todo sistema social y político moralmente legítimo. Este es uno de los ejes que desarrollaremos a partir de nuestro análisis.

[14] Facebook Investor Relations (2019, 30 de octubre). *Facebook Reports Third Quarter 2019 Results.* Recuperado de https://s21.q4cdn.com/399680738/files/doc_financials/2019/q3/FB-Q3-2019-Earnings-Release.pdf

3. Facebook y el valor de los datos personales

En este apartado nos dedicaremos a estudiar la red social Facebook desde la perspectiva desarrollada por Van Dijck, particularmente en base a las dimensiones que se desprenden de su análisis: regímenes de Propiedad, Gobierno, Modelos de negocios, Tecnología, Usuarios y Contenido. Esto nos permitirá analizar su lógica particular de funcionamiento y entender el valor que los datos personales representan en ella.

La red social Facebook fue creada en Estados Unidos el 4 de febrero de 2004 por Mark Zuckerberg, Dustin Moskovitz, Chris Hughes y Eduardo Saverin. Originalmente fue pensada para un uso exclusivo dentro de la Universidad de Harvard, luego se expandió su acceso a las Universidades de Stanford, Columbia y Yale. De acuerdo a los datos provistos por la plataforma en su sitio de noticias Facebook *Newsroom*, el 1 de diciembre de ese mismo año ya contaba con 1 millón de usuarios activos[15]. En los años siguientes continuó incorporando nuevas redes universitarias, escuelas secundarias, colegios internacionales y redes de trabajo hasta habilitar el registro en septiembre de 2006 para cualquier persona que tuviera una dirección de correo electrónico. Así lo anunció a través de un artículo redactado por una colaboradora, en el cual se advertía el valor de uso de la red social no sólo para los estudiantes o para aquellos que pertenecieran a una red de trabajo. En el artículo, también, se resaltaba el hecho de que la configuración de privacidad no sufriría alteraciones:

> Esto no significa que cualquiera pueda ver tu perfil, sin embargo. Tu perfil está tan cerrado como siempre lo estuvo. Nuestra estructura de red no va a desaparecer. Las universidades y las redes de trabajo aún requieren una dirección de correo electrónico autenticada para unirse. Solo las personas en tus redes y amigos confirmados pueden ver tu perfil. (Facebook, 2006)

Luego de ampliar sus posibilidades de registro, el número de usuarios activos de la plataforma se elevó a 12 millones en diciembre de 2006. Desde entonces, empezó a incorporar nuevas funcionalidades como la aplicación Marketplace para anuncios clasificados, en mayo de 2007; la plataforma de Facebook para celulares, en octubre de 2007; la plataforma de publicidad de autoservicio y las páginas de Facebook, en noviembre de 2007; el botón Me gusta, en febrero de 2009; la función de Grupos, en octubre de 2010, que permite la creación de comunidades cerradas o públicos con un número determinado de participantes; y también la función de videollamada, creando una alianza con la empresa Skype, en julio de 2011, entre otras[16].

[15] Facebook Newsroom (2016-2019). *Información de la empresa.* Recuperado de https://ltam.newsroom.fb.com/company-info/

[16] Facebook Newsroom (2016-2019). *Información de la empresa.* Recuperado de https://ltam.newsroom.fb.com/company-info/

La corporación continuó expandiéndose con la adquisición de nuevas plataformas. En abril de 2012 ejecutó la compra de la red social Instagram por 1000 millones de dólares[17], realizó su oferta pública de venta en mayo de ese mismo año y adquirió el servicio de mensajería WhatsApp en febrero de 2014, por la suma total de 22 000 millones de dólares[18]. También fue incorporando nuevas funcionalidades, desde el servicio de chat y videollamada Messenger, la solicitud de servicio de transporte llamada Transportation en Messenger, hasta la posibilidad de registrarse como donante de sangre para los usuarios de India. Las últimas cifras publicadas por la empresa declaran 2450 millones de usuarios activos al 30 de septiembre de 2019 en Facebook[19] y más de 400 millones de usuarios activos por mes en Instagram en el año 2015.

3.1 Régimen de Propiedad

Estudiar el régimen de propiedad de una plataforma permite analizar su funcionamiento como un "sistema de producción" (Van Dijck, 2016, p.39). Su composición permite identificar los valores que guían su desenvolvimiento y objetivos empresariales. En el caso de Facebook, se trata de un sistema de producción caracterizado por el rol preponderante de las Tecnologías de la Información y la Comunicación, cuya característica principal consiste en estar centrado en el procesamiento de la información: "La información constituye tanto la materia prima como el producto" (Castells, 1995, p.10). Esto genera un gran impacto sobre los procesos de desarrollo más que sobre el producto final, influyendo, además, en el resto de las esferas de interacción social:

> Porque los procesos, a diferencia de los productos, se incorporan a todas las esferas de la actividad humana, y su transformación por dichas tecnologías, centrándose en los omnipresentes flujos de la información, conduce a una modificación en la base material de la organización social en su conjunto (Castells, 1995, p.11)

Como hemos visto, Facebook fue lanzada en 2004 por un grupo de estudiantes cuyo fin inicial se restringía al uso exclusivo dentro de su universidad. Luego fue ampliando su alcance y permisos de acceso, pero conservando su limitación al ámbito académico. Hasta 2012 fue propiedad de Facebook Inc, año en que la empresa abrió las puertas a capitales inversores a través de la oferta pública de acciones. Sin embargo, en la actualidad, el mayor accionista

[17] Facebook compró Instagram por 1000 millones de dólares. (2012, 9 de abril). *La Nación.* Recuperado de https://www.lanacion.com.ar/tecnologia/facebook-compro-instagram-nid1463518

[18] Aprueban la compra de WhatsApp por Facebook: 22 000 millones de dólares. (2014, 6 de octubre). *La Nación.* Recuperado de https://www.lanacion.com.ar/tecnologia/aprueban-la-compra-de-whatsapp-por-facebook-22000-millones-de-dolares-nid1733420

[19] Facebook (2019, 30 de octubre). *Facebook Reports Third Quarter 2019 Results.* Recuperado de https://s21.q4cdn.com/399680738/files/doc_financials/2019/q3/FB-Q3-2019-Earnings-Release.pdf

de la compañía continúa siendo uno de sus fundadores y Director Ejecutivo, Mark Zuckerberg, quien además controla la mayor parte de las acciones de clase B, que equivalen a 10 votos cada una frente a las acciones de clase A, que representan un voto por unidad. Otros de sus fundadores, Eduardo Saverin y Dustin Moskovitz, también controlan gran parte del paquete accionario, mientras que el resto de los principales propietarios individuales pertenecen o han pertenecido a la estructura corporativa de Facebook: Jan Koum, el fundador y ex CEO de WhatsApp y ex miembro de la junta de Facebook, Sheryl Sandberg, la Directora de Operaciones de Facebook y Michael Schroepfer, el Director de Tecnología de Facebook[20].

También participan del régimen de Propiedad de la empresa grandes Fondos de Inversión, los cuales podemos encontrar detallados en el siguiente cuadro:

Accionistas

Nombre	Acciones	%
Vanguard Group, Inc.	179,302,593	7,45%
Fidelity Management & Research Co.	115,540,678	4.80%
T. Rowe Price Associates, Inc. (Gestión de inversiones)	104,115,861	4,33%
SSgA Funds Management, Inc.	93,435,833	3.88%
Capital Research & Management Co. (Inversores globales)	72,701,753	3,02%
BlackRock Fund Advisors	59,233,113	2,46%
Capital Research & Management Co. (Inversores internacionales)	44,408,046	1,85%
Capital Research & Management Co. (Inversores mundiales)	44.294.899	1,84%
Geode Capital Management LLC	33,178,690	1,38%
Northern Trust Investments, Inc. (Gestión de inversiones)	27,896,730	1,16%

Figura 1: ***Accionistas de Facebook.*** **Listado de los principales Fondos de Inversión que participan del paquete accionario de la empresa.** Recuperado de https://www.marketscreener.com/FACEBOOK-10547141/company/

En la práctica, esta estructura otorga un gran poder en la toma de decisiones al principal accionista, Mark Zuckerberg, ya que una posición unánime del resto de los accionistas no logra imponerse sobre su voluntad, dado su control mayoritario de acciones. Luego de las acusaciones de filtración de datos que provocaron un descenso del valor de las acciones de Facebook, sus accionistas presentaron distintas propuestas para desplazar a Zuckerberg de su cargo ejecutivo, pero ninguna ha podido prosperar sin su aprobación[21].

Esta demanda de sus accionistas permite vislumbrar cómo la apertura de la empresa para la cotización en bolsa implica una mayor presión para incrementar las posibilidades de

[20] Maverick, J. (2019, 25 de noviembre). The Top 6 Shareholders of Facebook. *Investopedia.* Recuperado de https://www.investopedia.com/articles/insights/082216/top-9-shareholders-facebook-fb.asp

[21] Facebook: accionistas votaron en masa para echar a Zuckerberg (2019, 4 de junio). *El economista.* Recuperado de https://www.eleconomista.com.ar/2019-06-facebook-accionistas-votaron-en-masa-para-echar-a-zuckerberg/

monetización de su plataforma. Detrás del discurso de transparencia y flexibilidad en el "compartir", se sustenta una lógica de negocios centrada en la explotación de la información personal del usuario para construir una sólida plataforma de publicidad online, sobre la que el negocio de Facebook se sostiene (Fumagalli et. al., 2018). Este modelo determina el valor de las plataformas digitales, cuyo activo principal está dado por la cantidad de usuarios activos y la gran cantidad de datos que proveen a la empresa para su aprovechamiento.

Las plataformas digitales orientan sus estrategias comerciales a incrementar este número de usuarios, a incorporar nuevas funcionalidades a su entorno y mejorar las técnicas de recolección y procesamiento de datos. Facebook ha llevado adelante la adquisición de 65 compañías que pueden agruparse, según Fumagalli et. al. (2018), en cuatro categorías diferentes de acuerdo a los objetivos comerciales que las motivaron.

Un primer grupo de adquisiciones se vincula a las mejoras implementadas en el nivel de la Tecnología - siguiendo a Van Dijck - y en el nivel del Código - según Lessig -, que permite a la empresa incorporar funcionalidades para la actividad del usuario en línea y como nuevas oportunidades de recolección y análisis de datos, como el agregador de noticias *FriendFeed* que incorpora el botón *like* o "Me gusta" y atribuye las características de la página de inicio de los usuarios de Facebook que funciona como "Sección de Noticias" o *News Feed,* donde se muestran las publicaciones más recientes de los "amigos" y páginas de empresas a las que "sigue" de acuerdo a una lógica de relevancia para el usuario.

Un segundo grupo de adquisiciones, que también opera en el nivel de la Tecnología y el Código, responde a la necesidad de la empresa de optimizar su plataforma para el uso en dispositivos móviles o *smartphones*, a través de los cuales creó la versión Facebook Mobile y el servicio de mensajería Facebook Messenger, que funciona como una aplicación paralela a la plataforma de Facebook. En esta categoría los autores incluyen también las adquisiciones ya mencionadas de la red social Instagram por mil millones de dólares y la aplicación de mensajería WhatsApp por 22 000 millones de dólares.

El tercer grupo se vincula directamente a su Modelo de negocios, que permitió a la empresa implementar el modelo de ingresos por publicidad, a partir de la incorporación de herramientas de medición de rendimiento, técnicas de rastreo y la asociación con proveedores de datos de terceros para un mayor enriquecimiento de sus bases de datos y análisis de los metadatos.

El cuarto grupo de compañías absorbidas por Facebook se orienta a un objetivo de diversificación de su Modelo de negocios, pero que continúa vinculado al sector de la publicidad. Podemos mencionar, entre otros: "La compañía de tecnología de realidad virtual, Oculus VR; la compañía de aplicaciones de rastreo de la salud y entrenamiento ProtoGeo; y

Ascenta, el fabricante de drones con energía solar del Reino Unido" (Fumagalli et. al., 2018, p.20).

También ha llevado adelante algunos procesos de asociación, que consisten en convenios con otras empresas de servicios digitales para acceder al flujo de datos de sus usuarios, por medio del intercambio de botones como el "Me gusta" o permitiendo el registro en la plataforma a partir de una cuenta ya creada en Facebook, como es el caso de su asociación con la plataforma de distribución de contenidos musicales Spotify (Van Dijck, 2016, p.40). También se desarrollan procesos de integración verticales, que implican una alianza de la plataforma digital con un medio masivo de comunicación tradicional. Facebook ha experimentado en este sentido colaborando con la cadena NBC para transmitir la cobertura del canal de los Juegos Olímpicos de 2012 desde su interfaz (Van Dijck, 2016, p.40) y acordando con diarios como *The New York Times* para la difusión de artículos periodísticos[22].

Para Van Dijck (2016), es de suma importancia realizar un recorrido por las alianzas e integraciones comerciales que las plataformas llevan adelante para advertir las relaciones de poder que dan forma al ecosistema general de medios digitales. Se trata de un entramado de empresas centradas en la apropiación de los procesos sociales que se generan dentro de sus plataformas. Siguiendo a Fumagalli et. al. (2018), vemos como "las facultades humanas, desde las relacionales-lingüísticas a las afectivas-sensoriales" y las "emociones personales" (p.25) que circulan a través de la actividad en línea de los usuarios, son procesadas de manera sistemática por estas plataformas para la creación de valor de cambio.

Identificar los propietarios que encabezan estos procesos permite comprender en qué manos recae el control de la información personal, quienes asumen el rol de responsables o encargados del tratamiento de los datos de millones de usuarios que interactúan en estos entornos y bajo qué principios y garantías lo hacen.

3.2 Lógica de Gobierno

El Gobierno de las plataformas está compuesto por las reglas y protocolos que definen un entorno digital específico y guían la conducta de los usuarios en él. Existen, por un lado, los protocolos técnicos, relacionados íntimamente con el nivel de la Tecnología y las restricciones del Código (Lessig, 1998) y los protocolos sociales, que son normas explícitas e implícitas que modelan el comportamiento del usuario, determinando niveles de conducta aceptables y

[22] Alianza de medios de comunicación con Facebook genera ansiedad y esperanza. (2015, 14 de mayo). *La Vanguardia.* Recuperado de https://www.lavanguardia.com/tecnologia/20150513/54431226234/alianza-de-medios-de-comunicacion-con-facebook-genera-ansiedad-y-esperanza.html

regulando sobre cuestiones relacionadas al tráfico de los contenidos, como la privacidad y la propiedad intelectual (Van Dijck, 2016).

En el caso de Facebook, podemos advertir este tipo de normas explícitas en las políticas de privacidad y condiciones de uso que toda persona debe aceptar de forma obligatoria para acceder a un perfil de usuario en la red social. Para hacerlo, se debe ingresar a su sitio web www.facebook.com y completar el formulario de registro con una serie de campos obligatorios, a través de los cuales el interesado deberá brindar los siguientes datos personales: nombre, apellido, número de celular o correo electrónico (se puede optar por el primero o el segundo, pero es obligatorio proveer al menos uno de ellos), fecha de nacimiento y sexo, en el cual se ofrecen las opciones “Mujer”, “Hombre” y “Personalizado”. Debajo de este formulario de registro y antes del botón “Registrarte” para confirmarlo, se introduce la siguiente leyenda: “Al hacer clic en "Registrarte", aceptas nuestras Condiciones, la Política de datos y la Política de cookies. Es posible que te enviemos notificaciones por SMS, que puedes desactivar cuando quieras”. Haciendo click sobre cada una de las frases destacadas el sitio redirige al usuario a otra ventana de navegación donde se presentan en detalle cada una de las políticas mencionadas, agrupadas de la siguiente manera:

1. Nuestros servicios
2. Nuestra política de datos y tus opciones de privacidad
3. Tus compromisos con Facebook y nuestra comunidad
4. Disposiciones adicionales
5. Otras condiciones y Políticas que se pueden aplicar a tu caso: Controles de anuncios de Facebook, Aspectos básicos de la privacidad, Política de cookies, Política de datos.

Sobre este tipo de normas, Van Dijck (2016) señala que la gran mayoría de los usuarios confirma expresamente su aceptación sin realizar una lectura atenta de ellas. Quien desee registrarse en Facebook podrá hacer click en el botón “Registrarte” sin siquiera haber accedido al sitio donde se alojan las disposiciones de uso - las cuales, para la autora, son de naturaleza “intrincada y extensa” (Van Dijck, 2016, p.41).

Estas normas establecen una relación contractual entre el usuario y la plataforma, mediante la cual el usuario se compromete a ceder a las restricciones y limitaciones impuestas a cambio del servicio otorgado por la red social, pero no tienen fuerza de ley. En muchos casos, esto puede generar tensiones entre lo que se encuentra sancionado por ley y lo que el usuario está dispuesto a ceder por el uso de la plataforma. Para la autora, en este tipo de disposiciones se dirimen cuestiones centrales relacionadas al uso de la plataforma y el rol asignado a los usuarios, que en muchos casos ya cuentan con leyes que regulan sobre el tema.

En este sentido, es interesante retomar los planteos de Lessig (1998) respecto al rol que debería ocupar la ley como restricción para incidir en la naturaleza propia del Código. Para el autor, la ley debe poder traducir los valores constitucionales de una sociedad democrática también al entorno del ciberespacio. Esto implicaría, en base a lo desarrollado anteriormente, que los derechos consagrados constitucionalmente con leyes especiales que los amparan como el derecho a la privacidad y a la protección de datos personales, formen parte también de la arquitectura de la red como valores fundamentales para su funcionamiento. Que estos valores y límites sancionados puedan traducirse no sólo en los protocolos técnicos y sociales que dan forma a la plataforma sino también en las normas sociales que guían la conducta del usuario, a través de sus propias expectativas y grados de aceptación sobre el comportamiento reforzaría la existencia de un entorno digital que proteja estos derechos y conciba al usuario como centro. Se ponen en juego tanto la voluntad y negociación política a través de la ley, como los valores construidos culturalmente sobre el uso de las redes sociales (retomando la idea de Van Dijck sobre lo que el usuario está dispuesto a ceder por conseguir su participación en este tipo de plataformas), los protocolos sociales y técnicos que dan forma al Código de la red social tal cual la conocemos, y también cuestiones relacionadas a la fuerza del mercado. Este trabajo se centrará particularmente en el rol que ejerce la ley para promover una mayor regulabilidad del ciberespacio, específicamente, en el ámbito de las redes sociales.

3.3 Modelo de Negocios: El valor de los datos personales para su funcionamiento

Facebook se basa en un modelo de servicio sostenido principalmente por los ingresos por publicidad. El éxito en el proceso de monetización radica en el uso de la información provista por los usuarios y los metadatos consecuentes de sus acciones en la plataforma, que permiten trazar patrones de comportamiento, hábitos de consumo, intereses, perfiles sociodemográficos e identificar momentos clave en la vida de cada usuario (como el nacimiento de un hijo o la celebración de una boda). Esto posibilita un nivel de acceso a la información personal de los consumidores de altísimo valor para las empresas oferentes de productos y servicios.

De acuerdo con los planteos de Van Dijck, Facebook logró construir sus estrategias de monetización luego de varios años de consolidar el tamaño de su plataforma, tanto en el volumen creciente de usuarios como en su nivel de actividad e interacción en línea. Esto ha permitido a la red social comercializar todo su entorno a partir de la venta de espacios publicitarios y la incorporación de otras aplicaciones y servicios de pago que se ejecutan a través de ella o valiéndose de ella como herramienta de registro.

Fumagalli et. al. (2018) enmarcan este modelo de negocios dentro de la economía de plataformas, entendida como una nueva forma de acumulación del capital centrada en la recolección de información personal y su transformación en valor:

> En la emergente economía de las plataformas digitales, los datos son el resultado final que luego se realiza en los mercados globales de la comunicación y la publicidad, originando un "valor de red" como resultado de un proceso continuo y dinámico de interacción entre trabajo (labour) humano y lingüístico y las infraestructuras digitalizadas (las plataformas). (p.15)

Para los autores, se trata de un modelo de producción centrado en la explotación de las relaciones humanas y el trabajo no asalariado de los usuarios en la plataforma. Este proceso de creación de valor comienza con la oferta de servicios por parte de Facebook. Los usuarios pueden acceder completando el formulario obligatorio de registro y aceptando las condiciones de uso y políticas de privacidad, cediendo entonces a las restricciones impuestas en su Lógica de Gobierno. Desde el momento en que ingresan a la plataforma, los usuarios proveen a la empresa todo tipo de información rastreable de su actividad en línea, como sus datos personales, el contenido que producen, las publicaciones con las que interactúan, las páginas de empresas a las que "siguen", entre otros. Facebook recopila esta gran masa de datos, la integra, la analiza y la entrecruza con bases de datos de terceros, consolidando así el proceso de producción de valor a partir de la materia prima provista por los usuarios.

