

*Cómo citar este texto:*

Salvador Benítez, A. (2019). Entre la privacidad y el negocio. Condiciones de uso y política de datos en redes sociales. *Derecom*, 27, 139-161. <http://www.derecom.com/derecom/>

## **ENTRE LA PRIVACIDAD Y EL NEGOCIO. CONDICIONES DE USO Y POLITICA DE DATOS EN REDES SOCIALES**

## **BETWEEN PRIVACY AND BUSINESS. TERMS OF USE AND DATA POLICY IN SOCIAL NETWORKS**

© Antonia Salvador Benítez  
Universidad Complutense de Madrid (España)  
[asalvado@ucm.es](mailto:asalvado@ucm.es)

### **Resumen**

La transformación digital constituye un factor para el crecimiento económico de las empresas, a la vez que implica importantes desafíos en materia de protección de datos personales, tema que en los últimos años se ha convertido en prioridad. El último hito ha sido la entrada en vigor de la nueva normativa europea, el Reglamento General de Protección de Datos (RGPD). En este escenario, las redes sociales tienen un gran protagonismo y son empleadas cada vez más por los usuarios para relacionarse con las empresas, intercambiando gran cantidad de información personal. En este trabajo se analizan las condiciones de uso y políticas de datos de las redes sociales Facebook, Twitter, Instagram, Youtube y WhatsApp- con el fin de poner de relieve cuánta información y de qué tipo estamos compartiendo, y quién tiene acceso a ella. Asimismo, se revisa el RGPD, identificando las principales novedades en materia de protección de datos y se analiza en qué medida las plataformas de redes sociales han adaptado sus políticas de privacidad a la nueva normativa.

### **Summary**

The digital transformation is a key factor for the economic growth of companies, at the same time as it implies important challenges in terms of protection of personal data, that has become a priority in recent years. The last milestone has been the entry into force of the new European regulations, the General Data Protection Regulation (GDPR). Social networks have a great role and are increasingly used by users to interact with companies, exchanging a large amount of personal information. In the present work we analyze the terms of use and data policies of social networks Facebook, Twitter, Instagram, YouTube and WhatsApp - in order to highlight how much information and what kind of information we are sharing, and who has access to it. Likewise, the GDPR is reviewed, identifying the main novelties in terms of data protection and

analyzing the extent to which social network platforms have adapted their privacy policies to the new regulations.

**Palabras clave:** Condiciones de uso. Contenidos. Datos personales. Políticas de privacidad. Protección de datos. Redes sociales.

**Keywords:** Conditions of use. Contents. Personal data. Privacy policies. Data protection. Social networks.

## 1. Introducción.

En la actualidad, la mayoría de los movimientos y actividades que se llevan a cabo en la Red están estrechamente relacionados con las redes sociales, consideradas por muchos usuarios y empresas como una herramienta de comunicación, *networking* y productividad indispensable. Así lo revela el IX Estudio Anual de Redes Sociales 2018 elaborado por IAB Spain y Elogia. Todas las interacciones con estas plataformas exigen al usuario la cesión de datos personales mediante la aceptación de condiciones de uso y políticas de privacidad que a menudo desconoce o no comprende y que afectan al tratamiento de sus datos, de su intimidad y vida privada y por extensión a los derechos a la propia imagen y al honor. El sencillo gesto de marcar la casilla de aceptación es suficiente para ceder los derechos de una gran cantidad de datos personales y contenidos (fotografías, vídeos, entre otros) a empresas intermediarias que a menudo también obtienen el permiso de compartirlas con terceros.

La filtración de datos de Facebook a la consultora Cambridge Analytica -vinculada a la campaña de las elecciones presidenciales que ganó Donald Trump- ha sido el último escándalo en cuanto a infracciones de los derechos de privacidad de los usuarios. El modelo gratuito en Internet a cambio de nuestros datos viene a redefinirse con la entrada en vigor en 2018 de la nueva normativa de la Comisión Europea -el Reglamento General de Protección de Datos (GDPR en inglés)- que busca más seguridad y privacidad para los ciudadanos y más obligaciones para las empresas, poniendo límites al comercio de información personal en la Red. Esto ha supuesto la actualización de las políticas de privacidad de las grandes plataformas tecnológicas para ajustarse a una nueva normativa que cambia las reglas del juego de la privacidad europea pero con un impacto mundial, y cuyo incumplimiento las expone a cuantiosas sanciones.