En este punto, ingresa otro actor fundamental para el modelo de negocios: los anunciantes. La empresa brinda una plataforma específica para la auto-gestión de campañas publicitarias, llamada Facebook *Ads Manager* o Administrador de Anuncios de Facebook[23]. Para acceder a este servicio, el usuario debe crear una cuenta en la plataforma para negocios de Facebook *Business Manager,* a través de la cual podrá administrar su página y campañas publicitarias (también podrá hacerlo mediante terceros, como por ejemplo, agencias de marketing, ya que la plataforma brinda distintos niveles de acceso según el rol asignado a cada usuario dentro del negocio). A través de esta funcionalidad específica para el uso comercial de la plataforma, los anunciantes compran espacios publicitarios dentro del entorno de Facebook (incluidas la plataforma de Messenger e Instagram) para que sus anuncios se muestren a los usuarios mientras navegan en la red social y también fuera de ella, a través de la herramienta Facebook *Audience Network* (FAN), incorporada en el año 2014: "FAN es una red enfocada a teléfonos móviles que provee a los anunciantes nuevas formas de extender sus campañas fuera de los límites de Facebook mismo, aprovechando el inigualable tesoro escondido de información personal de Facebook" (Fumagalli et. al., 2018, p.21). Esta plataforma involucra

[23] Facebook para empresas (2019). *Guía para principiantes*. *Información sobre el administrador de anuncios de Facebook.* Recuperado de https://www.facebook.com/business/help/200000840044554?id=802745156580214

a los desarrolladores de sitios web y aplicaciones, que pueden comercializar sus activos digitales ofreciéndolos como un espacio de visualización más para los anuncios creados a partir de la herramienta de Facebook.

El anunciante no paga un valor adicional por este servicio, sino que configura la campaña con un presupuesto y duración estimados y el monto total gastado no excede el tope determinado. Una vez que los anuncios entran en circulación, ingresan a un sistema de subasta con el resto de los anunciantes y según el puntaje que asigne la plataforma serán mostrados en los espacios disponibles, teniendo en cuenta: la puja máxima que el anunciante esté dispuesto a pagar para conseguir un espacio, la relevancia de la pieza gráfica y/o audiovisual para el usuario (que Facebook determina mediante un puntaje del 1 al 10) y la tasa estimada de demanda, que calcula las probabilidades de que la audiencia potencial del anuncio realice la acción para la cual es interpelada.

El gran aporte de Facebook a este ecosistema es el valor creado a partir de la información personal de los usuarios, que le permite ofrecer a sus anunciantes sofisticadas herramientas de direccionamiento y personalización de sus campañas, además del análisis en tiempo real del rendimiento y entrega de sus anuncios. Para crear una audiencia específica, el anunciante puede segmentar por ubicación geográfica, por edad, por género, por idiomas, por dispositivo y sistema operativo utilizados, por intereses, por datos demográficos y por datos de comportamiento.

Otro gran valor construido es el uso del botón “Me gusta” en sitios de terceros, a través del cual recaban grandes volúmenes de información y datos sobre el comportamiento de los usuarios, ya no exclusivamente dentro de Facebook sino en el resto de los sitios web, enriqueciendo aún más la información ya recopilada tanto en volumen como en la distinción refinada de intereses, gustos, comportamiento, operaciones de compra y venta, entre otros. Van Dijck (2016), además, enfatiza el hecho de que la plataforma se ha mantenido firme en preservar la confidencialidad de sus algoritmos, ocultando o invisibilizando las lógicas de recolección y análisis de datos, de entrecruzamiento con otras bases de datos, transferencias a terceros y finalidades. En este punto nos interesa profundizar, ya que apenas unos años después de que la autora escribiera *La cultura de la conectividad,* con la entrada en vigencia del RGPD se advierten numerosos cambios sobre la información que Facebook provee a sus usuarios e interesados en acceder a su plataforma. Desarrollaremos en profundidad estos cambios en nuestro trabajo, analizando las políticas de privacidad y condiciones de uso de la red social y vinculándolas con la normativa vigente.

3.4 Tecnología

Analizar la dimensión tecnológica de una plataforma permite identificar los modos en que codifica las actividades sociales del usuario. Ya hemos advertido cómo la Lógica de Gobierno opera como restricción a la conducta del usuario a través de normas explícitas e implícitas. Esta lógica también se traduce en su dimensión tecnológica, configurando un campo de acción particular para el usuario entre múltiples escenarios posibles.

Van Dijck (2016) advierte dos mecanismos de codificación en la Tecnología de Facebook que responden al doble significado de “compartir” que la autora propone. Como hemos visto, la autora realiza una distinción entre los conceptos de conexión y conectividad como elementos constitutivos de este doble sentido. Esta distinción permite identificar, por un lado, todos los mecanismos de la interfaz visible que fomentan la conexión entre usuarios y el intercambio de información personal al mayor nivel posible de exposición. Estos mecanismos establecen por defecto el formato y la organización de la información de los perfiles personales de cada usuario, que deben incluir obligatoriamente su nombre y apellido, una foto, su correo electrónico, fecha de nacimiento y sexo. Esta información puede mostrarse de manera “pública”, es decir, visible para todos los miembros de Facebook y como resultado en los motores de búsqueda, restringirse a los “amigos” del usuario, a algunas personas específicas, o puede incluirse también a los “amigos” de sus contactos. El usuario tiene posibilidades de modificar la configuración de privacidad de su página, ingresando a la herramienta de “Configuración y herramientas de privacidad”, desde donde puede limitar la visualización de su información de perfil y publicaciones. Cabe señalar, sin embargo, que no se trata de una acción que pueda realizarse de manera sencilla: cada elemento que forma parte del perfil del usuario debe revisarse por separado y también los cambios en la configuración de privacidad que se desee realizar en cada uno de ellos. De esta manera, se advierte la importancia de la acción del usuario y su nivel de conocimiento sobre los límites y posibilidades de privacidad y la protección que puede ejercer sobre ella dentro de la plataforma. Es necesario destacar, además, que tanto para el nombre y apellido como para la foto visible de perfil no es posible restringir el acceso público.

En relación al concepto de conectividad, según el cual Van Dijck (2016) hace referencia a la lógica de compartir la información personal y datos de comportamiento de los usuarios con terceros, la autora identifica los distintos elementos que la red social fue incorporando desde que abandonó su restricción al ámbito educativo y permitió el acceso a nivel global para facilitar su estrategia de monetización. En este sentido, la plataforma implementó mecanismos de recolección, análisis y procesamiento de datos para la transformación de la información personal en valor de cambio (Fumagalli et. al., 2018). Dentro de este grupo

podemos mencionar el botón “Me gusta”, mencionado anteriormente, y el botón de “Iniciar sesión”, un elemento exportado del entorno específico de Facebook para ser utilizado como herramienta de registro para el uso de aplicaciones de terceros u otros sitios web, los cuales facilitan la recolección de información sobre los intereses y comportamiento del usuario tanto dentro como fuera del entorno de facebook.

Los datos que aportan este tipo de elementos, sumados a la información generada por los usuarios dentro de la plataforma y la asociación de Facebook con proveedores de datos de terceros, constituyen la materia prima sobre la cual operan las técnicas de procesamiento de la información y personalización. Éstas, en el nivel de la Tecnología, organizan el contenido de las “páginas de inicio” de los usuarios, para crear un entorno visible alineado con sus intereses, con sus pautas de comportamiento y el nivel de interacción con sus “amigos” y páginas de empresas, servicios o figuras públicas con las que frecuenta[24].

Nos ocuparemos de las normas explícitas de la plataforma sobre la privacidad y la protección de datos personales en el desarrollo de este trabajo, para reflexionar sobre los niveles de protección que la plataforma propone en su diseño y protocolos técnicos y en su lógica de gobierno, y si éstos cumplen o no, y en qué medida, con las leyes que protegen estos derechos fundamentales.

3.5 Usuarios

Al considerar esta dimensión, Van Dijck (2016) advierte el rol particular que ejerce el usuario, no solo como consumidor o receptor sino también como productor y generador de contenidos, como un partícipe más de la compleja trama de interacción social, datos e información personal que constituye la red social. Podemos vincular esta conclusión con el concepto de Prosumidor propuesto por Fumagalli et. al. (2018), quienes consideran al usuario como una fuerza productiva clave en el sistema de producción de valor del capitalismo de plataformas: “Son los usuarios, interactuando con las plataformas, mediantes las cuales se comunican y entablan diversas formas de relaciones, los que suministran la materia prima que es subsumida luego por la organización productiva del capital” (p.29).

Considerando al usuario según la figura del Prosumidor, advertimos dos campos de acción posibles. El primero está relacionado con el uso del servicio ofrecido por Facebook y el aprovechamiento de todas sus funcionalidades. Esta red social ofrece al usuario la capacidad de conectarse con su red de “amigos”, crear una identidad en línea y la posibilidad de involucrarse en grupos y pertenecer a una comunidad. La plataforma se ha consolidado como

[24] Boyd, J. (2018, 2 de agosto). El algoritmo de Facebook, explicado en detalle. *Brandwatch.* Recuperado de https://www.brandwatch.com/es/blog/algoritmo-facebook/

un espacio de disputa por el capital social, alimentado por la presión de los usuarios a pertenecer a la red social y permanecer en ella, y a adquirir cierto grado de popularidad entre sus pares (Van Dijck, 2016). Teniendo en cuenta la multiplicidad de acciones que los usuarios pueden realizar a través de ella, como iniciar conversaciones privadas con “amigos”, leer artículos periodísticos, visualizar videos con fines de entretenimiento, publicar fotos o adquirir un producto o servicio, podemos advertir el nivel de penetración de la plataforma en la vida social de cada miembro.

Un segundo campo de acción se vincula directamente con la figura del usuario ejerciendo el rol de productor o generador de contenidos, como proveedor de los datos como materia prima para consolidar el modelo de negocios de Facebook actual. Como hemos visto, la misma plataforma que provee un variado universo de posibilidades de acción e interacción, también incorpora una serie de protocolos y reglas que limitan y guían su comportamiento para ejercer el control sobre la información y un tratamiento sistemático sobre ella. Su Tecnología incorpora tanto los elementos necesarios para fomentar la participación del usuario en la red social como las técnicas de recolección y análisis de este volumen de información. Esto garantiza el éxito de su comercialización, ya que no sólo depende de la información personal y los datos que el usuario provee al interactuar a través de ella, sino también de su capacidad de atención; es necesario que el usuario encuentre atractiva la plataforma y decida permanecer en ella, para que pueda también interactuar con los anuncios publicitarios que allí se distribuyen como cierre del ciclo productivo.

En su análisis, Van Dijck (2016) se centra en estudiar el rol de los usuarios en relación a los cambios implementados por Facebook en sus condiciones de uso e interfaz a lo largo del tiempo. La autora entiende que este tipo de modificaciones posibilita espacios de negociación entre lo que la plataforma impone a través de su Lógica de Gobierno y la apropiación o refutación del usuario ante dichos cambios. Estas reacciones se traducen en el uso efectivo por parte del usuario de la plataforma y pueden adoptar distintas formas de apropiación o desafío. Entre las formas en que el usuario expresa su descontento podemos mencionar las prácticas de hackeo a su Tecnología hasta el abandono de la red social por una equivalente. Los usuarios también se han organizado históricamente para manifestarse frente a la arbitrariedad de estos cambios en foros y grupos de Facebook, apropiándose de las funcionalidades de la plataforma para incidir sobre su funcionamiento:

> Si bien la gran mayoría de los usuarios de Facebook manifiesta su conformidad con los protocolos de socialidad online del sitio – que, después de todo, benefician su interés personal –, una parte sustancial de sus miembros reconoce distintas preocupaciones acerca del modo en que sus datos son utilizados. Un grupo de usuarios pequeño pero muy

> interesado en hacer oír su voz ha objetado de manera explícita los distintos cambios en las funciones de la interfaz del sitio. (Van Dijck, 2016, p.55)

Este tipo de reacciones son advertidas por la autora como un espacio de acción posible de los usuarios para pujar por la definición de las reglas de uso de las plataformas. Esta conclusión invita a pensar en el rol del usuario como sujeto crítico de su condición y partícipe del entramado de las redes sociales: “Las actitudes de los usuarios dan cuenta de un ámbito de disputa mucho más amplio entre sus intereses y los de los propietarios en torno al control de la información” (Van Dijck, 2016, p.57). Para los fines de este trabajo, es importante advertir la capacidad de acción del usuario frente a las políticas de privacidad impuestas por la red social. Este espacio de negociación o disputa debe analizarse además considerando las herramientas que la ley contempla para garantizar una efectiva protección de los datos personales.

3.6 Contenido

El contenido que circula en las redes sociales forma parte de los insumos necesarios para poner en funcionamiento su modelo de negocios. Se trata de producciones en múltiples formatos generadas por los usuarios, que retroalimentan su lógica de creación de valor a partir del uso de los datos.

Para Van Dijck (2016), la dimensión del contenido no pertenece exclusivamente a los lazos generados entre usuarios ni a la esfera del uso y consumo de las plataformas, sino que representa para cada empresa un elemento constitutivo de sus sistemas de producción de valor: el contenido cultural y los diferentes niveles de interacción que acompañan su circulación permiten trazar perfiles de usuario, patrones de comportamiento y tendencias sociales.

En Facebook, particularmente, podemos encontrar contenido compartido por los usuarios en formato de fotos y videos, sobre los que todos los “amigos” del usuario pueden interactuar, ya sea dejando un comentario de manera textual o incluyendo imágenes animadas o emoticones, o “reaccionando” al contenido. La “Reacción” es una función específica de Facebook que permite al usuario expresar sus sentimientos respecto al contenido que visualizó, limitada a las siguientes opciones: “Me gusta”, “Me encanta”, “Me divierte”, “Me sorprende”, “Me entristece” y “Me enoja”. Esta función estuvo disponible a nivel global a partir de 2016 (Krug, 2016). Previo a esta implementación, sólo era posible reaccionar a través del ya mencionado botón “Me gusta”.

Figura 2: ***Reacciones de Facebook.*** Recuperado de www.facebook.com

Para los formatos de video, Facebook cuenta, además, con la función de Videos en Vivo, que permite al usuario realizar una transmisión audiovisual en tiempo real desde su dispositivo móvil, a la cual se pueden incorporar sus “amigos” como espectadores, reaccionar y dejar comentarios. También desarrolló, en 2017, una interfaz específica dentro de su plataforma para la visualización de *shows*, eventos en vivo y videos de mayor duración, llamada Facebook *Watch*, la cual fomenta su alianza con otros medios para la generación y distribución de contenido.

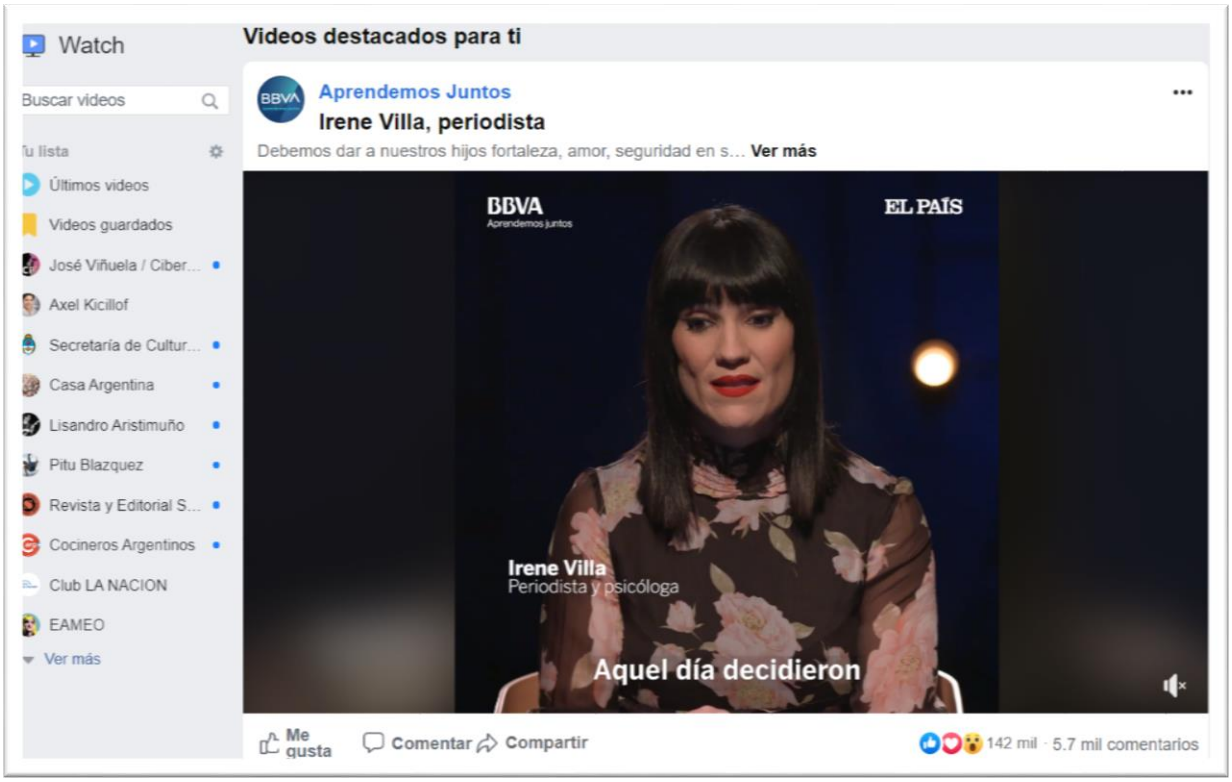


Figura 3: ***Facebook Watch.*** Recuperado de https://www.facebook.com/watch

Los usuarios también generan contenido en formato de texto. Una variante de ello son los fragmentos de texto en sus propios perfiles denominados “Estados”, en los que el usuario es invitado por default a comunicar a su red de contactos “en qué está pensando” (Figura 4). Además, entablan conversaciones privadas con sus contactos a través del servicio de mensajería Facebook Messenger.

Figura 4: ***Estados de Facebook.*** Recuperado de www.facebook.com

Todos los contenidos generados por los usuarios se organizan por orden cronológico en sus páginas personales, denominadas como “Biografías” o *Timeline* en inglés (línea de tiempo). Este concepto, para Van Dijck, convoca al usuario a involucrarse desde un plano aún más íntimo que las versiones anteriores de la plataforma. Antes, el contenido se organizaba según una lógica similar a una base de datos:

> En los primeros años de esta plataforma, el contenido se organizaba en función de los contactos del usuario, las actualizaciones de noticias y amigos y las discusiones en curso. La interfaz de Facebook, según observa el investigador británico Garde-Hansen (2009: 141), se presentaba como una base de datos de usuarios y para usuarios, en la que "cada página de usuario funcionaba como una base de datos de su vida, haciendo de este sitio de red social una colección de colecciones y colectivos. (Van Dijck, 2016, p.57)

A partir de las modificaciones de su interfaz por otra que apela a la organización del contenido según una lógica narrativa, la plataforma refuerza la presencia de emociones y una fuerte conexión del usuario con su vida personal, invitando a los usuarios a compartir "Acontecimientos importantes" sobre categorías como Trabajo, Relaciones, Estudios, Hogar y Vivienda, entre otros, que permiten al usuario publicar hitos de su vida personal, como el ingreso a un nuevo puesto de trabajo y en qué empresa, el inicio de una relación sentimental, la finalización de estudios o un cambio en el lugar de residencia.

Siguiendo esta lógica, la plataforma también introdujo la función de "Recuerdos"[25], en la que se le muestran al usuario publicaciones del pasado para que comparta nuevamente con sus "amigos" (Figura 5).

Figura 5: ***Tus recuerdos en Facebook*****.** Recuperado de **https://www.facebook.com/memories/?source=bookmark**

Todos estos cambios implican un salto cualitativo en cuanto al nivel de información personal provista por el usuario, que cada vez encuentra una mayor cantidad de llamadas a la acción para volcar su trayectoria biográfica en la red social. Estos elementos permiten a la plataforma refinar sus estrategias de personalización y segmentación de anuncios, ofreciendo a sus

[25] Hod, O. (2017, 25 de agosto). Facebook anuncia nuevas formas de disfrutar recuerdos con amigos. *Facebook Newsroom.* Recuperado de https://ltam.newsroom.fb.com/news/2017/08/facebook-anuncia-nuevas-formas-de-disfrutar-recuerdos-con-amigos/

anunciantes la capacidad de filtrar su audiencia por características demográficas como “padres recientes”, “padres con bebés pequeños”, empresa o sector donde trabajan y el cargo que ocupan, situación sentimental, nivel de formación y campos de estudio, mudanza reciente o “lejos de la ciudad de origen”, entre otras múltiples opciones.

El contenido y nivel de interacción de los usuarios con él permite también alimentar esta herramienta de personalización según los intereses y flujo de comportamiento. Estas características ofrecen las posibilidades de seleccionar una audiencia específica para campañas publicitarias en función de los intereses en temas como comida y bebidas, deportes, entretenimiento, familia y relaciones, negocios, moda, tecnología, o basadas en las intenciones o comportamiento del usuario como consumidor o comprador. Esta última dimensión incluye segmentos de usuarios agrupados por “afinidad multicultural”, clasificación de consumidores, personas que realizaron una compra o manifestaron la intención de realizarla, si se trata de viajeros frecuentes y, exclusivamente para el público de Estados Unidos, ofrece la opción de seleccionar a personas con probabilidad de interactuar con anuncios que contengan contenido político.

Otra funcionalidad que enriquece el volumen de contenido y la multiplicidad de acciones generadas por los usuarios dentro de la red social es la denominada como *Marketplace*, introducida en el año 2016, destinada específicamente a la compra y venta de productos y oferta de servicios.

Estas dimensiones específicas dentro del ecosistema de Facebook forman parte, además, de los espacios que la plataforma comercializa para la publicación de campañas publicitarias de terceros. La herramienta de creación de anuncios de Facebook permite configurarlos según las distintas variantes analizadas de contenido multimedia, de manera tal que se muestren como un elemento más de la interfaz e impacten de la manera menos invasiva en su actividad en línea.

El análisis detallado de cada elemento constitutivo de la plataforma nos permite comprender su lógica de funcionamiento, los intereses comerciales a los que responde y las consecuentes estrategias de comercialización. De esta manera, identificamos que la red social fomenta la creación de comunidades, de interacciones y generación de contenido en línea para conseguir la materia prima de su sistema de producción. Así es como advertimos el rol central que representa para la empresa la información personal de los usuarios y el tratamiento sistemático de datos personales a gran escala. Reconocer estas operaciones e identificarlas como una de las actividades principales de Facebook implica a su vez analizar los marcos regulatorios vigentes y el nivel de protección que proponen para los datos personales de los usuarios.

4. Marco regulatorio para la protección de los datos personales

Es importante desarrollar algunas cuestiones centrales que estructurarán el análisis del marco regulatorio. En principio, debemos considerar el derecho a la vida privada y el derecho a la protección de los datos personales como derechos autónomos (Cerda Silva, 2012).

Ambos derechos son consagrados a nivel internacional como derechos fundamentales. Podemos encontrar el derecho a la vida privada en el artículo 12 de la Declaración Universal de los Derechos Humanos (1948) y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966):

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

También podemos encontrar contemplado el derecho a la privacidad en el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre (1948): “Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar” y en el Artículo 11º, inciso 2 de la Convención Americana sobre Derechos Humanos (1969): “Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación”.

En la Unión Europea, podemos encontrarlos distinguidos en la Carta de los Derechos Fundamentales de la Unión Europea (2000), en la cual se contempla en el artículo 7 que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones” y, en el artículo 8, que “toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan”.

En Argentina, el derecho a la protección de los datos personales se encuentra reconocido a nivel constitucional a partir del artículo 43 de la Constitución Nacional y por la Ley 25.326 de Protección de Datos Personales.

Si bien en sus orígenes el derecho a la protección de los datos personales encontró sus fundamentos en el derecho a la intimidad y a la vida privada, a partir de los años ochenta tomó entidad propia, resguardando como bien jurídico la capacidad del individuo de controlar toda la información y datos vinculados a su persona, independientemente de su carácter privado o público:

> La protección de los datos personales satisface fines de interés público inherentes a una sociedad democrática. Dicha protección no solo evacúa la necesidad individual de quien

> quiere excluirse de la vida social, sino que también actúa como salvaguarda para el libre ejercicio de sus derechos. (Cerda Silva, 2012, p.166)

Es decir, el derecho a la protección de los datos personales no restringe su alcance a la esfera de lo privado, sino que su objeto es resguardar el principio de autodeterminación informativa o libertad informativa, garantizando la protección y el tratamiento legítimo de toda información personal. Esto no implica, sin embargo, que no existan consideraciones especiales para aquellos datos vinculados a la esfera más íntima de las personas. En este punto debemos profundizar sobre lo que entendemos por dato personal y diferenciarlo de las categorías especiales de datos personales que requieren un nivel de protección mayor.

Consideramos dato personal todo tipo de información vinculada a una persona. De acuerdo a las regulaciones específicas que abordaremos en este trabajo (la legislación europea y argentina sobre la protección de datos personales), la persona puede ser identificada o identificable, es decir, que se considerará como dato personal tanto la información que pueda ser vinculada de manera directa a un sujeto determinado como aquella que mediante un procedimiento adicional pueda vincularse a su titular. A su vez, ambos sistemas legislativos reservan un nivel de protección especial para aquellos datos que, en caso de ser tratados de manera ilícita, puedan representar un riesgo para el ejercicio de los derechos fundamentales de la persona. La legislación europea contempla este punto en el artículo 9 del RGPD sobre el “Tratamiento de categorías especiales de datos personales”, estableciendo la prohibición de cualquier operación de tratamiento sobre aquellos:

> (...) datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (RGPD, 2016, art.9)

Por su parte, la Ley 25.326 de Protección de Datos Personales argentina propone la definición de dato sensible para garantizar un nivel especial de protección a los “datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual” (Ley 25.326, 2000, art.2). Ningún sujeto puede verse obligado a proporcionar estos datos y se prohíbe además “la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles” (Ley 25.326, 2000, art.7). Se contemplan en ambos casos ciertas excepciones, para los casos en que intervengan cuestiones de interés público o fines estadísticos y/o científicos, siempre y cuando no sea posible establecer la identificación del titular de los datos.

A partir del reconocimiento de este nivel de protección especial, Cerda Silva (2012) destaca la importancia del derecho a la protección de datos personales como garante del ejercicio de otros derechos fundamentales: “Así, por ejemplo, al imponer limitaciones al tratamiento de datos relativos a nuestras opciones políticas, religiosas o sexuales, se fortalece el libre ejercicio del derecho de asociación, de la libertad de pensamiento y de la autodeterminación sexual, entre otros” (p.166). Es por esto que el autor discute con aquellas posturas que critican una amplitud excesiva de la definición del dato personal. Autores como Villegas Carrasquilla (2012) argumentan que el alcance del derecho a la protección de los datos debería limitarse a la información de carácter privado, que una definición más abarcativa obstruye el desarrollo tecnológico en general y las funciones de Internet y el mundo de las comunicaciones digitales en particular. Para Cerda Silva (2012), lo que se busca a partir de esta perspectiva es acotar la protección a los datos de carácter estrictamente privado en pos de una flexibilización de las condiciones de uso de las plataformas digitales:

> Los argumentos tendentes a socavar una protección adecuada a los datos personales han sido especialmente oficiosos cuando se los aplica a Internet; de hecho, han sido enarbolados con el propósito de brindar mayor flexibilidad a la prestación de servicios en línea. (p.166)

Se trate de información pública o privada, lo que el derecho a la protección de los datos personales garantiza al sujeto titular de los datos es el control sobre la información vinculada a su persona, sobre el tratamiento que se hace de ella, quién es responsable y con qué fines, además de resguardarse el derecho a acceder a esta información y rectificarla en caso de ser necesario.

Llegados a este punto, es menester definir con claridad qué entendemos por tratamiento de datos personales para una correcta interpretación del RGPD. Se considera como tratamiento de datos personales a todas las operaciones o procedimientos que se realicen sobre la información de carácter personal - ya sea de manera automatizada o realizados manualmente - “como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción” (RGPD, 2016, art.4).

La legislación argentina coincide en este sentido, dictaminando que podrán tratarse de procedimientos electrónicos o de carácter manual “que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión

a terceros a través de comunicaciones, consultas, interconexiones o transferencias" (Ley 25.326, 2000, art.2).

Advirtiendo las similitudes en ambos cuerpos legislativos, Cerda Silva (2012) consolida su posición respecto al alcance de la definición de dato personal y las críticas que apuntan a una mayor flexibilidad del mismo. Para el autor, restringir el alcance de las definiciones que hemos desarrollado implicaría también "un enorme retroceso en la armonización normativa internacional, un costo bastante elevado de cara a los efectos de la globalización" (Cerda Silva, 2012, p.171).

Por su parte, la Unión Europea contempla mecanismos para evaluar los niveles de protección en países terceros y organismos internacionales y dictaminar si cuentan con un nivel adecuado de protección. Esto favorece las transferencias internacionales de datos en un marco homogéneo de principios para su licitud y contención de riesgos. Cerda Silva (2011) analiza, en particular, el proceso a través del cual la Comisión Europea dictaminó que Argentina cuenta con un nivel adecuado de protección, garantizando que nuestra normativa vigente se adecúa a los principios estipulados a nivel europeo. Su análisis nos permitirá reflexionar en un apartado final sobre los vínculos existentes entre los principios europeos y las disposiciones contempladas en nuestro país, determinando de qué manera se asemejan unas con otras, si existe una armonización legal al respecto o no.

4.1 Reglamento General de Protección de Datos de la Unión Europea

Al analizar el marco regulatorio europeo es importante distinguir los diferentes actos legislativos que lo conforman. Algunos de ellos son vinculantes, otros aplican para todos los Estados miembros o para Estados u organismos específicos y tienen diferentes condiciones de aplicación y grado de obligatoriedad en su cumplimiento. Por un lado, debemos mencionar los Reglamentos que son vinculantes y deben aplicarse en el total de los países de la UE. También existen las Directivas, en las que se disponen ciertos objetivos obligatorios para todos los Estados miembros, pero que pueden ser aplicados internamente según la elaboración de sus propias leyes nacionales. Las Decisiones se dirigen específicamente a un país miembro o empresa y son de carácter vinculante, mientras que las Recomendaciones no lo son; si bien permiten sugerir líneas de acción sobre algún tema en particular, no son de aplicación obligatoria. Por último, los Dictámenes son instrumentos que permiten a las instituciones de la UE (Comisión, Consejo y Parlamento), el Comité de las Regiones y el Comité Económico y Social Europeo emitir un juicio o declaración sobre una temática, también de manera no vinculante.

Para los objetivos de este trabajo, nos centraremos en analizar los cambios introducidos por el Reglamento General de Protección de Datos de la UE - publicado el 27 de abril de 2016 y de aplicación obligatoria a partir de mayo de 2018 (en adelante, RGPD) - en la protección de los datos personales de las personas físicas. Este derecho está consagrado en el artículo 16 del Tratado de Funcionamiento de la Unión Europea y en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. A nivel internacional, el 28 de enero de 1981 se sancionó el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, al que Argentina suscribió como 54° estado parte en febrero de este año (los instrumentos de adhesión entraron en vigor el 1 de junio de 2019) y en el marco del cual ya ha participado de la 38° Reunión Plenaria, ya no como Estado observador.

El Convenio 108 advierte la necesidad de garantizar el derecho a la protección de los datos de carácter personal, dado el creciente flujo de intercambio de datos e información entre los Estados. Asume como objetivo garantizar el derecho a la vida privada a través de la protección de los datos de carácter personal “que son objeto de tratamientos automatizados”, para todos los Estados miembro del Consejo de Europa y para aquellos Estados no miembro que sean invitados a adherirse. Este instrumento comprende el “tratamiento automatizado” como las operaciones de registro, modificación, extracción o difusión de datos y la aplicación de operaciones lógicas sobre un conjunto de datos específico (Convenio 108, 1981, art.2). En su Protocolo adicional, sancionado en el año 2001, se contemplan las condiciones necesarias para la transferencia de datos de carácter personal a un tercero que no fuera alcanzado por las disposiciones del mencionado Convenio. Para estos casos, se establece que sólo pueda realizarse la transferencia del dato si el Estado u organización destinataria garantiza “un nivel de protección adecuado” (Protocolo adicional, 2001, art.2). Bajo estas condiciones, en 2003 la Argentina fue reconocida con un nivel adecuado de protección por la Comisión de las Comunidades Europeas.

Hasta la sanción del RGPD, podemos mencionar a su vez como parte del esquema legislativo para la protección de los datos personales de las personas físicas la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sancionada el 24 de octubre de 1995. Se vincula con la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Por otro lado, cabe destacar la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, sancionada el 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Cambios implementados

El RGPD entró en vigor el 25 de mayo de 2016, pero se estableció un plazo de dos años a partir de esta fecha para considerarse de cumplimiento obligatorio. Este Reglamento surgió como una propuesta de marco legal capaz de unificar las diferentes normativas de los Estados Miembros de la UE, desplazando todas las normas anteriores que no contemplaban sus principios y articulado. Previo a su sanción, en el ámbito de la protección de datos personales a nivel europeo se contaba con la Directiva 95/46/CE adoptada en 1995 por la UE, el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. En sus disposiciones finales, el RGPD estipula la derogación de la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.

En relación a la Directiva 2002/58/CE, debemos mencionar que este instrumento surge como complementario a la Directiva 95/46/CE para proteger el derecho a la intimidad y regular sobre el tratamiento de los datos personales específicamente en el ámbito de las comunicaciones electrónicas. A los efectos de adecuar esta disposición a la diversidad de servicios electrónicos prestados en la actualidad - los cuales representan un desafío constante para ser alcanzados en su totalidad por las definiciones de tratamiento de datos y datos personales ya consagradas en la legislación vigente -, se presentó en enero de 2017 una propuesta para un Reglamento específico de privacidad en el ámbito de las comunicaciones electrónicas[26], también conocido como Reglamento *e-privacy*[27]. Dado que aún no ha sido sancionado, no será objeto de desarrollo en el presente trabajo, por lo tanto nos enfocaremos en el RGPD como marco legal general para la protección de los datos personales. Respecto a las disposiciones de la Directiva 2002/58/CE, el RGPD establece que no impondrá nuevas obligaciones a las ya establecidas por esta Directiva.

Teniendo en cuenta estos antecedentes y considerando el caso de estudio seleccionado, debemos mencionar como actualizaciones novedosas que introduce el RGPD en la materia los siguientes elementos:

- **Ámbito territorial de aplicación**

En su artículo 3, el RGPD estipula un ámbito de aplicación mucho mayor que la Directiva 95/46/CE. Por un lado, contempla las operaciones de tratamiento de datos personales

[26] Puede consultarse el texto completo de la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

[27] El nuevo Reglamento sobre Privacidad y Comunicaciones Electrónicas (ePrivacy) en 8 claves. *Bluered.* Recuperado de https://bluered.es/blog/el-nuevo-reglamento-sobre-privacidad-y-comunicaciones-electronicas-eprivacy-en-8-claves/

realizadas por encargados o responsables establecidos en la UE. Pero además, amplía su alcance para todas las operaciones de tratamiento de datos personales cuyo titular resida en la UE, en tanto estas operaciones se vinculen con la oferta de bienes y servicios o el control de su comportamiento. Es decir, en este último caso, su alcance no depende de que las operaciones se realicen dentro o fuera de la Unión o de la localización de la empresa u organización encargada del tratamiento, sino que establece como prioridad la protección de los derechos fundamentales de los ciudadanos europeos como condición necesaria para su aplicación.

Esto impacta en el accionar de las empresas establecidas dentro y fuera de la UE, siempre que realicen operaciones de tratamiento de datos personales sobre ciudadanos europeos, vinculados a las actividades arriba mencionadas. Bajo estas condiciones, la red social Facebook se encuentra alcanzada por las disposiciones y obligaciones del RGPD para las operaciones de tratamiento de datos que realice sobre la información personal de los ciudadanos europeos, independientemente de la localización de su casa matriz, ya que entre sus actividades se destaca la oferta publicitaria de bienes y servicios y el seguimiento del comportamiento de los usuarios en la plataforma.

- **Consentimiento del interesado**

Tanto la Directiva como el RGPD consideran el consentimiento del interesado o titular de los datos como una de las condiciones para garantizar la licitud del tratamiento, si bien no es la única[28]. En el artículo 4 el RGPD amplía la definición de consentimiento contemplada por la Directiva 95/46/CE indicando que no sólo se considerará “toda manifestación de voluntad libre, específica, informada e inequívoca” sino que se estipula que sea realizada “mediante una declaración o una clara acción afirmativa”, es decir que no admite el consentimiento del interesado por omisión o de manera tácita, sino que debe existir una clara prueba de ello, ya que el responsable deberá poder demostrar la voluntad del interesado de aceptación y conformidad para el tratamiento de sus datos personales (tal como se estipula en las Condiciones para el consentimiento desarrolladas en el artículo 7). Es necesario destacar que el titular de datos posee el derecho de revocar este consentimiento en cualquier momento, y se establece que retirarlo sea tan sencillo como brindarlo.

Otra novedad a señalar son las condiciones específicas en relación al consentimiento del niño para los servicios de la sociedad de la información, contempladas en el artículo 8. Sólo se

[28] Ambos instrumentos contemplan seis fundamentos posibles para garantizar la licitud del tratamiento. Ésta puede garantizarse por medio del consentimiento del interesado o si el tratamiento es necesario para: la ejecución de un contrato, para el cumplimiento de una obligación legal aplicable al responsable, para proteger intereses vitales, para el cumplimiento de una misión realizada en interés público o para la satisfacción de intereses legítimos, siempre que no prevalezcan los intereses o derechos y libertades fundamentales del interesado (RGPD, 2016, art.6).

considerará lícito el consentimiento del interesado mayor de 16 años o del titular de la patria potestad o tutela sobre el niño, en caso que sea menor a este límite de edad, si bien se admite que a nivel nacional los Estados miembros puedan ampliar este límite por ley hasta los 13 años. El responsable del tratamiento deberá, considerando la tecnología disponible, hacer "esfuerzos razonables" por determinar que el consentimiento fuera otorgado bajo estas condiciones.

De estas disposiciones debemos extraer como relevante para nuestro caso de estudio la obligatoriedad de obtener el consentimiento expreso e informado del interesado, por lo cual la red social deberá contemplar en el diseño de su Lógica de Gobierno y su Tecnología los elementos necesarios para garantizar la comunicación efectiva al usuario de toda la información pertinente al tratamiento de sus datos y la posibilidad técnica de expresar de manera clara y probable su consentimiento, mediante algún instrumento probatorio para futuras instancias en que fuera requerido. Para el caso de los menores de edad, la red social deberá implementar mayores esfuerzos en el diseño de su arquitectura para garantizar el cumplimiento de lo dispuesto y detectar cualquier infracción o desvío. En los siguientes apartados veremos qué información debe proveer obligatoriamente Facebook a sus usuarios y bajo qué condiciones.

En relación con el caso seleccionado, cabe mencionar además que en las condiciones para el consentimiento se establece una consideración particular para los casos en que exista un contrato y/o la prestación de un servicio de por medio. En estos casos, para determinar que el consentimiento se ha otorgado libremente, deberá constatarse que los datos personales fueron adecuados y limitados a los fines para los cuales fueron requeridos y que la ejecución del contrato o la prestación del servicio no estuvo condicionada por el consentimiento del titular para el tratamiento excesivo de sus datos. Esto debe vincularse con los principios relativos al tratamiento detallados en el artículo 5, que contemplan que los datos deben ser "adecuados, pertinentes y limitados" en función a los fines para los que son tratados (principio de minimización de datos). Es decir, Facebook no debería limitar el uso y acceso a su plataforma a aquellos usuarios que no acepten el uso de su información y datos personales que no fueran necesarios para la prestación de sus servicios.

- **Transparencia**

Tal como adelantamos en el apartado anterior, el responsable del tratamiento de datos tiene la obligación de proveer toda la información necesaria al titular de los datos para que pueda brindar un consentimiento libre e informado. Se establece que el responsable lleve adelante esta obligación bajo el principio de transparencia de la información, según el cual deberá comunicar toda información al interesado sobre las operaciones de tratamiento "en forma

concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo" (RGPD, 2016, art.12), atendiendo especialmente a los casos en que el destinatario de la comunicación sea un menor de edad.