Nos encontramos ante dos posiciones enfrentadas: por un lado, un planteamiento empresarial con fuertes beneficios, y por otro, una normativa cuyo fin es combatir un modelo de negocio basado en el tratamiento masivo e indiscriminado de datos personales a cambio de una supuesta gratuidad del servicio. Mientras algunos advierten que el reglamento supone una amenaza para el sector de la publicidad digital, otros exigen que sean los propios usuarios quienes gestionen sus datos personales. Aunque las redes ofrecen varios tipos de gestión de la privacidad, los usuarios no suelen conocer el alcance de sus publicaciones, y menos en un entorno social de "ciberdesinhibición", debido al cambio de valores sobre la intimidad y el anonimato (Díaz Buck, 2013). No obstante, la fase de notoriedad alimentada por la premisa "si no estás en la red no eres nadie" parece superada y el usuario comienza a dejar atrás la necesidad de transmitir su información privada a través de las redes.

En este sentido, la nueva normativa aplicable al uso de redes sociales facilita que los usuarios puedan ejercer sus derechos y gestionar su propia privacidad al exigir que los medios disponibles para hacerlo sean fácilmente accesibles. Además, se regula el modo en que debe informarse a los usuarios acerca del tratamiento de sus datos optándose, específicamente en el ámbito de internet, por un sistema de información por capas que le permita conocer de forma clara y concisa los aspectos más importantes del tratamiento, pudiendo acceder a los restantes a través de un enlace directo.

Sin duda, la sensibilidad de los datos en las redes sociales está directamente ligada a la concepción de intimidad y privacidad que tengan los usuarios, porque son ellos quienes dan el consentimiento a la publicación y difusión de los mismos (Roura y Ferré, 2014). Así pues, la intimidad ha perdido su forma exclusiva e individual y adquiere una posición pública y colectiva. Por ello exige modificar las formas de protección, porque hay nuevos fenómenos de agresión a los derechos y libertades (Díaz Buck, 2013).

En este trabajo se analizan las condiciones de uso y políticas de datos de las redes sociales Facebook, Twitter, Instagram, Youtube y WhatsApp- destacando aquellas partes más sensibles para el usuario, con el fin de poner de relieve cuánta información y de qué tipo se está compartiendo, y quién tiene acceso a ella. Asimismo, se revisa la nueva normativa europea identificando las principales novedades en materia de protección de datos y se analiza en qué medida las plataformas de redes sociales han adaptado sus políticas de privacidad al nuevo reglamento.

## **2. Datos personales y privacidad. El Reglamento General de Protección de Datos.**

La principal dificultad que presenta la regulación de la información personal en Internet y en particular, en las redes sociales, es la globalización del mercado online, con una variedad de legislaciones nacionales que limitan la capacidad para tomar decisiones jurídicas respecto a las empresas a escala global. Por otro lado, existe una diferencia ideológica que ha marcado históricamente el debate sobre la privacidad en el entorno online: la legislación europea en materia de protección de datos tiende a tener un papel de defensa del usuario y, en cambio, los Estados Unidos consideran que Internet es la herramienta por excelencia de la libertad de expresión. En tercer lugar, y desde una perspectiva sociológica cada vez más compleja, la seguridad en las redes sociales depende de la consciencia de los usuarios sobre su propia privacidad e intimidad (Roura y Ferré, 2014).

El Reglamento General de Protección de Datos (RGPD) viene a unificar y a actualizar la normativa europea, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas ganar confianza entre los usuarios de Internet. Esta nueva norma incide mucho más en aspectos de protección de datos y favorece el respeto a los derechos fundamentales de los ciudadanos: al honor, a la intimidad, a la propia imagen.