Nuestro análisis sobre las políticas de privacidad de Facebook se enfocará en determinar el grado de cumplimiento de este principio, considerando el lenguaje utilizado, la extensión de los documentos, la ubicación y acceso a los mismos dentro de la plataforma y el procedimiento para el consentimiento expreso incorporado a la interfaz.

- **Información que debe facilitarse al interesado**

Respecto a la información relativa al tratamiento que el responsable debe facilitar, la Directiva 95/46/CE establecía como obligatorio: la identidad del responsable y, en caso de ser necesario, de su representante, los fines del tratamiento, los destinatarios de los datos y sus derechos de acceso y rectificación sobre sus datos.

En su artículo 14, el RGPD amplía este listado, contemplando, además, los datos de contacto del responsable y de su representante, los datos de contacto del Delegado de protección de datos, las categorías de datos personales que se traten y la intención del responsable de transferir sus datos a un destinatario en un tercer país u organismo internacional.

En el apartado 2 del mencionado artículo, se establecen también como información de carácter obligatoria una serie de elementos para garantizar la transparencia del tratamiento. Entre ellos podemos mencionar el plazo de conservación de los datos y los derechos del interesado: acceso, rectificación o supresión, limitación y oposición al tratamiento, derecho a la portabilidad de los datos, a retirar el consentimiento al tratamiento y el derecho a presentar un reclamo ante la autoridad de control. También deberá informarse la fuente de la que proceden los datos personales y si se trata de fuentes de acceso público.

Otro elemento adicional a lo estipulado por la Directiva, que se vincula directamente con el caso estudiado, es la obligación de informar al interesado si en las operaciones sobre los datos personales se toman decisiones automatizadas. En ese caso, debe brindarse información sobre la lógica aplicada y las consecuencias de estos procesos para el interesado. Este elemento cobra una relevancia fundamental para el caso a analizar, ya que, como hemos visto, la red social Facebook codifica la información personal de los usuarios y sus datos de comportamiento mediante el uso de algoritmos para su procesamiento, para la organización de contenido y la personalización de campañas publicitarias. Nos proponemos relevar si en sus políticas de privacidad la plataforma establece de manera clara y concisa cuáles son las operaciones automatizadas que se aplican sobre este tipo de datos y si el usuario tiene un acceso efectivo a los derechos contemplados sobre este tipo de tratamiento.

- **Nuevos derechos del interesado**

En el apartado anterior advertimos las novedades respecto de la información que el responsable debe facilitar al interesado. En las secciones 3, 4 y 5 del Reglamento se especifican en detalle los derechos del interesado, que además de contar con los ya consagrados en la Directiva 95/46/CE respecto del acceso, rectificación y oposición, se suman los derechos de supresión o "derecho al olvido", a la limitación del tratamiento y a la portabilidad de los datos.

El derecho de supresión o "derecho al olvido", incluido en el artículo 17, hace referencia al derecho del interesado a solicitar la supresión de sus datos personales al responsable del tratamiento en los casos en que los datos ya no fueran necesarios para los fines con los que fueron obtenidos, el titular de los datos retire el consentimiento o se oponga al tratamiento, el tratamiento no haya respetado los principios relativos a la licitud del tratamiento, si existe una obligación legal de por medio o si se trata de datos obtenidos de menores a través del uso de los servicios de la sociedad de la información. Los primeros dos casos no serán de aplicación válida cuando la supresión de los datos personales en cuestión colisione con el derecho a la libertad de expresión e información, si el tratamiento de esos datos es necesario para el cumplimiento de una obligación legal o para cuestiones de interés público o fines de investigación, estadísticos y de archivo, o para el ejercicio de ciertas reclamaciones.

El derecho a la limitación del tratamiento, comprendido en el artículo 18, se considera para los casos en los que se establezca la inexactitud de los datos, la ilicitud del tratamiento, cuando los datos ya no sean necesarios según los fines del tratamiento del responsable pero el interesado los precise para el ejercicio de algún reclamo, y para los casos en que el interesado se oponga, de acuerdo con el derecho a la oposición contemplado en el artículo 21.

Por último, el derecho a la portabilidad de los datos, mencionado en el artículo 20, introduce el derecho del interesado a acceder a sus datos personales "en un formato estructurado, de uso común y lectura mecánica", en los casos en los que el tratamiento se realice a través de métodos automatizados. Estos deberán poder transmitirse de un responsable a otro mientras que la técnica empleada lo permita.

En cuanto al derecho de oposición, presente en ambos actos legislativos, cabe destacar algunas especificaciones incluidas en el artículo 21 del RGPD. En primer lugar, se hace una mención explícita de los fines de tratamiento para la "mercadotecnia directa", bajo los cuales el interesado tiene derecho a oponerse en cualquier momento al tratamiento de sus datos

personales, lo cual abarcaría las operaciones automatizadas de elaboración de perfiles y análisis de comportamiento.

En cuanto a las decisiones individuales automatizadas, mencionadas tanto en el artículo 15 de la Directiva 95/46/CE como en el artículo 22 del RGPD, se establece que todo interesado tendrá derecho a "no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Este resguardo no es aplicable si entre el responsable y el interesado media la ejecución de un contrato, si está autorizada por ley o si está basada en el consentimiento explícito del titular de los datos.

- **Protección de datos desde el diseño y por defecto**

En el artículo 25 del RGPD se establece que el responsable del tratamiento incorpore medidas técnicas y organizativas, tales como la "seudonimización", que consiste en operaciones que permiten que los datos ya no sean directamente atribuibles a su titular sin información adicional, y la "minimización de los datos", un principio relativo al tratamiento en el artículo 5, según el cual los datos que se obtengan del interesado deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados", para hacer efectivos los derechos del interesado y cumplir con las disposiciones del Reglamento.

Estas medidas deben aplicarse no sólo en el momento de realizar el tratamiento sino desde que se seleccionen los métodos apropiados para hacerlo, teniendo en cuenta la técnica utilizada y sus costos, los fines para los cuales serán tratados los datos y los riesgos probables que surgieran de dicho proceso para la protección de los derechos del interesado, lo cual implica, para nuestro caso de estudio, que en aquellos casos en los que Facebook proceda a desarrollar nuevos productos o servicios o añadir funcionalidades a los existentes, mientras impliquen el tratamiento de datos personales de ciudadanos de la Unión Europea, deberá considerar y aplicar los requisitos y obligaciones del Reglamento desde el momento de su diseño.

- **Tratamiento de categorías especiales de datos personales**

Tanto la Directiva 95/46/CE en su artículo 8 como el RGPD en su artículo 9 prohíben el tratamiento de aquellos datos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos relativos a la salud o a la sexualidad" pero, como novedad, el RGPD incluye además dentro de estas categorías especiales de datos personales, los datos genéticos y biométricos. En cuanto a las excepciones a esta prohibición, ambos admiten una variedad de casos en los que el

tratamiento sería admisible, dentro de los cuales cabe mencionar para nuestro trabajo: aquellos casos en los que el interesado haya otorgado un consentimiento explícito para el tratamiento de sus datos según los fines especificados y en los casos en los que los datos personales de categoría especial hayan sido “manifiestamente públicos” por el interesado.

Según esta condición, si el usuario de la red social comparte de manera pública datos personales de carácter especial de manera pública, no estarían alcanzados por la prohibición del Reglamento. Es por esto que una configuración por default que fuerce una configuración de privacidad pública podría dejar obsoleto el nivel de protección especial contemplado para estos datos. Se requiere un nivel de información adecuado para el usuario y un manejo consciente de la herramienta para gestionar su configuración de privacidad de manera tal que se garantice la protección efectiva de sus datos personales.

- **Principio de Responsabilidad proactiva**

Este principio constituye otra de las novedades introducidas por el RGPD en lo que respecta a las obligaciones del responsable del tratamiento, el cual implica no sólo la obligación del responsable de cumplir con lo dispuesto por el Reglamento, sino también de ser capaz de demostrar de qué manera se compromete a cumplir con estas disposiciones (RGPD, 2016, art.5, inc. 2).

Este principio compromete al responsable a acreditar que ha tomado todas las medidas necesarias para garantizar el nivel adecuado de protección de los datos personales, atendiendo a los principios y obligaciones relativos al tratamiento.

Podemos advertirlo en la obligación de llevar un registro de las operaciones de tratamiento y de cooperar con la autoridad de control cuando ésta lo requiera. En pos de garantizar la seguridad de estas operaciones, se contempla además que el responsable implemente las medidas técnicas y organizativas necesarias, además de mecanismos de notificación pertinentes ante una posible brecha de seguridad.

En relación a la seguridad, se introducen además dos nuevos mecanismos para evaluar los riesgos del tratamiento y notificar a la autoridad de control en caso de ser necesario. Se establecen las “evaluaciones de impacto”, para determinar si las operaciones previstas a ejecutar sobre los datos personales representarían un riesgo significativo para los derechos del interesado. En los casos en que la evaluación de impacto concluya que, en efecto, las actividades de tratamiento previstas ocasionarían un alto riesgo, el responsable además deberá ejercer el mecanismo de “consulta previa” a la autoridad de control antes de realizar el tratamiento.

- **Seguridad del Tratamiento: obligaciones ante violaciones o brechas de seguridad**

En cuanto a la Seguridad del tratamiento, tanto la Directiva 95/46/CE como el RGPD disponen la obligación del responsable del tratamiento a aplicar las medidas técnicas y organizativas necesarias para garantizar un nivel adecuado de la protección de datos personales, teniendo en cuenta los riesgos que pudiera suponer dicho tratamiento y la categoría de datos que se trate.

El RGPD acentúa este nivel de responsabilidad, estableciendo en el artículo 33 la obligación de notificar a la autoridad de control en caso de una violación de seguridad en un plazo de 72 horas, exceptuando los casos en que se contemple que la brecha de seguridad no implica un riesgo para la protección de la persona física interesada en relación al tratamiento y acceso a sus datos personales. Dicha notificación deberá incluir un informe de las medidas adoptadas por el responsable para restaurar la seguridad y confidencialidad debida. En el artículo 34, además, se dispone que para los casos en que la violación de seguridad implique un alto riesgo para los derechos y libertades de las personas físicas, el responsable lo comunique inmediatamente al interesado. Este mecanismo podrá evitarse si el responsable tomó las medidas apropiadas para que los datos no fueran susceptibles de ser interpretados por terceros ajenos a las operaciones de tratamiento - como es el caso de las técnicas de cifrado - o si aplicó medidas que mitigaron posteriormente el alto nivel de riesgo para el interesado. También podrá optar por emitir un comunicado público para los casos en que fuera dificultoso establecer la comunicación directa con el interesado, pero que garantice una efectiva comunicación del hecho.

- **Figura del Delegado de Protección de Datos**

El RGPD introduce en la Sección 4 una nueva figura denominada “Delegado de Protección de Datos”, el cual deberá ser designado por el responsable y el encargado en los casos en que el tratamiento de datos personales o de categorías especiales de datos personales a gran escala constituya su actividad principal, que requieran “una observación habitual y sistemática de interesados” (RGPD, 2016, art.37).

También se contempla la figura del Delegado de Protección de Datos para los casos en que el tratamiento sea realizado por un organismo o autoridad pública. Sus funciones consisten en informar y asesorar al responsable y al encargado sobre la normativa vigente y supervisar el cumplimiento de sus obligaciones, además de cooperar con la autoridad de control. Sus datos de contacto deberán ser informados a los interesados, que podrán hacerlo en virtud de los derechos contemplados en el RGPD.

En nuestro caso de estudio nos compete relevar si la red social considera este tipo de operaciones sobre los datos personales como una actividad principal para el funcionamiento de su modelo de negocios y si ha nombrado un Delegado de Protección de Datos como consecuencia de ello.

- **Comité europeo de protección de datos**

A través del artículo 29 de la Directiva 95/46/CE se creó el "Grupo de protección de las personas en lo que respecta al tratamiento de los datos personales", como un organismo de carácter consultivo e independiente, compuesto por "un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión" (Directiva 95/46/CE, art.29). Entre sus funciones se contemplaba el análisis de todas las disposiciones de los Estados miembros creadas para acatar los objetivos de la mencionada directiva, velando por una aplicación uniforme de sus principios en toda la UE y la elaboración de dictámenes sobre los niveles de protección dentro de la UE y en países terceros. Con la sanción del Reglamento de Protección de Datos y la consecuente derogación de la Directiva 95/46/CE (RGPD, 2016, art.94) se crea el "Comité europeo de protección de datos" como organismo de la UE con personalidad jurídica e independiente, que ocupará desde entonces el rol y funciones reservados para el Grupo de Protección mencionado, con una mayor autonomía y capacidad de acción en lo que respecta a la supervisión de la aplicación del Reglamento. Podrá, además, emitir directrices, recomendaciones y buenas prácticas, asesorar a la Comisión y emitir dictámenes sobre los niveles adecuados de protección en un país tercero u organización internacional (RGPD, 2016, art.70).

Estos elementos y modificaciones incorporados por la normativa europea representan un avance significativo para la protección de los datos personales, ya que incorporan aspectos y problemáticas presentes en la lógica de Gobierno y Tecnología de las plataformas de redes sociales y de Facebook en particular, analizados en este trabajo. Elementos como la protección de datos desde el diseño y por defecto, la incorporación de los datos biométricos como categoría especial de datos personales, la ampliación del alcance de su ámbito de aplicación, proponen una actualización de la normativa que busca adaptarse a la multiplicidad de funcionalidades de las TIC y sus posibles arquitecturas o códigos. Por ejemplo, la herramienta de reconocimiento facial incorporada por Facebook ahora es alcanzada por este reglamento y con un nivel de protección especial, gracias a la incorporación de la definición de datos biométricos como categoría especial de datos personales.

Además, un ámbito de aplicación que ya no depende exclusivamente del establecimiento físico de la empresa responsable del tratamiento o de dónde se realice el tratamiento, se ajusta también a los regímenes de propiedad actuales de las grandes empresas de tecnología.

Primeras sanciones del RGPD

Desde la entrada en vigencia del RGPD, en mayo de 2018, pueden enumerarse las primeras sanciones que se han impuesto en virtud de sus disposiciones. Cabe destacar que este nuevo instrumento estipula un máximo de 20.000 euros o de hasta el 4% de la facturación anual, si se trata de una empresa, para la imposición de multas administrativas (RGPD, 2016, art.83). Para determinar el monto de la sanción, la Autoridad de Control de cada Estado miembro deberá considerar una serie de elementos, tales como la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia, si el responsable o encargado del tratamiento tomó alguna medida para contrarrestar los daños ocasionados, las categorías de los datos personales afectados, de qué manera la autoridad de control tomó conocimiento de la infracción, entre otros. (RGPD, 2016, art.83).

Entre las primeras sanciones tras la implementación del RGPD - que alcanzan a diferentes empresas e instituciones, además de los tipos de plataformas digitales analizados - se encuentran tres multas impuestas al Hospital Do Barreiro de Portugal, de las cuales dos corresponden por violación del principio de confidencialidad y ascienden a los 150.000 euros cada una y otra por violación del principio de minimización de datos por 100.000 euros[29].

En Alemania, se impuso la sanción de 20.000 euros a una red social llamada *Knuddles* que fue hackeada, lo cual permitió la filtración de 808.000 direcciones de correo y más de 1,8 millones de usuarios y contraseñas. En este caso, la multa representa un monto mucho menor, ya que al darse a conocer la brecha de seguridad la empresa optimizó sus medidas de seguridad[30].

En Francia, la Comisión Nacional de Protección de Datos (CNIL) sancionó a la empresa Google por un total de 50 millones de euros, por una infracción del principio de transparencia y del derecho de información de los usuarios y por una infracción de la obligación de tener una base legal para el tratamiento de personalización de anuncios. La CNIL fijó este monto entendiendo que “las infracciones privan a los usuarios de garantías esenciales en cuanto al

[29] Así han sido las primeras multas a empresas por vulnerar el GDPR. (2018, 13 de diciembre). *Ticbeat.* Recuperado de https://www.ticbeat.com/seguridad/multas-empresa-gdpr/

[30] ¿Cuánto han pagado las primeras empresas sancionadas por incumplir con el GDPR? (2018, 12 de diciembre). *Panda Security.* Recuperado de https://www.pandasecurity.com/spain/mediacenter/noticias/primeras-sanciones-incumplimiento-gdpr/

tratamiento de datos, el cual puede revelar partes importantes de la vida privada de los usuarios, dado el extenso número de datos personales que se tratan, la amplia variedad de servicios y las posibles combinaciones"[31].

Pero la multa más elevada fue impuesta a la empresa British Airways por un valor total de 183,39 millones de libras (más de 200 millones de euros), debido a una brecha de seguridad que vulneraba la protección de los datos personales de más de 500.000 usuarios que realizaron operaciones a través de su sitio web y aplicación móvil[32].

En lo que respecta específicamente a Facebook, la empresa fue sancionada por varios Estados miembro de la UE a causa del mencionado caso de filtración de datos que involucraba a la consultora Cambridge Analytica. Si bien la mayor parte de los usuarios afectados por este caso se localizó en Estados Unidos, (por lo cual la empresa fue multada por la Comisión Federal de Comercio de Estados Unidos de EEUU por 5000 millones de dólares[33]) de acuerdo a los datos proporcionados por Facebook a la Comisión Europea, también se vulneró la protección de datos personales de alrededor de 2,7 millones de ciudadanos europeos[34].

Pero, como este hecho aconteció previamente a la entrada en vigencia del RGPD, las sanciones impuestas se alejan significativamente de los casos anteriores: la Oficina del Comisionado de Información de Reino Unido impuso una multa de 500 000 libras[35], mientras que Italia impuso dos multas de 10 millones de euros "por la falta de transparencia" y la "explotación económica de los datos de los usuarios sin contar con el consentimiento adecuado de estos"[36]. Teniendo en cuenta que durante el año 2018 la empresa obtuvo un total de 55 800 millones de dólares de ingresos[37] (aproximadamente unos 50 000 millones de

---

[31] Sánchez-Jara, G. (2019, 18 de marzo). Multa récord a Google por infracción del RGPD: 50 millones de euros. *RGPD Blog.* Recuperado de http://rgpdblog.com/multa-record-a-google-por-infraccion-del-rgpd-50-millones-de-euros/

[32] Muñoz, R. (2019, 8 de julio). Multa de 205 millones a British Airways por el robo de datos de los clientes. El País. Recuperado de https://elpais.com/economia/2019/07/08/actualidad/1562569904_267036.html

[33] Pozzi, S. (2019, 12 de julio). EE UU multa a Facebook con 5000 millones por violar la privacidad de los usuarios. *El País.* Recuperado de https://elpais.com/economia/2019/07/12/actualidad/1562962870_283549.html

[34] Mark Zuckerberg declaró ante el Parlamento Europeo por Cambridge Analytica. (218, 22 de mayo). *Perfil.* Recuperado de https://www.perfil.com/noticias/internacional/mark-zuckerberg-declara-ante-el-parlamento-europeo-por-cambridge-analytica.phtml

[35] Facebook y sus pasadas, presentes y futuras multas. (2019, 10 de julio). *Panda Security.* Recuperado de https://www.pandasecurity.com/spain/mediacenter/noticias/facebook-multa-gdpr/

[36] Multa récord a Facebook en Italia por vender datos de sus usuarios. (2018, 10 de diciembre). *Perfil*. Recuperado de https://www.perfil.com/noticias/tecnologia/italia-multa-a-facebook-por-vender-datos-de-sus-usuarios.phtml

[37] Facebook (2018). *Facebook Reports Fourth Quarter and Full Year 2018 Results.* Recuperado de https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx

euros), se advierte que estas sumas representan tan sólo un 0,02% de la facturación anual de la empresa. Hasta la fecha, se conocen algunas investigaciones en marcha sobre las operaciones de tratamiento de datos personales llevadas adelante por Facebook que, en caso de incurrir en algún tipo de infracción, serían alcanzadas y pasibles de sanción en el marco del RGPD, como es el caso de la Comisión Irlandesa de Protección de Datos[38].

En el próximo apartado, nos dedicaremos a analizar la adecuación de la red social Facebook a las nuevas disposiciones que introduce el RGPD, para identificar en qué medida fueron implementadas por una plataforma de redes sociales específica y el nivel de protección de los datos personales que esta empresa ofrece a los usuarios.