Conviene definir qué se entiende por datos personales, un término de uso frecuente cuyo significado hemos asumido sin ser realmente conscientes de lo que representa. Se

considera un dato personal *toda información sobre una persona física identificada o identificable*. Esta breve definición ya abarca la mayor parte de los datos referentes a cualquier persona que se pueden utilizar para identificarla directa o indirectamente. La UE en el marco del RGPD ha ampliado sustancialmente la definición de datos personales:

*Toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (art. 4.1).*

Pero no todos los datos de carácter personal tienen la misma consideración ante la normativa. Hay determinados datos que, por su especial incidencia en la intimidad, las libertades públicas y los derechos fundamentales de la persona, requieren una mayor protección que el resto de datos personales. Estos son denominados datos sensibles o especialmente protegidos, es decir, los ciudadanos no están obligados a revelarlos ni otros tienen derecho a publicarlos. En este sentido, la nueva normativa mantiene una protección de datos personales y privados estricta según la Directiva de 1995, pero a las categorías de datos ya contempladas - Ideología, religión o creencias; origen racial o étnico; salud y vida sexual - el RGPD añade nuevas categorías de datos adaptadas a las posibilidades que ofrece Internet para identificar a las personas o transmitir información sobre ellas:

- Datos genéticos: todos los datos, con independencia de su tipo, relativos a las características de una persona que sean hereditarias o adquiridas durante el desarrollo prenatal temprano;
- Datos biométricos: cualesquiera datos relativos a las características físicas, fisiológicas o conductuales de una persona que permitan su identificación única, como imágenes faciales o datos dactiloscópicos;
- Datos relativos a la salud: cualquier información que se refiera a la salud física o mental de una persona, o a la asistencia prestada por los servicios de salud a la persona.

De especial relevancia es la inclusión del concepto de datos biométricos como datos sensibles al mismo nivel de protección que los datos de la salud. Se trata de una novedad que afecta a la mayoría de redes sociales y motores de búsqueda ya que se refiere específicamente a las imágenes.

De manera excepcional, se contempla la gestión de datos por parte de partidos políticos, iglesias, sindicatos, centros sanitarios o por parte de las Administraciones, respetando siempre un precepto básico: tales datos no pueden ser exigidos y para obtenerlos y almacenarlos se necesita el consentimiento de la persona que, además, tiene que estar informada sobre la finalidad de la recopilación de dichos datos con carácter sensible.

En España, la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPD GDD) -conocida como LOPD 2018- deroga la antigua Ley Orgánica de Protección de Datos de Carácter Personal y da cobertura al Reglamento General de Protección de Datos (RGPD), de obligado cumplimiento en todos los países de la Unión Europea. En el caso de España -donde la protección de datos es un derecho fundamental protegido por el artículo 18.4 de la Constitución- el RGPD incorpora novedades, tanto en el régimen de consentimiento y tratamiento de los datos como en la introducción de nuevas figuras y procedimientos, que señalamos a continuación.

#### 1) Obtención del consentimiento para el tratamiento de datos

El RGPD elimina las prácticas enmarcadas en el llamado consentimiento tácito e incluye la necesidad de recabar el consentimiento explícito de los propietarios de los datos personales objeto de tratamiento. Esto significa que deberá existir una declaración del interesado o una acción positiva que manifieste su conformidad. Este principio obliga a las organizaciones a la modificación de las fórmulas para recabar el consentimiento, cuya redacción debe ser clara y concisa. Se indica que el consentimiento del interesado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas. En relación con el tratamiento de datos de menores, se mantiene en 14 años la edad a partir de la cual el menor puede prestar su consentimiento.