[38] Facebook: Irlanda investiga la exposición de millones de contraseñas (2019, 25 de abril). *Gestión.* Recuperado de https://gestion.pe/tecnologia/facebook-irlanda-investiga-exposicion-millones-contrasenas-nndc-265115-noticia/

5. Protección de datos personales en Facebook

Con la entrada en vigencia del RGPD en mayo de 2018, la empresa Facebook se vio obligada a adecuar sus políticas de privacidad y condiciones de uso a sus principios y disposiciones. Aunque, como hemos visto, el Reglamento vela por la protección de los datos personales de los ciudadanos europeos, la red social decidió implementar estos cambios a nivel mundial, introduciendo algunos elementos específicos en el ámbito de la UE:

> Si bien el contenido de nuestra política de datos es el mismo a nivel mundial, las personas en la UE verán detalles específicos relevantes solo para las personas que viven allí, como, por ejemplo, la forma de contactar a nuestro Oficial de Protección de Datos bajo el GDPR. Queremos dejar en claro que no hay ninguna diferencia sobre los controles y protecciones que ofrecemos en el resto del mundo (Egan, 2018).

Es interesante señalar que luego de que se diera a conocer públicamente la filtración de datos sin consentimiento de los usuarios hacia la consultora Cambridge Analytica, el Presidente y Director Ejecutivo de la red social, Mark Zuckerberg, procuró manifestar públicamente su adhesión a los principios de este Reglamento y promoverlos como marco regulador común para el escenario de Internet en su totalidad:

> (...) la protección efectiva de la privacidad y la información necesita un marco global armonizado. Personas de todo el mundo han pedido una regulación integral para la privacidad en línea con el reglamento general de la protección de datos de la Unión Europea, y estoy de acuerdo. Creo que sería bueno para Internet si más países adoptaran regulaciones como el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) como marco común. (Zuckerberg, 2019)

De esta manera, la implementación de estas modificaciones impacta a los usuarios de la red social a escala mundial y el RGPD se posiciona como marco legal de referencia en materia de protección de datos personales. Nos proponemos, entonces, analizar estos cambios en relación a las novedades que la legislación europea introduce para proteger el derecho de los usuarios y regular el tratamiento de sus datos personales.

5.1 Tensiones emergentes

Si bien en el próximo apartado desarrollaremos en profundidad un análisis comparativo entre las condiciones de uso de la red social Facebook y los principios propuestos por el RGPD, nos interesa destacar algunas tensiones que se desprenden de nuestro análisis en general

sobre el funcionamiento de este tipo de plataformas y el nivel de protección que puede garantizarse para los datos personales de los usuarios.

En primer lugar, se advierte una tensión entre la protección de los datos personales y los fundamentos básicos del funcionamiento y lógica de negocios de las redes sociales, los cuales se sustentan sobre operaciones sistemáticas de tratamiento de datos. Así lo indica Facebook en sus Condiciones del Servicio:

> En lugar de pagar por usar Facebook y el resto de los productos y servicios que ofrecemos, al usar los Productos de Facebook que se incluyen en estas Condiciones, aceptas que podamos mostrarte anuncios de las empresas y organizaciones que nos pagan por promocionarse dentro y fuera de los Productos de las empresas de Facebook. Usamos tus datos personales, como la información sobre tu actividad y tus intereses, para mostrarte aquella publicidad que pueda resultarte más relevante. (Facebook, 2019)

Los intereses comerciales de estas plataformas promueven una constante proliferación de información y contenido personal, la interacción con otros y una multiplicidad de acciones en línea, sobre las cuales se aplican las técnicas de procesamiento y análisis de la información que ya hemos analizado. Facebook define como su misión principal “dar a la gente el poder de crear comunidades y unir más al mundo” (Facebook, 2019). Este objetivo se traduce en una facilitación constante de herramientas y servicios para incentivar al usuario a compartir su biografía y vida personal en línea, a hacer público cada acontecimiento importante de su vida, sus gustos, sus deseos, sus intereses y comportamiento. Todas estas acciones generan enormes cantidades de datos, que son recopilados sistemáticamente por la plataforma, analizados y consolidados para diferentes usos, entre ellos, para la implementación de campañas publicitarias en su entorno digital.

Nissenbaum (2011) señala que existen al menos tres tipos de problemas que emergen en el contexto de las redes sociales en relación al flujo de la información personal. Uno de ellos tiene que ver con los daños que pueden ocasionarle a la persona la circulación de manera pública de su información personal, como por ejemplo, ser discriminada en una búsqueda de empleo por los contenidos que publica. Otro problema relacionado surge con el contenido compartido por otras personas, sobre el cual el usuario involucrado puede decidir no quedar vinculado mediante una “etiqueta”[39] pero no tiene el control sobre la información para eliminarla o restringir su visualización a un público determinado. Un tercer problema tiene que ver con las posibilidades de monitoreo y rastreo que ofrecen las redes sociales, a partir de la

[39] Servicio de ayuda de Facebook (2019). *¿En qué consiste el etiquetado y cómo funciona?* Recuperado de https://es-la.facebook.com/help/124970597582337

integración de la información personal y datos de comportamiento de cada usuario en bases de datos para la elaboración de perfiles y personalización de contenidos.

Pero, además, se suman otros actores al ecosistema que también logran tener acceso a este gran volumen de datos, ya sean aplicaciones o sitios web que integran algunas de las funcionalidades de Facebook, las empresas o agencias de marketing anunciantes y los socios externos con los que la plataforma comparte información abiertamente. Cabe preguntarse, entonces, cómo es posible garantizar en un sistema tan complejo, con la participación de múltiples actores, que todas las operaciones de tratamiento y los niveles de acceso a estos datos protejan los derechos de cada usuario.

A estos interrogantes debemos sumar nuestras reflexiones acerca del diseño del código y la Tecnología de la plataforma. Como hemos visto, retomando el trabajo de Lessig (1998), estas configuraciones de protocolos técnicos y sociales son el producto de decisiones políticas e intereses particulares de los propietarios de la red social, por lo tanto pueden tomar múltiples formas. Es decir, advertimos que es posible modificar las restricciones y posibilidades que ofrecen estas herramientas, por lo cual podríamos pensar en un entorno digital más regulable que incluya en su diseño el derecho a la protección de los datos personales como un valor fundamental. De esta forma, su arquitectura o código sería capaz de facilitar su ejercicio y proveer mecanismos de garantía.

Lessig (1998) argumenta que ante una configuración del ciberespacio en apariencia inabarcable y compleja por naturaleza, la ley se presenta como una alternativa posible para fomentar una mayor regulabilidad, impregnando la arquitectura de red de los valores democráticos y constitucionales ya consagrados en “el espacio real”. Podemos decir que los planteos de la UE en materia de protección de datos personales han ejercido una presión considerable con la sanción del RGPD sobre las decisiones de las grandes empresas en cuanto al desarrollo de sus plataformas de redes sociales. Si bien aún se advierten algunas imprecisiones o falta de claridad en su operatoria - como veremos en profundidad en el próximo apartado - la ley ha forzado a estas empresas a implementar modificaciones en su código y en sus normas, a ser más transparentes en la comunicación de sus propósitos y modelo de negocios, y ha permitido una mayor difusión y conocimiento sobre los derechos de los usuarios en relación a la protección de sus datos personales.

Pero, también en relación a estas reflexiones encontramos un punto de tensión emergente, vinculado con las diferentes posturas acerca de los marcos regulatorios posibles. Entre ellas, se encuentran planteos como el de Nissenbaum (2011), quien propone el modelo conceptual de “integridad contextual” para evaluar por contextos las restricciones al flujo de la información personal en relación a los valores compartidos por los actores en cada una de las esferas de

la actividad social. Es decir, en el caso particular de las redes sociales, se debería evaluar según una serie de parámetros predeterminados - como el contexto, actores, atributos y principios de transmisión de la información - si las actividades ejercidas por las plataformas sobre la información personal contradicen las normas sociales compartidas por los usuarios respecto a los valores esperables de protección de sus datos. En este sentido, la autora define como un modelo regulatorio ejemplificador el desarrollado en el ámbito de los Estados Unidos, según el cual el derecho a la privacidad es regulado de manera "sectorial":

> El enfoque estadounidense de las leyes de la privacidad informativa, en contraste, se describe como sectorial, porque en la Constitución no se expresa un derecho explícito a la privacidad y la legislación ha tendido a desarrollarse de modo un tanto independiente, sector por sector. (Nissenbaum, 2011, p.230)

Este modelo se contrapone al propuesto por la UE, el cual es considerado por la autora como un enfoque "amplio", por considerar los derechos a la privacidad y a la protección de datos personales como derechos humanos fundamentales a nivel constitucional. Un enfoque "sectorial" basado en el derecho de la integridad contextual trabajaría en definir las restricciones al flujo de la información personal en relación a cada contexto en particular y no forzaría, en este caso, una adaptación de las TIC a las regulaciones ya consagradas en el "espacio real". Cabe preguntarse, en relación a lo propuesto por Nissenbaum (2011) y las regulaciones sectoriales o por contexto, si es posible determinar las expectativas de los millones de usuarios que comparten su información personal con las plataformas de redes sociales.

5.2 Facebook y las políticas de privacidad. Adecuación al RGPD

En este apartado profundizaremos sobre el análisis de la Lógica de Gobierno de Facebook, analizando las normas explícitas propuestas por la plataforma y los cambios más recientes para regular su funcionamiento, en relación a las disposiciones introducidas por el RGPD. Consideraremos específicamente las Condiciones del servicio modificadas el 19 de abril de 2018 y las posteriores incorporaciones que se realizaron el 31 de julio de 2019. También analizaremos su Política de datos modificada por última vez el 19 de abril de 2018. En ambos casos estudiaremos las modificaciones que se realizaron de manera uniforme a nivel mundial y señalaremos también los cambios específicos que aplican exclusivamente para la UE de acuerdo a su regulación.

Como hemos desarrollado, para acceder al registro en la red social es necesario manifestar expresamente que se han leído y aceptado estas normativas. Procederemos a desarrollar las

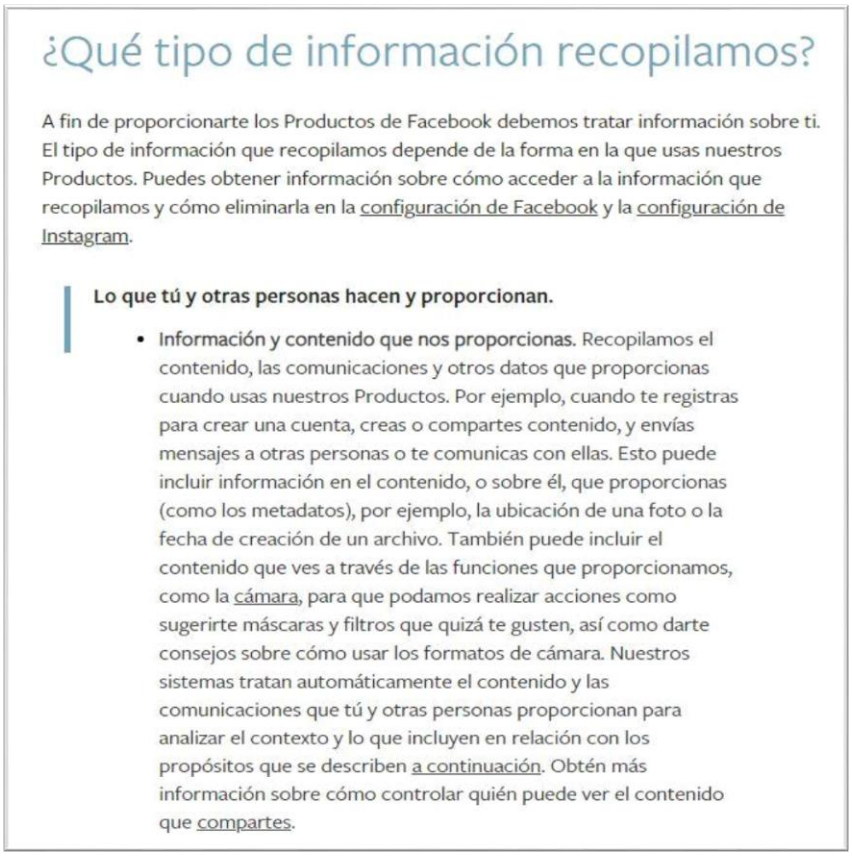
modificaciones introducidas por la red social agrupándolas de acuerdo a los principios y disposiciones del RGPD analizadas en la sección anterior.

- **Transparencia e Información que debe facilitarse al interesado**

Para adecuarse al principio de Transparencia en relación a la información que debe proveerse al titular de datos, Facebook introduce como novedad la explicitación de su modelo de negocios, señalando los pagos que los anunciantes realizan para ofrecer bienes y servicios dentro de su plataforma:

> No cobramos por el uso que haces de Facebook ni de los otros productos y servicios que abarcan estas Condiciones. Por el contrario, los negocios y las organizaciones nos pagan para que te mostremos anuncios de sus productos y servicios. Al usar nuestros Productos, aceptas que podemos mostrarte anuncios que consideremos que te resultarán relevantes para ti y tus intereses. Usamos tus datos personales como ayuda para determinar qué anuncios mostrarte. (Facebook, 2019)

En este sentido, también procede a informar al usuario que recopila sus datos personales, qué tipos de datos es capaz de recolectar y las finalidades para las cuales son utilizados. De este modo, menciona en primer lugar la información personal provista por el usuario y el contenido que genera, como en los casos en que publica una foto o entabla una conversación privada con otro contacto. Además, la red social indica que posee el acceso a los metadatos de estos contenidos, que pueden incluir la ubicación geográfica en la cual fue tomada esa fotografía o la fecha de creación (Figura 6).



¿Qué tipo de información recopilamos?

A fin de proporcionarte los Productos de Facebook debemos tratar información sobre ti. El tipo de información que recopilamos depende de la forma en la que usas nuestros Productos. Puedes obtener información sobre cómo acceder a la información que recopilamos y cómo eliminarla en la configuración de Facebook y la configuración de Instagram.

Lo que tú y otras personas hacen y proporcionan.

- **Información y contenido que nos proporcionas.** Recopilamos el contenido, las comunicaciones y otros datos que proporcionas cuando usas nuestros Productos. Por ejemplo, cuando te registras para crear una cuenta, creas o compartes contenido, y envías mensajes a otras personas o te comunicas con ellas. Esto puede incluir información en el contenido, o sobre él, que proporcionas (como los metadatos), por ejemplo, la ubicación de una foto o la fecha de creación de un archivo. También puede incluir el contenido que ves a través de las funciones que proporcionamos, como la cámara, para que podamos realizar acciones como sugerirte máscaras y filtros que quizá te gusten, así como darte consejos sobre cómo usar los formatos de cámara. Nuestros sistemas tratan automáticamente el contenido y las comunicaciones que tú y otras personas proporcionan para analizar el contexto y lo que incluyen en relación con los propósitos que se describen a continuación. Obtén más información sobre cómo controlar quién puede ver el contenido que compartes.

Figura 6: ***¿Qué tipo de información recopilamos?*** Fragmento de la Política de Datos de Facebook. Recuperado de https://www.facebook.com/about/privacy/update

También señala que recopila información resultante de la interacción del usuario con otras personas, páginas de empresas y grupos. En este caso, la red social es capaz de relevar los usuarios y las páginas con las que más se interactúa y las comunidades a las que la persona decide sumarse, además de sugerirle nuevos contactos y páginas basados en la información de contacto que el usuario decida sincronizar con la plataforma a través de su dispositivo, como por ejemplo, el listado de contactos de su teléfono celular o del servicio de correo electrónico que utilice. De esta manera, la plataforma puede rastrear a estos contactos a través de su número telefónico o dirección de correo.

Se incluye además, la información sobre operaciones de compras o donaciones realizadas a través de los productos de Facebook, los contenidos que otros usuarios compartan sobre la persona, la información sobre los dispositivos a través de los cuales se accede a la plataforma y la información provista por los “socios”. Este último es un elemento importante ya que Facebook informa sobre su asociación con terceros y la información a la cual es capaz de acceder gracias a esto. En este punto se aclara que a través de la exportación de algunas de sus funciones como el botón “Me gusta” o el inicio de sesión a otros sitios web y aplicaciones, la red social es capaz de recolectar información sobre el comportamiento del usuario fuera de

Facebook. De acuerdo a su "Política de Datos", procura asegurarse que "todos los terceros cuenten con derechos legítimos para recopilar, usar y compartir sus datos" (Facebook, 2018).

En cuanto a las finalidades del tratamiento, Facebook declara en su Política de Datos que esta multiplicidad de datos es utilizada para brindar todos los servicios que ofrecen al usuario, implementar mejoras en sus productos y ofrecer al usuario una experiencia personalizada y uniforme en cada uno de ellos. También se incluyen las finalidades de investigación para el desarrollo de nuevos productos y la implementación de la función de "reconocimiento facial". En este punto, se advierte que la información generada a partir de esta función puede considerarse como dato sensible por algunas legislaciones. Como hemos visto, este es el caso del RGPD, ya que incluye en las categorías especiales de datos personales a los datos biométricos. Para estos casos, la red social se vio obligada a introducir esta funcionalidad como opcional, con la posibilidad de limitar o permitir su implementación en sus herramientas de configuración.

En cuanto a la información adicional brindada específicamente para el ámbito de la UE, debemos resaltar que se incorporan los datos de contacto de Facebook *Ireland* como responsable del tratamiento y del Delegado de protección de datos. También se introduce al final de las Políticas de Datos de la UE el derecho del usuario a "presentar una demanda ante la autoridad de control principal de Facebook *Ireland*, la Comisión de protección de datos de Irlanda o la autoridad de control local". Cabe señalar que la empresa cuenta con su sede principal para la Unión Europea en Dublín, Irlanda[40]. Un gran número de empresas multinacionales se ha instalado en este país, que favorece la entrada de capitales extranjeros con bajas tasas de impuestos y una flexible legislación laboral[41].

- **Nuevos derechos del interesado**

En cuanto a los derechos del usuario, se incorpora la posibilidad de acceder a los datos, rectificarlos, transferirlos y suprimirlos (Facebook, 2018), en consonancia con los derechos de acceso, rectificación y supresión reconocidos por el RGPD. Facebook traduce esta disposición en su interfaz a través de la herramienta de configuración, que presenta las siguientes opciones:

[40] Pico, R. (2008, 2 de octubre). Facebook se asienta en Irlanda. *Silicon.es*. Recuperado de https://www.silicon.es/facebook_se_asienta_en_irlanda-2171406

[41] Fariza, I. (2016, 1 de septiembre). Irlanda, una economía dopada por sus ventajas a las multinacionales. *El País.* Recuperado de https://elpais.com/economia/2016/08/31/actualidad/1472671229_159313.html

Figura 7: ***Tu Información de Facebook.*** Acceso a la configuración de la cuenta. Recuperado de https://www.facebook.com/settings?tab=your_facebook_information

En la Política de Datos de la UE se incluyen, además, mecanismos específicos que contemplan los derechos de oposición y limitación al tratamiento del usuario. Como desarrollamos anteriormente en el análisis del RGPD, el reglamento introduce como novedad una mención explícita a la "mercadotecnia directa" como una finalidad de tratamiento a la cual el titular de los datos tiene derecho a oponerse en cualquier momento. En línea con esta disposición, la Política de Datos de la UE incorpora la siguiente modificación:

> También tienes derecho a oponerte a ciertos tratamientos de tus datos y restringir dichos tratamientos. Esto incluye: el derecho a oponerte al tratamiento de tus datos para fines de marketing directo mediante el enlace "Cancelar suscripción" que figura en dichas comunicaciones de marketing; y el derecho a oponerte a nuestro tratamiento de tus datos cuando realicemos una tarea en pro del interés público o de nuestros intereses legítimos o aquellos de un tercero. Puedes ejercer este derecho en Facebook e Instagram. (Facebook, 2018)

Sin embargo, debemos señalar que las configuraciones según las cuales se admite el ejercicio de los derechos de acceso, rectificación y supresión (Figura 7) no permiten un acceso total a la información recopilada de los usuarios. En principio, si bien se permite gestionar a qué aplicaciones se otorga permiso para acceder a la información personal, no

es posible acceder a la información provista por terceros o “socios”. En las Figuras 8 y 8.1 podemos encontrar el listado de información a la que Facebook brinda acceso.

Figura 8: ***Acceder a tu información.*** Listado de información a la cual el usuario tiene acceso y la posibilidad de descarga. Recuperado de https://www.facebook.com/your_information/

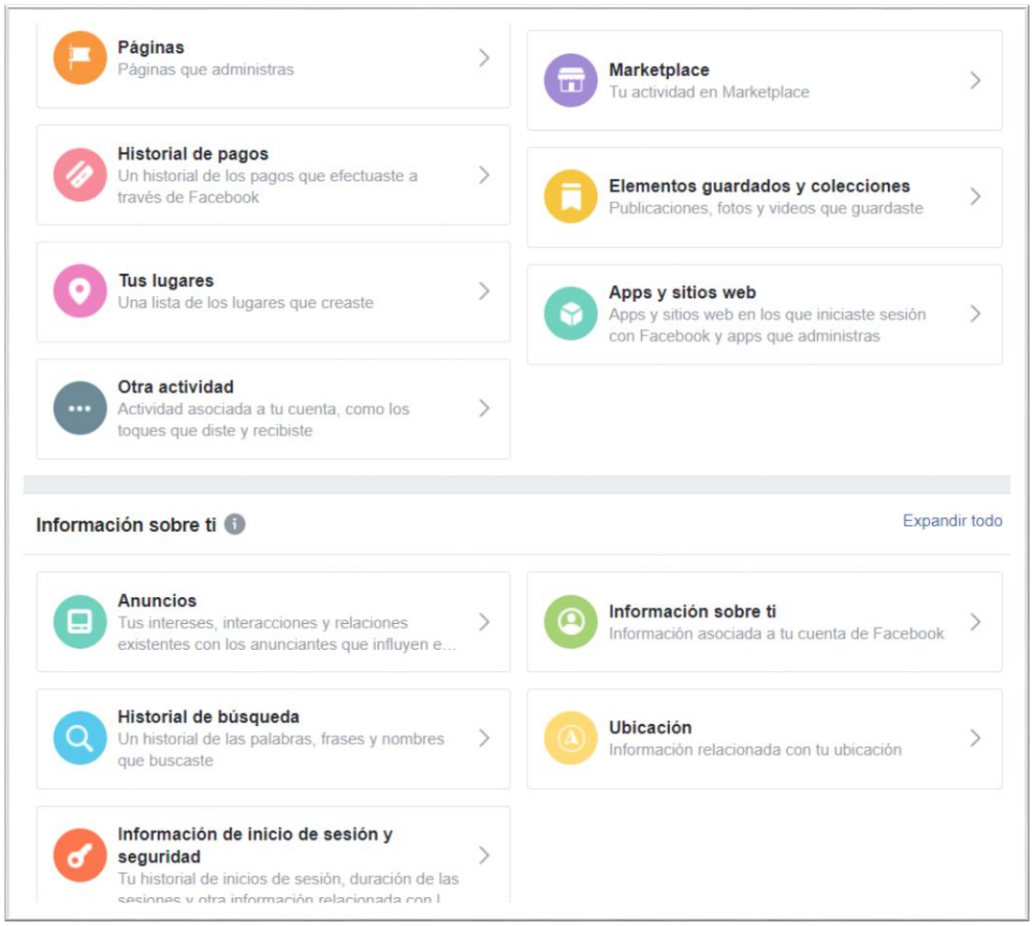


Figura 8.1: ***Acceder a tu información.*** Listado de información a la cual el usuario tiene acceso y la posibilidad de descarga. Recuperado de https://www.facebook.com/your_information/

Se incluye, sin embargo, una sección específica para los anuncios publicitarios denominada “Tus preferencias de anuncios” (Figura 9) que permite, entre otras cosas, visibilizar en qué categorías de intereses la plataforma incluye al usuario según sus datos y comportamiento y qué empresas anunciantes compartieron en la plataforma una base de datos en la que el usuario estaba incluido y la utilizaron para personalizar la audiencia de sus anuncios.

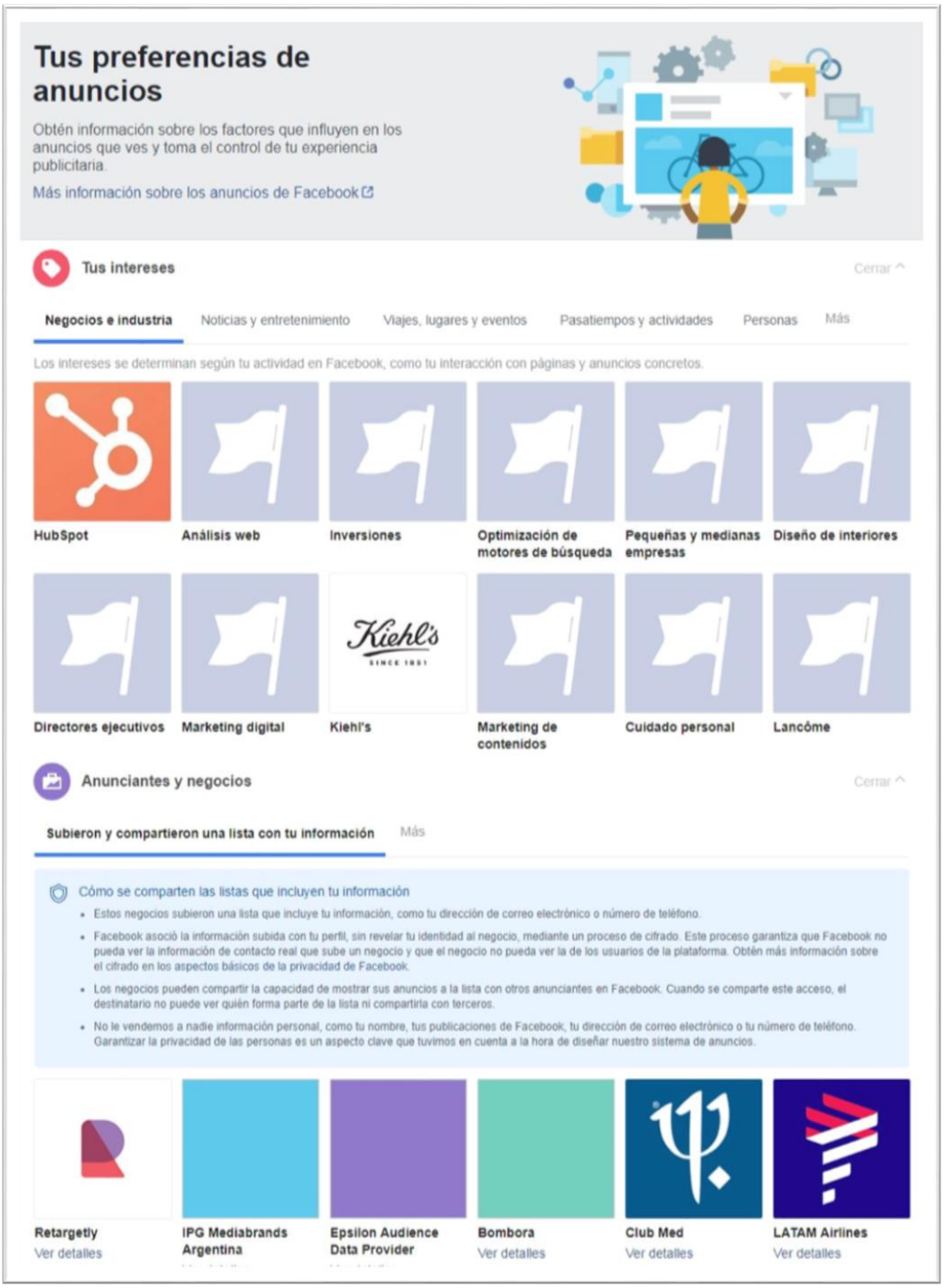


Figura 9: ***Tus preferencias de anuncios.*** Recuperado de https://www.facebook.com/ads/preferences

A través de esta herramienta también se puede revocar el permiso para la visualización de anuncios basados en datos de terceros o basados en la información del usuario fuera de Facebook (Figura 10), pero no es posible conocer los datos específicos que posee la plataforma, sólo se brindan categorías o tipos de información agrupados en función de intereses o grupos sociodemográficos predeterminados.

Figura 10: Tus preferencias de Anuncios. ***Configuración de anuncios.*** Recuperado de https://www.facebook.com/ads/preferences

En cuanto al tiempo de conservación de la información personal del usuario, la red social estipula que se preserva su almacenamiento hasta que ya no son necesarios para la oferta de sus servicios y productos o hasta que el usuario decida eliminar su cuenta (Facebook, 2018).

Para los casos en que el usuario decida eliminar contenido de su cuenta, Facebook estableció una nueva disposición en las modificaciones incorporadas en julio de 2019 con un mayor nivel de claridad en cuanto a los tiempos de conservación de la información, estipulando un plazo máximo de 90 días desde el momento en que el usuario realice esta acción.

- **Protección de datos desde el diseño y por defecto**

En relación al desarrollo de sus productos, Facebook se refiere específicamente al diseño de su herramienta de anuncios publicitarios en las modificaciones de sus Condiciones del Servicio introducidas en julio de 2019. En este punto, declara que la protección de la privacidad del usuario es prioritaria en el desarrollo de esta herramienta. Bajo esta premisa, asegura que no vende los datos personales de sus usuarios ni revela su identidad personal.

Sus funcionalidades de personalización y segmentación ofrecen a los anunciantes la posibilidad de refinar el direccionamiento de sus anuncios creando audiencias específicas en función de intereses y datos de comportamiento, pero la creación de estas audiencias no se vincula, según Facebook, con la identificación directa de cada usuario como receptor del anuncio y titular del dato.

En este caso, debemos señalar que los anunciantes pueden compartir en la herramienta de creación de anuncios de Facebook bases de datos propias sobre clientes, contactos y otros, las cuales pueden incluir dirección de correo electrónico y número telefónico. Si bien se podría admitir, de acuerdo a lo estipulado por Facebook, que los anunciantes no acceden a la totalidad de los datos personales de los usuarios ni son informados de la identidad de cada titular de estos datos, sí debemos considerar que Facebook recepciona estas bases de datos consolidadas, por lo cual cabe preguntarse si es capaz de integrarlas a la información de sus usuarios, identificándolos con su dirección de correo o número de teléfono. En este punto, continúa siendo poco claro el volumen de datos que la red social obtiene de cada usuario y no se incorpora un mecanismo que garantice el ejercicio de los derechos del usuario sobre sus datos personales.

- **Tratamiento de categorías especiales de datos personales**

En la Política de datos de Facebook (2018) se hace una referencia específica a los datos con protecciones especiales dentro de los tipos de información que Facebook recopila de sus usuarios. Este breve apartado contempla lo siguiente:

> Puedes optar por proporcionar información en los campos de tu perfil de Facebook o acontecimientos importantes relacionados con tus creencias religiosas, tus ideologías políticas, tus intereses o aspectos relacionados con tu salud. Esta y otra información (como el origen étnico o racial, las creencias filosóficas o la afiliación sindical) puede estar sujeta a protecciones especiales en virtud de las leyes de tu país. (Facebook, 2018)

De esta manera, se procede a una enumeración de los posibles campos del perfil personal de cada usuario que podrían constituir un dato sensible o una categoría especial de dato personal de acuerdo a la legislación de cada país y se contempla la posibilidad de que existan particularidades en relación a la protección de estos datos. En el caso de la Política de Datos de la UE, se informa específicamente que estos datos “están sujetos a protecciones especiales en virtud de la ley de la UE” (Facebook, 2018). Sin embargo, no se advierten los riesgos posibles que pueden derivar del tratamiento de datos personales de estas características ni se informa sobre la imposibilidad de tratarlos sin el consentimiento expreso de su titular. Si bien incluye un enlace adicional para ofrecer al usuario información sobre la

configuración de privacidad de la información que comparte (de manera que pueda limitar su acceso a su círculo de "amigos" o incluso exclusivamente para él), no se indica información específica respecto al tratamiento de estos datos por parte de Facebook, de las aplicaciones, sitios web o integraciones de terceros y/o de sus socios externos.

- **Principio de Responsabilidad Proactiva y Seguridad del Tratamiento**

En cuanto a la responsabilidad de Facebook como entidad responsable de tratamiento de datos personales, también encontramos una clara divergencia respecto a las condiciones de uso de la plataforma vigentes para los usuarios de la UE. En el apartado "Límites de responsabilidad", se reconoce la responsabilidad de la empresa en caso de incurrir en algún tipo de negligencia que ocasionara "muerte, lesiones personales o representaciones engañosas" (Facebook, 2019), mientras que en las Condiciones de Servicio vigentes por fuera del territorio de la UE no lo mencionan.

Garantiza, además, que proporcionará sus productos y servicios con "diligencia profesional" y se compromete a brindarlos promoviendo un "entorno seguro y libre de errores" (Facebook, 2019).

Estas aseveraciones respecto a los límites de su responsabilidad difieren sustancialmente de lo estipulado en las Condiciones de Uso a las que podemos acceder por fuera de la UE, por ejemplo, en Argentina. En este caso, la empresa reconoce que pueden existir fallas técnicas o de seguridad en los productos y servicios que proveen:

> Nos esforzamos por proporcionar los mejores Productos posibles y definir pautas claras para todos aquellos que los usen. No obstante, nuestros Productos se proporcionan tal como están y no podemos garantizar que siempre serán seguros, nunca tendrán errores o funcionarán sin interrupciones, demoras o imperfecciones. (Facebook, 2019)

A pesar de manifestar públicamente su recomendación para adoptar las disposiciones del RGPD de manera uniforme, advertimos que la plataforma estipula el alcance de su responsabilidad - en lo relativo al tratamiento que ejerce sobre los datos personales de los usuarios, derivado de su Modelo de negocios[42] - de acuerdo a la normativa vigente en cada país y/o región. Por fuera del ámbito del Reglamento, se introducen disposiciones más laxas en cuanto a la seguridad de los productos y servicios que ofrece a los usuarios:

[42] Consideramos relevante señalar que este trabajo no problematiza sobre la responsabilidad de intermediarios relativa a ilícitos cometidos por terceros. En los casos en que se hace uso del término "Responsabilidad", el mismo se circunscribe al rol ejercido por la empresa Facebook como responsable y encargada del tratamiento de datos personales de sus usuarios tal como lo concibe el RGPD (RGPD, 2016, art.4). Nos interesa abordar específicamente el accionar de esta empresa como plataforma de anuncios publicitarios sobre los datos personales de sus usuarios y los niveles de protección que contempla para ello.

> (...) nuestra responsabilidad se limitará al máximo alcance que la ley aplicable permita, y bajo ninguna circunstancia seremos responsables ante ti por la pérdida de ganancias, ingresos o información, ni por daños consecuentes, especiales, indirectos, ejemplares, punitivos o incidentales que surjan a raíz de estas Condiciones o los Productos de Facebook, o en relación con ellos, incluso si se nos advirtió sobre la posibilidad de que ocurran dichos daños. (Facebook, 2019)

De este apartado podemos extraer como relevante para nuestro caso de estudio que la empresa se desliga de cualquier tipo de pérdida de información del usuario, por lo cual no se contempla ningún tipo de mecanismo de notificación ante una brecha de seguridad que pueda suponer un alto riesgo para la protección de sus datos personales. También excluye su responsabilidad para los casos en que fuera notificada de posibles riesgos, de modo que se desprende que no reconocen la obligación de realizar evaluaciones de impacto en relación al tratamiento de los datos ni la necesidad de tomar medidas adicionales en caso de advertir una posible violación de la protección de los datos. Si bien entendemos que este tipo de obligaciones se desprenden exclusivamente del RGPD, no encontramos en las normativas de la plataforma para el ámbito de la UE una referencia específica a estos mecanismos que se desprenden del principio de Responsabilidad Proactiva, el cual, como hemos mencionado, obliga al responsable del tratamiento a ser capaz de demostrar de qué manera ejerce el cumplimiento de los principios relativos al tratamiento de los datos personales.

- **Consentimiento del interesado**

Como hemos visto, obtener el consentimiento del interesado es una de las condiciones para garantizar la licitud del tratamiento de datos personales. Facebook da cuenta de ello en su Política de Datos de la UE, explicitando los posibles fundamentos de las operaciones de tratamiento que ejerce sobre los datos personales de sus usuarios:

> Recopilamos, usamos y compartimos los datos que tenemos como se indica a continuación: según sea necesario para cumplir con las Condiciones del servicio de Facebook o las Condiciones del servicio de Instagram; de conformidad con tu consentimiento, que puedes revocar en cualquier momento desde la configuración de Facebook y la configuración de Instagram; según sea necesario para cumplir con nuestras obligaciones legales; para proteger tus intereses fundamentales o los de otras personas; según sea necesario para el interés público; y según sea necesario para nuestros intereses legítimos (o los de otras personas), incluidos nuestros intereses en ofrecer un servicio innovador, personalizado, seguro y rentable a nuestros usuarios y socios, a menos que dichos intereses sean invalidados por tus intereses o derechos y libertades fundamentales que requieren la protección de datos personales. (Facebook, 2018)

De esta forma, si bien la empresa considera el consentimiento del interesado como una condición y reserva su derecho de revocación, incluye la posibilidad de resguardar su trabajo sistemático sobre los grandes volúmenes de información y datos personales que hemos advertido anteriormente sobre fundamentos jurídicos relacionados con la protección de intereses legítimos o intereses vitales, por ejemplo.

6. Protección de los datos personales en Argentina

En Argentina, la protección integral de los datos personales está consagrada en la Ley 25.326 de Protección de Datos Personales, sancionada el 4 de octubre de 2000. El país cuenta, además, con el recurso de hábeas data como garantía constitucional para el ejercicio de este derecho, contemplado en el tercer párrafo del artículo 43 de la Constitución Nacional. Este doble reconocimiento es advertido por Cerda Silva (2012) como una tendencia latinoamericana que refuerza los niveles de protección de este derecho:

> (...) el constitucionalismo latinoamericano ha sido más eficiente en la salvaguarda del derecho a la protección de los datos personales. Primero, reconociéndolo como un derecho autónomo. Segundo, proveyéndolo de acciones constitucionales para su protección, ya sea a través de la acción de amparo –conocida como acción de tutela en Colombia; recurso de protección en Chile; y mandado de segurança en Brasil–, o bien, de una acción específica también denominada de habeas data. (p.169)

La Ley 25.326 de Protección de Datos Personales se reglamentó a través del Decreto 1558/2001, a partir del cual se creó la Dirección Nacional de Protección de Datos Personales (DNPDP) - en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos - como órgano de control.

Se han realizado varias modificaciones a esta Ley, de las cuales cabe mencionar como incorporaciones o normas complementarias:

- Año 2008: La incorporación del artículo 47 a través de la Ley 26.343, que establece disposiciones específicas sobre el tiempo de conservación de los datos para los bancos de datos destinados a la prestación de servicios de información crediticia.

- Año 2009: Se establece que toda comunicación con fines publicitarios, deba informar obligatoriamente sobre los derechos del titular de datos de retiro o bloqueo de su nombre de los bancos de datos creados con fines de publicidad, además del deber de incluir los mecanismos previstos para el ejercicio efectivo de estos derechos, de acuerdo a la Disposición 4/2009 de la DNPDP.

- Año 2010: A través del Decreto 1160/2010, se modificó el procedimiento para la aplicación de sanciones establecido en el artículo 31 del Anexo I del Decreto reglamentario 1558/01. De acuerdo a sus considerandos, esta modificación se realiza para brindar una mayor precisión y simplificar la labor de la DNPDP en materia de supervisión y control de lo dispuesto por la Ley 25.326.

- Año 2010: Se aprueba la Política de Intercambio Electrónico de Información a través de la Disposición 313/2010 de la Dirección Nacional de Migraciones, con el objeto de adecuar las actividades de esta Dirección a las disposiciones establecidas por la Ley 25.326 en materia de Protección de datos personales.

- Año 2010: Para los casos en que se realice la difusión pública de datos sensibles, se establece la obligación de preservar la identificación del titular del dato a través de mecanismos de disociación o similares, de acuerdo con la Disposición 12/2010 de la DNPDP.

- Año 2012: Se aprueba el Protocolo General de Funcionamiento de Videocámaras en Espacios Públicos que se implementen en el ámbito de Policía Federal Argentina, Gendarmería Nacional, Prefectura Naval Argentina y/o Policía de Seguridad Aeroportuaria, a través de la Resolución Nº 283/2012 del Ministerio de Seguridad.

- Año 2014: Se crea el Registro Nacional “No Llame”, a través de la Ley 26.951, al cual puede incorporarse toda persona física o jurídica que no desee ser contactado telefónicamente con el fin de ofrecer o publicitar bienes o servicios.