#### 2) Deber de información

La normativa anterior ya establecía la obligación de informar en todo proceso de recogida de datos sobre la existencia de un fichero o tratamiento de datos de carácter personal, la identidad del responsable del tratamiento, la finalidad de la recogida de los datos y del ejercicio de los derechos de los interesados. El RGPD añade requisitos adicionales en cuanto a la necesidad de informar a las personas interesadas sobre la base legal para el tratamiento de los datos, el período de conservación de los mismos, los datos de contacto del Delegado de Protección de Datos, en su caso, y dónde dirigir las reclamaciones, la existencia de decisiones automatizadas o elaboración de perfiles, la previsión de transferencias a Terceros Países y el derecho a presentar una reclamación ante las Autoridades de Control. En el caso de que los datos no se obtengan del propio interesado (cesión de datos), deberá indicarse además el origen de los datos. Esta información deberá facilitarse en el plazo máximo de un mes, en lugar de los tres meses indicados en la normativa anterior. Esta información debe quedar claramente explicada en las leyendas legales incorporadas en los procesos de recogida de datos (on line/off line), y de forma específica en el aviso de privacidad (y políticas de cookies) de los servicios.

#### 3) Derechos de los interesados

Además de los ya contemplados en la normativa anterior- derecho de acceso, rectificación, oposición y cancelación- el RGPD reconoce a los interesados el derecho de supresión (derecho al olvido), derecho de limitación del tratamiento efectuado y derecho de portabilidad (derecho a exportar los datos en un formato estructurado e interoperable).

#### 4) Evaluación de Impacto del tratamiento de datos personales

Este aspecto representa una novedad en el RGPD, que establece la obligación de realizar una evaluación de impacto (*Privacy Impact Assessment*) para las organizaciones que realicen tratamientos de datos que puedan implicar un alto riesgo para los derechos y libertades de las personas físicas. Se trata principalmente de un análisis en el que se evalúe el origen, la naturaleza, la particularidad y la gravedad de los riesgos que un determinado sistema de información, producto o servicio puede suponer para el derecho a la protección de los datos de los afectados, así como la adopción de las medidas necesarias para eliminar o atenuar en lo posible aquellos riesgos identificados (Considerando 84 en el RGPD). La Agencia Española de Protección de Datos ofrece en su web la *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetos al RGPD*<sup>1</sup> para establecer las bases y aspectos esenciales a tener en cuenta en el proceso de evaluación de impacto que deberán realizar las organizaciones.

#### 5) Comunicación de fallos a la autoridad de protección de datos

El RGPD impone al responsable del tratamiento una nueva obligación de notificar los fallos de seguridad que se produzcan en su organización a la Agencia Española de Protección de Datos (AEPD) en un plazo de 72 horas. Esto implica que el responsable del tratamiento debe contar con un sistema efectivo para realizar el reporte a la AEPD y para comunicar el fallo a los afectados si existe algún riesgo para sus derechos. Por consiguiente, las organizaciones deben establecer, al menos, procesos internos para canalizar las comunicaciones de brechas de seguridad o incidentes que afecten a la protección de datos. Estas comunicaciones internas deben realizarse al Delegado de Protección de Datos, o en su defecto, a la persona encargada de coordinar el cumplimiento de la normativa de protección de datos.

#### 6) Registro de las actividades de tratamiento

Según lo previsto en el artículo 30 del RGPD, las organizaciones que habitualmente realicen tratamiento de datos de riesgo para la privacidad de los interesados o datos sensibles, deberán contar con un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener información relativa, entre otros aspectos, a los tratamientos de datos que se realicen, los datos personales que se traten, los destinatarios de los datos, los plazos previstos para la supresión, la finalidad de dicho tratamiento y las medidas técnicas y de seguridad adoptadas por la empresa para realizar dicho tratamiento. La Agencia Española de Protección de Datos facilita instrucciones concretas acerca del formato y gestión de este registro interno en la *Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*.<sup>2</sup>

#### 7) Aplicación de medidas de seguridad

El RGPD señala que el responsable del tratamiento debe implementar “medidas técnicas y organizativas apropiadas” para garantizar un nivel de seguridad, integridad y privacidad de la información adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse. El responsable debe contactar con la AGPD para determinar las medidas que se deben implantar. De momento, se precisa mantener actualizado el Documento de Seguridad siempre que las medidas técnicas y organizativas sean adecuadas para garantizar la seguridad de la información de carácter personal tratada.