- Año 2015: Se introduce una Guía de Buenas Prácticas en Privacidad para el desarrollo de aplicaciones a través de la Disposición 18/2015 de la DNPDP, como instrumento orientativo para el desarrollo de este tipo de activos digitales de acuerdo con los principios de Protección de datos personales.

- Año 2015: Se aprueban las Condiciones de Licitud para la recolección de datos personales a través de VANTs o Drones, según la Disposición 20/2015 de la DNPDP.

- Año 2016: Se sanciona la Ley 27.725 de Derecho de Acceso a la Información Pública, con el objeto de promover el efectivo ejercicio de este derecho, promover la participación ciudadana y la transparencia de la gestión pública. La Ley 27.725 crea además la Agencia de Acceso a la Información Pública.

- Año 2017: A través del Decreto 746/2017 que modifica la Ley de Ministerios, se introduce, además, una modificación a la Ley 27.725, según la cual se designa a la Agencia de Acceso a la Información Pública como Autoridad de Aplicación de la Ley 25.326 de Protección de Datos Personales y se establece como ente autárquico que funcionará con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros.

Además, en el año 2016, por iniciativa de la Dirección Nacional de Protección de Datos Personales - la Autoridad de Control de ese entonces -, se creó una plataforma colaborativa para que representantes del sector público, privado y de la sociedad civil participaran en la redacción de un proyecto de reforma de la Ley 25.326[43]. En septiembre de 2018, fue enviado al Congreso por el Poder Ejecutivo de la Nación. El proyecto de ley actualmente se encuentra en estado parlamentario, fue enviado el 20 de septiembre de 2018 a las Comisiones de Asuntos Constitucionales y de Derechos y Garantías del Senado de la Nación para ser tratado.

Como hemos mencionado, este proceso de reforma coincide con los cambios implementados por la UE con la sanción del Reglamento General de Protección de Datos. Dado que el Reglamento contempla mecanismos de certificación para países externos a la UE que posean un nivel de protección equivalente al propuesto y que Argentina ha sido reconocida con un nivel de protección adecuado según la Directiva anterior a la sanción del Reglamento, es esperable un proceso de revisión de la legislación actual para conservar los niveles de Protección de datos personales aceptables, de manera tal que se facilite el intercambio de información entre ambas regiones, si bien, como señala el Director de la Agencia de Acceso a la Información Pública, Eduardo Bertoni:

> Si queremos adaptar nuestra regulación al RGPD, es importante actualizar nuestro ordenamiento interno. La clave es tratar de avanzar sobre cambios regulatorios que permitan ser considerados un país de legislación adecuada, para facilitar los intercambios de información. Ahora, legislación adecuada es respetar principios generales, no un cortar y pegar del nuevo reglamento europeo.[44]

Cabe señalar, además, que tanto la Directiva europea que el RGPD deroga como la Ley 25.326 argentina fueron sancionadas previamente a la existencia de Facebook y las redes sociales en general.

Considerando que el proyecto de reforma presentado en Argentina vela por adecuarse a los principios generales del RGPD, creemos pertinente estudiarlo en profundidad y realizar un análisis comparativo con los ejes ya desarrollados en este trabajo. Para esto, comenzaremos por desarrollar el marco regulatorio vigente en materia de protección de datos personales para luego avanzar concretamente sobre el proyecto de reforma.

---

[43] Schulkin, J. (2018, 23 de junio). En la era de la big data, cuáles son los 5 cambios que buscan modernizar la Ley de Protección de Datos Personales. *Infobae.* Recuperado de https://www.infobae.com/tecno/2018/06/23/en-la-era-de-la-big-data-cuales-son-los-5-cambios-que-buscan-modernizar-la-ley-de-proteccion-de-datos-personales/

[44] Schulkin, J. (2018, 23 de junio). En la era de la big data, cuáles son los 5 cambios que buscan modernizar la Ley de Protección de Datos Personales. *Infobae.* Recuperado de https://www.infobae.com/tecno/2018/06/23/en-la-era-de-la-big-data-cuales-son-los-5-cambios-que-buscan-modernizar-la-ley-de-proteccion-de-datos-personales/

6.1 Ley 25.326 de Protección de los Datos Personales: Principios de la normativa

La Ley 25.326 tiene por objeto la protección integral de los datos personales tanto para las personas físicas como para las personas de existencia ideal. También propone una categoría especial de dato personal, denominada como dato sensible, para referirse a todos los datos que “revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual” (Ley 25.326, 2000, art.2).

Se advierte en sus principios una marcada inspiración en la legislación europea, ya que pueden establecerse similitudes con algunas de las disposiciones de la Directiva 95/46/CE analizadas. En primer lugar, con el principio de calidad de los datos, según el cual los datos personales recopilados deben ser adecuados y no excesivos de acuerdo a los fines para los que fueran recolectados.

En cuanto a los requisitos para garantizar la licitud del tratamiento, la ley argentina también incorpora el consentimiento del interesado como una de las condiciones, siempre y cuando éste sea otorgado de manera libre, expresa e informada. Al igual que la directiva europea, se contemplan algunas excepciones bajo las cuales sería lícito llevar a cabo el tratamiento de datos personales sin el consentimiento expreso del interesado, pero las circunstancias excepcionales varían. Además de las razones de interés público o por la mediación de un contrato u obligación legal como se estipula en la directiva, la Ley 25.326 contempla esta excepción para los casos en que los datos son obtenidos de “fuentes de acceso público irrestricto”, o si los datos se limitan a “nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio”, y para los casos en que el tratamiento esté a cargo de instituciones financieras sobre la información de sus clientes (Ley 25.326, 2000, art.5). En este caso, advertimos cierta imprecisión en cuanto a la primera excepción, ya que se debería poder identificar de manera clara a qué se refiere la ley con “fuentes de acceso público irrestricto”. En una publicación del Centro de Estudios en Derecho Informático de la Universidad de Chile (Alvarado, 2014), se realiza un análisis de las legislaciones europeas y latinoamericanas - en materia de derecho a la protección de datos personales - que incorporan la noción de “fuente de acceso público irrestricto”. En este trabajo, se destacan aquellas legislaciones que son taxativas en sus definiciones, detallando de manera clara qué tipos de fuentes se encuentran alcanzados por este concepto. Para el autor, en el caso de análisis de la legislación argentina “queda claro que lo dispuesto por la Ley 25.326 es un catálogo abierto que finalmente otorga libertad de interpretación sobre qué soportes quedarían dentro de esta figura, y cuáles no” (Alvarado, 2014, p.212).

Encontramos otra semejanza entre las normativas argentina y europea en las condiciones de transparencia para informar al titular de los datos sobre los fines del tratamiento y los derechos de acceso, rectificación y supresión de los datos que le conciernen, de forma clara y en lenguaje accesible. En cuanto a las definiciones de tratamiento del dato que ambas regulaciones incorporan en su texto, podemos decir que también coinciden en este punto, ya que ambas consideran como tratamiento a cualquier operación que se realice sobre los datos personales de manera automática o manual, ya sea de registro, almacenamiento, conservación, modificación o transmisión, que implique además la cesión de acceso a estos datos a un tercero.

La ley argentina también reconoce un nivel de protección especial para los datos personales que “revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual” (Ley 25.326, 2000, art.2) los cuales son reconocidos como datos sensibles. Esta ley contempla como excepción a la prohibición de su tratamiento los casos en que medien razones de “interés general autorizadas por ley”, o los casos en que los datos sean tratados “con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares (Ley 25.326, 2000, art.7).

En cuanto a la seguridad del tratamiento, ambas imponen la obligación al responsable del tratamiento de implementar todas las medidas necesarias a nivel técnico y organizativo para la prevención de cualquier violación a la seguridad o confidencialidad de los datos, si bien en la ley argentina no se hace referencia a una proporcionalidad de las medidas en relación a los posibles riesgos respecto a las operaciones que se realicen y las categorías de datos que se traten. Por último, la Ley 25.326 también enumera los derechos de acceso, rectificación y supresión del titular sobre sus datos personales.

En relación al caso de estudio seleccionado, cabe destacar que el artículo 27 de la ley argentina se refiere particularmente a las operaciones de tratamiento de datos personales derivadas de actividades con fines publicitarios, venta directa o promocionales. En estos casos, los datos podrán ser tratados para configurar perfiles o hábitos de consumo siempre que el titular haya otorgado el consentimiento expreso para ello, o los datos a tratar figuren en documentos accesibles al público.

Sobre este último punto, cabe preguntarse si la definición de documentos accesibles al público podría facilitar también el tratamiento de los datos personales por parte de Facebook sin un consentimiento expreso de los usuarios.

Como hemos mencionado anteriormente, además, la ley dispone en su capítulo VII los procedimientos de la acción de protección de datos personales o de hábeas data, la cual podrá ejercerse para conocer los datos personales almacenados y sus fines o para ejercer el derecho de rectificación, supresión, confidencialidad o actualización.

6.2 Proyecto de reforma de la Ley 25.326 de Protección de Datos Personales

En función de las observaciones realizadas en el apartado anterior, es interesante indagar sobre la propuesta enviada por el Poder Ejecutivo al Congreso de la Nación el 19 de septiembre de 2018 a través del Mensaje 147/2018 para la reforma de la Ley 25.326 y su relación con los principios y disposiciones del RGPD.

Entre las incorporaciones del proyecto de reforma se destacan los cambios en las definiciones que figuran en el artículo 2, como es el caso de la definición de datos personales, la cual se restringe en el proyecto a toda información referida únicamente a “personas humanas” - ya no se incluyen las personas de existencia ideal -, además de incorporar explícitamente los datos biométricos y genéticos dentro de esta definición.

Respecto a la definición de datos sensibles, se advierte la inclusión de los posibles riesgos que pueden ocasionar su tratamiento, entendidos como “datos personales que afectan la esfera íntima de su titular con potencialidad de originar una discriminación ilícita o arbitraria” (Proyecto de Ley de Protección de Datos Personales, 2018, art.2). En cuanto a las condiciones para su tratamiento, en el artículo 16 se determina su prohibición, considerando las excepciones también contempladas en el RGPD. En este punto cobra importancia la disociación de datos, otra de las definiciones incorporadas, entendida como un mecanismo de tratamiento de datos según el cual se impide que el titular sea identificado (similar al mecanismo de “seudonimización” que incluye el RGPD). Se estipula la implementación obligatoria de este procedimiento para los casos de tratamiento de datos sensibles con fines estadísticos, científicos o históricos.

También se diferencian las figuras de Responsable y Encargado del tratamiento, mientras que la Ley 25.326 sólo hace referencia al responsable del archivo o base de datos.

En cuanto al ámbito de aplicación, el proyecto amplía su alcance, al igual que el RGPD, para garantizar la protección de datos personales de todos los titulares de datos que residan en Argentina, aunque el responsable del tratamiento no se encuentre establecido en el país - para los casos en que las operaciones de tratamiento estén vinculadas a la oferta de bienes y servicios o al seguimiento del comportamiento-, si bien se incluye como excepción que en el lugar donde resida el responsable del tratamiento exista una ley que proteja aún más los derechos del interesado. También se considera aplicable cuando el responsable del

tratamiento se encuentre establecido en el país, aunque las operaciones de tratamiento se realicen fuera del territorio, y para los casos en que el responsable se encuentre establecido en un país o región donde se aplique la legislación argentina de acuerdo a tratados internacionales (Proyecto de Ley de Protección de Datos Personales, 2018, art.4).

Sobre los principios relativos al tratamiento de datos (Proyecto de Ley de Protección de Datos Personales, 2018, cap.2) podemos señalar que se explicitan como principios diferenciados algunos elementos ya contenidos en la Ley 25.326, como el principio de lealtad y transparencia (art.5), el de finalidad (art.6) y el de exactitud (art.8), los cuales apuntan a clarificar las finalidades para las cuales son tratados los datos y que éstas no sean incompatibles con el nivel de datos requerido. En esta misma línea, se incorpora el principio de minimización de datos (art.7), el cual refuerza la idea de que los datos personales recopilados no deben ser excesivos respecto a los fines declarados por el responsable. El principio de exactitud, además, resalta los derechos del titular de los datos a rectificar o suprimir su información en caso que este principio no se cumpla. Siguiendo lo dispuesto por el RGPD, también se incorpora un límite al plazo de conservación de los datos, el cual está dado según el cumplimiento de los fines para los cuales fueron recolectados. Ambos, además, incluyen como excepción a esta regla los casos en que los datos fueran tratados “con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos” (Proyecto de Ley de Protección de Datos Personales, 2018, art. 9).

Por último, se incorpora el principio de responsabilidad proactiva (art.10), el cual, como hemos visto en el caso del RGPD, impone al responsable la obligación de cumplimiento de todo lo dispuesto y que sea capaz de demostrarlo. Con el fin de garantizar este principio, encontramos incorporados dentro de las obligaciones del responsable del tratamiento (Proyecto de Ley de Protección de Datos Personales, 2018, cap. 4) la protección de datos desde el diseño y por defecto, la realización de evaluaciones de impacto para los casos en que se perciba un alto riesgo para los derechos de los titulares y el informe consecuente a la autoridad de control, procedimientos también reconocidos por el RGPD como obligaciones del responsable.

Al igual que el RGPD, se enumeran las bases jurídicas posibles según las cuales puede garantizarse un tratamiento de datos personales lícito. Éstas coinciden en su totalidad con las reconocidas por el reglamento europeo, si bien se incorpora, además, que el tratamiento de datos sea legítimo si se realiza “sobre datos que figuren en fuentes de acceso público irrestricto” (Proyecto de Ley de Protección de Datos Personales, 2018, art.11). Como hemos visto en el caso de la Ley 25.326, este concepto puede representar cierta ambigüedad. Sin embargo, el proyecto incluye una definición sobre lo que se considera como “fuente de acceso

público irrestricto" - a diferencia de la Ley 25.326 -, entendida como: "La que contiene información destinada a ser difundida al público, de libre acceso e intercambio por razones de interés general, accesible ya sea en forma gratuita o mediante una contraprestación" (Proyecto de Ley de Protección de Datos Personales, 2018, art.2).

Eduardo Ferreyra, abogado y analista de políticas públicas del Área Digital de la Asociación por los Derechos Civiles (2018) analiza el proyecto de ley y advierte sobre los riesgos que esta disposición podría ocasionar teniendo en cuenta las técnicas de recolección de datos a través de Internet:

> Con el actual desarrollo tecnológico, la recolección de información que las personas dejan a través de Internet y otros entornos digitales se ha convertido en una herramienta que permite la elaboración de perfiles y el ejercicio de actividades de vigilancia sobre los individuos. Esto ha llevado a que la investigación de fuentes abiertas sea uno de los principales métodos utilizados por las fuerzas de seguridad en Argentina. (Asociación por los Derechos Civiles, 2018, p.5)

En este informe, se destaca la importancia de introducir algún tipo de limitación a esta excepción, que permita ejercer un mayor control sobre las actividades de tratamiento basadas en fuentes de acceso público irrestricto, cuyo fin sea la elaboración de perfiles o tareas de vigilancia:

> (...) el hecho de que dichas prácticas se realicen en base a datos surgidos de fuentes consideradas de "acceso público irrestricto" no debe ser un justificativo para otorgar una discrecionalidad absoluta a los responsables o encargados de un tratamiento de esa naturaleza. En consecuencia, consideramos que, si el tratamiento y la cesión de datos basado en fuentes de este tipo tiene por objeto la realización de actividades de perfilamiento o profiling, vigilancia u otra actividad sensible, debería contar con el consentimiento del titular de datos, sin perjuicio del cumplimiento de las demás garantías que la ley establece. (Asociación por los Derechos Civiles, 2018, p.5)

Respecto a las restantes bases jurídicas para la licitud del tratamiento, cabe destacar que, si bien el proyecto reconoce como el RGPD que el tratamiento de datos es lícito cuando se realice en el contexto de las actividades de los poderes del Estado, aporta cierta ambigüedad para los casos en que el responsable de datos es un organismo público o un organismo de las fuerzas de seguridad. En el artículo 36, contempla algunas excepciones de acuerdo con las cuales podría anularse el ejercicio de los derechos de acceso, rectificación, oposición, supresión, portabilidad de datos "en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros" (Proyecto de Ley de Protección de Datos Personales, 2018, art.36). Este artículo incorpora

imprecisiones para asegurar el ejercicio de los derechos del titular de los datos, lo cual afectaría el objetivo mismo de la ley.

Considerando también el consentimiento del titular como una de las bases jurídicas para un tratamiento lícito de los datos personales, este proyecto incorpora la posibilidad de obtener el consentimiento de manera tácita por parte del titular para los casos en que “surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización” (Proyecto de Ley de Protección de Datos Personales, 2018, art.12). Esta modalidad para prestar consentimiento no está incluida en el RGPD. A instancias del análisis antes desarrollado respecto al funcionamiento de una red social como Facebook (y las posibilidades de diseño de su arquitectura y protocolos), la inclusión de un mecanismo de este tipo al momento de aceptar el tratamiento de los datos personales implicaría nuevas tensiones respecto al nivel de protección garantizado. Sí se admite, en línea con el RGPD, el derecho del titular a revocar el consentimiento previamente otorgado.

En relación al tratamiento de datos personales de niños y adolescentes, el proyecto incorpora condiciones especiales de acuerdo con el RGPD, además de priorizar la garantía de los derechos del niño consagrados a nivel internacional en la Convención de los Derechos del Niño.

El proyecto de ley también enumera de manera específica la información que debe comunicar el responsable de manera obligatoria al titular de datos en el artículo 15, la cual también coincide con lo dispuesto en el RGPD, si bien se exceptúa la determinación del plazo de conservación de los datos y la información de contacto del Delegado de Protección de Datos.

En cuanto a la seguridad del tratamiento – contemplada en el artículo 19 -, el proyecto incorpora la evaluación del riesgo inherente según la naturaleza del dato personal para que el responsable considere las medidas necesarias a implementar en función de ello. Además, debe tener en cuenta si se trata de datos sensibles, la tecnología disponible, las consecuencias sobre los derechos del titular en caso de una violación de seguridad y si tienen un historial de violaciones de seguridad previas en el desarrollo de sus actividades de tratamiento.

Para estos casos, también se impone obligatoriamente un mecanismo de notificación a la autoridad de control ante una brecha de seguridad y al titular de los datos en los casos en que ésta represente un riesgo alto para él. Esta misma excepción es incorporada por el RGPD, la cual puede fomentar estrategias de discrecionalidad entre los responsables del

tratamiento, ya que queda a su cargo tanto la evaluación de estos riesgos como la decisión de notificar al titular.

Como hemos adelantado en los párrafos anteriores, el proyecto de ley también contempla los derechos del titular garantizados en el RGPD, estipulados en el capítulo 3. Encontramos en él los derechos de acceso, rectificación, a ser informado por el responsable de manera clara bajo el principio de transparencia, de oposición, de supresión y de portabilidad de los datos.

Otra semejanza está relacionada con las decisiones automatizadas y la elaboración de perfiles, ya que tanto el proyecto – en el artículo 32 - como el RGPD admiten el derecho de oposición del titular a este tipo de procedimientos, exceptuando los casos en que sean necesarios para la ejecución de un contrato, se autorice por ley, o si el titular brindó su consentimiento expreso para ser objeto de este tipo de prácticas.

El proyecto de reforma también incorpora la figura del Delegado de Protección de Datos en el artículo 43, de designación obligatoria para los casos en que el responsable sea un organismo público, si las operaciones de tratamiento se realizan sobre datos sensibles como actividad principal del organismo responsable, o los casos en que se realicen operaciones de tratamiento a gran escala.

En el artículo 68 del proyecto se incorpora una referencia específica a las bases de datos “destinadas a la publicidad”. Si se persiguen fines publicitarios o la oferta de bienes y servicios, se admite la licitud del tratamiento de los datos sin el consentimiento del titular. En estos casos, la condición admitida es que se utilicen los datos para la elaboración de perfiles en función de intereses y patrones de comportamiento y que los titulares no sean identificados de manera particular, sino exclusivamente dentro de estos grupos genéricos por categoría. La ley vigente contempla la licitud del tratamiento para estos casos siempre que los datos figuren en documentos públicos o el titular haya otorgado el consentimiento para esto.

Una eventual revisión de la Ley 25.326, sancionada en el año 2000 – anterior a la existencia de las plataformas de redes sociales -, propiciaría una actualización de la normativa, de modo tal que incorpore las nuevas TIC y las múltiples técnicas de procesamiento de la información. Esto se traduciría, teniendo en cuenta lo analizado en relación al funcionamiento de Facebook, en numerosas alternativas en que los datos personales pueden ser recopilados, almacenados y tratados con diferentes propósitos.

Estudiar estas nuevas realidades posibilitadas por la técnica y movilizadas por los intereses económicos de las grandes empresas de tecnología, permitiría un reconocimiento de la compleja situación del usuario al momento de identificar los mecanismos sobre los que

descansan estas plataformas, el tratamiento que realizan sobre sus datos y los riesgos que pudiera generar un tratamiento inadecuado.

Luego de un análisis del proyecto de reforma presentado por el PEN, puede apreciarse la incorporación de algunos de los principios y valores que el RGPD impone para la protección de los datos personales. Podría ejercerse un mayor control sobre algunas cuestiones, para evitar ciertos casos de ambigüedad o imprecisiones que pudieran derivar en una vulneración de los derechos y libertades fundamentales del titular de los datos. Tal es el caso de la inclusión del consentimiento tácito como fundamento para la licitud del tratamiento de datos personales, lo cual se aleja profundamente de los niveles de protección propuestos por la UE. También hemos señalado la ambigüedad que propone la definición de "fuentes de acceso público irrestricto", sobre las cuales sería lícito realizar cualquier operación de tratamiento sin la necesidad del consentimiento del titular. Este elemento tampoco es considerado por el RGPD y creemos que puede generar imprecisiones al momento de la definición de, por ejemplo, si se debe considerar a las plataformas de redes sociales como un tipo de fuente de acceso público irrestricto. En todo caso, podría contemplarse una definición más detallada de lo que la normativa considera dentro de esta definición.

Otro punto a considerar se vincula con la precisión sobre los casos de excepción para los derechos del interesado. Específicamente nos referimos a los casos en que el responsable del tratamiento sea un organismo público o un organismo de las fuerzas de seguridad, el cual puede anular el ejercicio de los derechos del titular de los datos por razones de seguridad, orden y/o defensa de la Nación. Creemos que la excepción de derechos es un elemento determinante y que, por lo tanto, debería exigirse una mayor explicitación sobre los casos en que esto pudiera ocurrir.

7. Conclusiones

El estudio de Facebook como plataforma de red social y de anuncios publicitarios a partir de sus elementos constitutivos: Propiedad, Gobierno, Modelo de Negocios, Tecnología, Usuarios y Contenido (Van Dijck, 2016) permitió comprender su lógica de funcionamiento y las estrategias de comercialización que la sustentan. De esto se desprende un modelo de creación de valor específico, basado en la generación de comunidades y contenido en línea para conseguir la materia prima de su sistema de producción: "(Facebook) representa un ejemplo de una plataforma publicitaria en la que el valor se basa esencialmente en un proceso de expropiación de las destrezas vitales de las personas" (Fumagalli et. al., 2018, p.15). De esta manera, se advierte la relevancia de la información personal de los usuarios y el tratamiento sistemático de los datos personales a gran escala para su Modelo de Negocios actual.

Si bien, en su Lógica de Gobierno, la empresa explicita algunas cuestiones sobre estas actividades de recolección y análisis de la información, hemos visto cómo en la práctica, se ha vulnerado en muchos casos la protección de los datos personales de los usuarios, en gran medida a partir de la cesión de datos a terceros sin el consentimiento de los titulares. Esto ha generado numerosas controversias en Estados Unidos y la Unión Europea, por las que la empresa ha sido sancionada en el marco de las regulaciones vigentes sobre la protección de datos personales.

Como hemos analizado, la entrada en vigencia del RGPD impone nuevos estándares de protección a los datos personales, incluyendo de manera taxativa mayores obligaciones para los responsables y encargados del tratamiento. Los cambios introducidos por el Reglamento europeo representan un avance significativo para la protección de los datos personales, ya que incorporan aspectos y problemáticas presentes en la lógica de Gobierno y Tecnología de las plataformas de redes sociales y en el caso de Facebook en particular, analizados en este trabajo. Elementos como la protección de datos desde el diseño y por defecto, la incorporación de los datos biométricos como categoría especial de datos personales, la ampliación del alcance de su ámbito de aplicación, proponen una actualización de la normativa que busca adaptarse a la multiplicidad de funcionalidades de las TIC y sus posibles arquitecturas o códigos. Por ejemplo, la herramienta de reconocimiento facial incorporada por Facebook ahora es alcanzada por este reglamento y con un nivel de protección especial, gracias a la incorporación de la definición de datos biométricos como categoría especial de datos personales. Un ámbito de aplicación que ya no depende exclusivamente del establecimiento físico de la empresa responsable del tratamiento o de dónde se realice el

tratamiento, se ajusta también a los regímenes de Propiedad actuales de las grandes empresas de tecnología.

Como hemos visto, la Lógica de Gobierno de Facebook - explicitada en sus Condiciones de Servicio y Política de Datos -, retoma muchos de estos aspectos para adecuarse al nuevo marco regulatorio. Además, su Fundador y Director Ejecutivo, Mark Zuckerberg, ha promovido de manera pública las disposiciones del RGPD como marco común a nivel global para la protección de la privacidad y de la información:

> Creo que sería bueno para Internet si más países adoptaran regulaciones como el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) como marco común. La nueva regulación de privacidad en los Estados Unidos y en todo el mundo debería basarse en las protecciones que proporciona el GDPR. (Zuckerberg, 2019).

No obstante, cabe señalar que la opinión del fundador de la compañía sobre la regulación de la privacidad y la protección de datos personales no ha sido siempre la misma. Su manifiesto apoyo a la regulación europea se da en el marco de las acusaciones por filtración de datos tanto en EEUU como en la UE y las consecuentes multas a la empresa, mientras que en el año 2010 afirmaba que sus políticas de privacidad debían adaptarse a los cambios en las normas sociales, las cuales, según él, apuntaban a una mayor difusión de la información personal: "La gente se siente realmente cómoda no sólo compartiendo más información, sino compartiéndola por diferentes medios, de forma más abierta y con más gente"[45].

Es posible identificar como un avance significativo ciertas incorporaciones, como la explicitación de su Modelo de Negocios - que implica una descripción pormenorizada de las diferentes finalidades para las cuales es utilizada la información del usuario -, la posibilidad de configurar ciertas limitaciones a los modos en que el usuario interactúa con los anuncios publicitarios mostrados por Facebook y las herramientas de acceso a la información del usuario, disponible para su consulta y descarga.

Sin embargo, hemos detectado que este tipo de funcionalidades no proveen un acceso a la información de manera exhaustiva, dado que grandes volúmenes de información proveída por socios externos o sitios web de terceros no se facilita a partir de las herramientas de Facebook. En cuanto al ejercicio de los derechos del usuario, no se identifica un acceso efectivo a la totalidad de los datos personales que la red social dispone, además de la cantidad y tipo de datos que la empresa comparte o no con terceros.

[45] Mark Zuckerberg, Facebook: "La Edad de la Privacidad ha terminado". (2010, 10 de enero). *Ticbeat.* Recuperado de https://www.ticbeat.com/entrevistas/facebook-la-edad-privacidad-ha-terminado/

Tampoco son accesibles las bases de datos que los anunciantes comparten en la plataforma a partir de la información recopilada de sus clientes en otros canales. De esto se desprende, además, un ejercicio poco efectivo del resto de los derechos contemplados por el RGPD dado el desconocimiento de los datos personales que la red social y sus socios tratan.

En cuanto a los datos personales de categoría especial, sería oportuno que la plataforma estipule específicamente sobre qué base jurídica fundamenta el tratamiento de estos datos y que en sus configuraciones por defecto para la publicación de estos datos no se estipule el alcance público como predeterminado.

También se introduce cierta ambigüedad con el uso del interés legítimo como fundamento para las operaciones de tratamiento. En este caso, es necesaria una explicitación de los intereses legítimos que la empresa persigue y que podrían imponerse sobre los derechos y libertades fundamentales de los usuarios, tal como lo dispone el RGPD en su artículo 14 sobre la informaciòn que debe facilitarse al interesado.

Tanto la normativa europea como el proyecto de reforma de la normativa argentina apuntan a un mayor control de las operaciones de tratamiento de datos personales, pero consideran también como un elemento relevante una mayor información y transparencia respecto al titular de los datos. La difusión de este derecho por parte de los organismos del Estado y las organizaciones de la sociedad civil, fortalecería los valores de esta ley, propiciando un mayor conocimiento del usuario sobre sus derechos y los riesgos que podrían derivar del tratamiento sistemático de sus datos personales, además de reconocer de qué manera funcionan las plataformas de redes sociales y por qué se dedican sistemáticamente a recolectar estos datos, de modo tal que puedan tomar una decisión informada al momento de registrarse en ellas y acceder a su uso.

Creemos que estas acciones, sumadas a una firme voluntad política que promueva los estándares impulsados por el RGPD hacia una mayor regulabilidad del ciberespacio (Lessig, 1998, p.5), pueden fortalecer la posición de cada usuario respecto a las reglas implícitas y explícitas que configuran las plataformas de redes sociales en todos sus componentes.

Es necesario también un trabajo constante de control y supervisión para la aplicación de la norma y de las políticas que cada plataforma define internamente, adecuándose en mayor o menor medida a la regulación vigente. Como hemos visto, ya se ha sancionado a algunas empresas de diferentes Estados miembro de la UE en virtud de lo dispuesto por el RGPD y sus operaciones de tratamiento de datos personales. Estos ejemplos de aplicación de la norma pueden resultar útiles para tomar como referencia en el análisis del proyecto de reforma de la Ley 25.326 en Argentina.

Resulta pertinente profundizar en el estudio de las tensiones emergentes del tratamiento de datos personales en las plataformas digitales. Una posible línea de investigación podría abordar el análisis de las condiciones de servicio de otras plataformas de anuncios publicitarios, como por ejemplo Google, a la luz de las tendencias regulatorias analizadas.

También podría emprenderse una línea de investigación que problematice la situación de las empresas extranjeras que deban adaptarse a la regulación europea por realizar operaciones de tratamiento sobre datos personales de ciudadanos de la UE.

8. Referencias bibliográficas

A Privacy-Focused Vision for Social Networking. (2019, 6 de marzo). Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2019/03/vision-for-social-networking/

Alvarado, F. (2014). Las fuentes de acceso público a datos personales. *Revista chilena de derecho y tecnología*, *3*(2), 225-226. doi: 10.5354/0719-2584.2014.33276

Álvarez Ugarte, R. (2013). La privacidad y las noticias exageradas sobre su muerte En B. Girard & F. Perini (Ed.), *Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe* (163-167). Montevideo - Ottawa: Fundación Comunica - IDRC.

Asociación por los Derechos Civiles (2018). *Análisis inicial del proyecto de ley de protección de datos personales de Argentina.* Recuperado de https://adcdigital.org.ar/wp-content/uploads/2018/10/ADC-Analisis-Reforma-LPDP.pdf

Budaraju, H. (2017, 27 de septiembre). Introducing a New Feature in India to Help Increase Blood Donations. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2017/09/blood-donations-in-india/

Budaraju, H. (2018, 13 de junio). Making it Easier to Donate Blood. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2018/06/making-it-easier-to-donate-blood/

Busaniche, B. (2013). La vida de los otros. En B. Girard & F. Perini (Ed.), *Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe* (169-176). Montevideo - Ottawa: Fundación Comunica - IDRC.

Castells, M. (1995). La ciudad informacional: tecnologías de la información, reestructuración económica y el proceso urbano-regional. Madrid: Alianza Editorial.

Castells, M. (2009). Comunicación y Poder. Madrid: Alianza Editorial.

Cerda Silva, A. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. Recuperado de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-68512011000100009

Cerda Silva, A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. En E. Bertoni (Ed.), *Hacia una Internet libre de censura* (165-180). Buenos Aires: Universidad de Palermo.

Cortés, C. (2012). Vigilancia de la Red. Qué significa monitorear y detectar contenidos en Internet. Recuperado de https://www.palermo.edu/cele/pdf/El-deseo-de-observar-la-red.pdf

Danker, D. (2017, 9 de agosto). Introducing Watch, a New Platform For Shows On Facebook. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2017/08/introducing-watch-a-new-platform-for-shows-on-facebook/

De Gràcia, C. (2013). ¿Está muerta la privacidad? Algunas reflexiones a modo de respuesta. En B. Girard & F. Perini (Ed.), *Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe* (147-152). Montevideo - Ottawa: Fundación Comunica - IDRC.

Egan, E. (2018, 18 de abril). Cumpliendo con las nuevas leyes de privacidad y ofreciendo nuevas protecciones de privacidad a todos, independientemente de dónde vivan. Facebook Newsroom. Recuperado de https://ltam.newsroom.fb.com/news/2018/04/cumplir-con-las-nuevas-leyes-de-privacidad-y-ofrecer-nuevas-protecciones-de-privacidad-a-todos-independientemente-de-donde-vivan/

Facebook (2018). Política de datos de Facebook de la UE. Disponible en https://docs.google.com/document/d/1emc_2mfrx7YhexAW4VIbGxsEG4BPQpjJsP4GNkkaIZc/edit?usp=sharing

Facebook (2018) Política de datos de Facebook en Argentina. Disponible en https://docs.google.com/document/d/1zvNO4xY17QEAolrZVoHHbPKe1qgr_P75ax-8cJ4ROHk/edit

Facebook (2019) Condiciones del servicio de Facebook en Argentina. Disponible en https://docs.google.com/document/d/12iEyYd515rybohW_rywwKZdhCdwbri1ZxO4pDtHjAVA/edit?usp=sharing

Facebook (2019). Condiciones del servicio de Facebook de la UE. Disponible en https://docs.google.com/document/d/17affW3HQHx9NK1CInju2Wq7P_CqOap2AlbrST5hvxr8/edit?usp=sharing

Facebook Announces Pricing of Initial Public Offering. (2012, 17 de mayo). Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2012/05/facebook-announces-pricing-of-initial-public-offering/

Facebook Newsroom (2016-2019). Información de la empresa. Recuperado de https://ltam.newsroom.fb.com/company-info/

Facebook to Acquire Instagram. (2012, 9 de abril). Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2012/04/facebook-to-acquire-instagram/

Facebook to Acquire WhatsApp. (2014, 19 de febrero de 2014). Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/

Fumagalli, A., Lucarelli, S., Musolino, E., & Rocchi, G. (2018). El trabajo (labour) digital en la economía de plataforma: el caso de Facebook. *Hipertextos, 6*(9), 12-40. Recuperado de http://revistahipertextos.org/wp-content/uploads/2015/12/Hipertextos-nro-9-final.pdf

Gendler, M. (2018). Gubernamentalidad algorítmica, redes sociales y neutralidad de la red. Avatares de la Comunicación y la Cultura, 15.

Krug, S. (2016, 24 de febrero). Reactions Now Available Globally. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2016/02/reactions-now-available-globally/

Ku, M. (2016, 3 de octubre). Introducing Marketplace: Buy and Sell With Your Local Community. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2016/10/introducing-marketplace-buy-and-sell-with-your-local-community

Lessig, L. (1998). Las leyes del ciberespacio. Recuperado de http://www.uned.es/ntedu/espanol/master/segundo/modulos/audiencias-y-nuevos-medios/ciberesp.htm

Magnani, E. (2014). Tensión en la red. Libertad y control en la era digital. Buenos Aires: Autoría Sherpa.

Milt, K. (2019, mayo). La protección de los datos personales. Fichas temáticas sobre la Unión Europea. Recuperado de http://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

Nissenbaum, H. (2011). Privacidad amenazada: tecnología, política y la integridad de la vida social. México, DF: Editorial Océano.

Rodríguez, K. (2013). El espionaje en Internet en América Latina. En B. Girard & F. Perini (Ed.), *Habilitando la apertura: el futuro de la sociedad de la información en América Latina y el Caribe* (153-162). Montevideo - Ottawa: Fundación Comunica - IDRC.

Rosenberg, S. (2015, 16 de diciembre). Introducing Transportation on Messenger. Facebook Newsroom. Recuperado de https://newsroom.fb.com/news/2015/12/introducing-transportation-on-messenger/

Van Dijck, J. (2016), La cultura de la conectividad: una historia crítica de las redes sociales. Buenos Aires: Siglo XXI.

Villegas Carrasquilla, L. (2012), Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet. En E. Bertoni (Ed.), *Hacia una Internet libre de censura* (125-164). Buenos Aires: Universidad de Palermo.

Web oficial de la Unión Europea. Reglamentos, directivas y otros actos legislativos. Recuperado de https://europa.eu/european-union/eu-law/legal-acts_es

Welcome to Facebook, everyone. (2006, 26 de septiembre). Facebook. Recuperado de https://www.facebook.com/notes/facebook/welcome-to-facebook-everyone/2210227130

Zuckerberg, M. (2019, 30 de marzo). Cuatro ideas para regular el Internet. Facebook Newsroom. Recuperado de: https://ltam.newsroom.fb.com/news/2019/03/cuatro-ideas-para-regular-el-internet/

8.1 Legislación

Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas. Niza, 7 de diciembre de 2000.

Convención Americana sobre Derechos Humanos. Organización de los Estados Americanos. San José, Costa Rica, 22 de noviembre de 1969.

Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Diario Oficial de la Unión Europea, Estrasburgo, 28 de enero de 1981.

Decisión C(2003) 1731 sobre la adecuación de la protección de los datos personales en Argentina. Comisión de las Comunidades Europeas. Bruselas, 30 de junio de 2003.

Declaración Americana de los Derechos y Deberes del Hombre. Comisión Interamericana de Derechos Humanos. Bogotá, Colombia, 1948.

Declaración Universal de los Derechos Humanos. Asamblea General de las Naciones Unidas. París, 10 de diciembre de 1948.

Decreto N° 1160/2010. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 13 de agosto de 2010.

Decreto N° 1558/2001. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 29 de noviembre de 2001.

Decreto N° 746/2017. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 25 de septiembre de 2017.

Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina. Grupo de Trabajo del art. 29 de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales. Unión Europea, 3 de octubre de 2002.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Diario Oficial de las Comunidades Europeas, Bruselas, 12 de julio de 2002.

Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

circulación de esos datos. Diario Oficial de la Unión Europea, Luxemburgo, 24 de octubre de 1995.

Disposición N° 12/2010 de la Dirección Nacional de Protección de Datos Personales. Boletín oficial de la República Argentina, Buenos Aires, 28 de junio de 2010.

Disposición N° 18/2015 de la Dirección Nacional de Protección de Datos Personales. Boletín oficial de la República Argentina, Buenos Aires, 16 de abril de 2015.

Disposición N° 20/2015 de la Dirección Nacional de Protección de Datos Personales. Boletín oficial de la República Argentina, Buenos Aires, 27 de mayo de 2015.

Disposición N° 313/2010 de la Dirección Nacional de Protección de Datos Personales. Boletín oficial de la República Argentina, Buenos Aires, 5 de marzo de 2010.

Disposición N° 4/2009 de la Dirección Nacional de Protección de Datos Personales. Boletín oficial de la República Argentina, Buenos Aires, 10 de marzo de 2009.

Ley de Acceso a la Información Pública comentada. Publicación de la Secretaría de Asuntos Políticos e Institucionales Ministerio del Interior, Obras Públicas y Vivienda de la Nación. Buenos Aires, Argentina, Año 2016. Recuperada el 2/07/19 de https://www.argentina.gob.ar/sites/default/files/ley-27275-comentada.pdf

Ley N° 25.326. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 02 de noviembre de 2000.

Ley N° 26.343. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 9 de enero de 2018.

Ley N° 26.951. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 5 de agosto de 2014.

Ley N° 27.275. Boletín oficial de la República Argentina, Buenos Aires, Argentina, 29 de septiembre de 2016.

Mensaje 147/2018 y Proyecto de Ley de Protección de Datos Personales. Buenos Aires, Argentina, 19 de septiembre de 2018. Recuperado de https://www.senado.gov.ar/parlamentario/comisiones/verExp/283.18/PE/PL

Pacto Internacional de Derechos Civiles y Políticos. Asamblea General de las Naciones Unidas. 16 de diciembre de 1966.

Protocolo adicional al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos. Diario Oficial de la Unión Europea, Estrasburgo, 8 de noviembre de 2001.

Reglamento 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, Bruselas, 27 de abril de 2016.

Resolución Nº 283/2012 del Ministerio de Seguridad. Boletín oficial de la República Argentina, Buenos Aires, 20 de abril de 2012.