#### 8) Delegado de protección de datos

En el RGPD se introduce la nueva figura del Data Protection Officer o Delegado de Protección de Datos -además de las ya existentes de responsable y encargado- que asume nuevas funciones y competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos. Esta figura será obligatoria cuando el tratamiento lo lleve a cabo una autoridad u organismo público (excepto los tribunales); cuando las actividades y operaciones de tratamiento requieran una observación habitual y sistemática de datos personales a gran escala y, en particular, si se trata de datos sensibles o de categorías especiales de datos de cuyo tratamiento pueda derivarse algún perjuicio económico o social para los usuarios.

#### 9) Privacidad desde el diseño y por defecto, códigos de conducta y esquemas de certificación

El RGPD da un paso más para reforzar el concepto de *accountability* empresarial, es decir, la responsabilidad proactiva en el cumplimiento normativo. Para ello, el RGPD hace especial hincapié en los tratamientos automatizados de datos, estableciendo la privacidad desde el diseño y por defecto,<sup>3</sup> con el fin de que se garantice el cumplimiento con carácter previo al tratamiento de datos y durante el mismo. Esto implica la elaboración de políticas de tratamiento de datos proporcionales a su finalidad, minimizando los datos recabados y garantizando su eliminación en un plazo razonable. Asimismo, el RGPD propone mecanismos efectivos de verificación del cumplimiento y la adhesión a códigos de conducta o a mecanismos de certificación (artículo 42.3). Es aconsejable que las organizaciones con procesos complejos de tratamiento de datos o que manejen datos especialmente sensibles, implementen protocolos internos o procesos de certificación que faciliten y garanticen el cumplimiento del RGPD.

### 3. Condiciones de uso y políticas de privacidad en las redes sociales

La gestión de la información de los usuarios constituye quizá el aspecto más desconocido, controvertido e incierto de las redes sociales. La investigación sobre la materia ha generado varios trabajos entre los que señalamos el estudio realizado por Inteco y la Agencia Española de Protección de Datos (2009); Salvador Benítez y Gutiérrez David (2010); Cabello (2013); Díaz Buck (2013); Roura y Ferré (2014) y Salvador, Olivera y Sánchez (2014).

El uso de los servicios que facilita una determinada red social en, desde o a través de su sitio web está sujeto a un acuerdo legal que exige al usuario la cesión de una serie de datos personales cuyo tratamiento y gestión se describe en las Condiciones de Uso y la Política de Privacidad. Las Condiciones de Uso constituyen un contrato legalmente vinculante entre el usuario y la red social en relación con la utilización del servicio y son de aplicación a todos los usuarios. La Política de Privacidad explica cómo se tratan los datos personales de los usuarios y cómo se protege la privacidad cuando se hace uso del servicio.

Cuando el usuario acepta las Condiciones de Uso de una red social, su información personal deja de ser privada y es recopilada y compartida con terceros. Todo esto se hace con el consentimiento expreso del usuario que, en muchas ocasiones, acepta a ciegas el contenido de estas condiciones y avisos legales, aun cuando afectan a sus datos personales.

Según el barómetro del CIS de mayo de 2018, a un 76,1% le preocupa entre mucho y bastante la protección de los datos personales y el uso posible de información personal por otras personas. Un 71,8% opina que las garantías que ofrecen las redes sociales para proteger sus datos personales son bajas o muy bajas; que es muy difícil controlar quién ve la información que se introduce en el perfil (73,2%); que las redes sociales no deberían cambiar sus políticas de privacidad sin el consentimiento de los usuarios (92,2%) y que no deberían comunicar datos personales a terceros sin autorización previa (97,1%).

A pesar de la inseguridad y vulnerabilidad que generan Internet y las redes sociales, el 33,3% de los internautas nunca consulta las políticas de privacidad de las páginas de Internet que visita o lo hace raramente (29,4%). Un 21,7% señala que las consulta algunas veces, o casi siempre (9,2%), y solo un 3,8% de los usuarios afirma consultarlas siempre. Un 2% señala que no sabe cómo hacerlo. Cabe preguntarse si la información resulta clara, directa, adecuada, accesible y entendible. Para un 16,7%, las políticas de privacidad y la información sobre el tratamiento de datos son claras y sencillas de entender, frente a un 74% que señala estar poco o nada de acuerdo con esta afirmación.

La extensión del texto y la amplitud de contenidos y el empleo de una terminología jurídica con la que el usuario no está familiarizado son factores disuasorios que no favorecen la lectura y comprensión de las políticas, que pueden presentar una dificultad añadida si no están traducidas al idioma del usuario del servicio (Salvador Benítez y Gutiérrez David, 2010).

Teniendo en cuenta los datos expuestos, sorprende que un 49,1% de los encuestados afirme que le importa más acceder a los servicios que le prestan los sitios web que la privacidad de sus datos. En suma, el interés del usuario hacia estas políticas de información sigue siendo muy escaso y casi una década después no han experimentado una evolución significativa (Tabla 1).

¿Con qué frecuencia lee las políticas de privacidad de las páginas web que visita?			
	2009 (%)	2013 (%)	2018 (%)
Siempre	4,1	4,5	3,8
Casi siempre	7,7	9,3	9,2
Algunas veces	21,7	22,3	21,7
Raramente	26,2	28	29,4
Nunca	35,6	31,2	33,3
No sabe cómo hacerlo	4	2,3	2

Tabla 1. Interés del usuario por las políticas de privacidad.

*Fuente: CIS septiembre 2009, mayo 2013 y mayo 2018*

La nueva normativa europea exige la privacidad desde el diseño y el consentimiento explícito del usuario para que una empresa pueda utilizar sus datos personales para fines distintos a los previstos inicialmente. Implica también un nuevo régimen sancionador con la intención de hacer ver la importancia de invertir en sistemas de seguridad, pero sobre todo en tener una adecuada planificación y evaluación de riesgos.

A continuación se realiza un análisis comparativo de las políticas de datos y condiciones de uso de las redes sociales con mayor penetración en las audiencias digitales según el IX Estudio de Redes Sociales 2018 realizado por IAB Spain -Facebook, Twitter, Instagram, Youtube y WhatsApp- con objeto de analizar la normativa tanto para los usuarios que ceden datos y publican contenidos como para el uso de los mismos por parte de terceros. Se tienen en cuenta aspectos como la accesibilidad a los avisos legales, la estructura de los mismos y la tipología de datos recopilados en cada plataforma.

En cuanto a la tipología de datos recopilados por estas redes sociales, se distinguen tres grupos o categorías: datos sobre la actividad en la plataforma y las personas con las que nos relacionamos; características de los dispositivos de acceso, redes y conexiones; y datos sobre la actividad realizada en sitios web y aplicaciones de terceros que utilizan los servicios de la plataforma (Tabla 2).

Tipo de datos recopilados	Descripción general
Actividad en la plataforma y personas con las que nos relacionamos	<ul style="list-style-type: none"> <li>- Actividad, contenidos que se crean y comparten, agenda de contactos, comunicaciones, compras, transacciones comerciales y otros datos que se proporcionan cuando se utilizan los productos y servicios</li> <li>- Actividad y contenido que otros usuarios proporcionan y que puede incluir información sobre nosotros.</li> </ul>
Información sobre dispositivos, redes y conexiones	<ul style="list-style-type: none"> <li>- Características de los dispositivos donde se instala o desde los que se accede a la plataforma, configuración, operaciones realizadas, aplicaciones utilizadas, ubicación geográfica, red y conexiones y datos de cookies.</li> </ul>
Actividad en sitios web y aplicaciones de terceros que utilizan los servicios (anunciantes, desarrolladores de aplicaciones y editores)	<ul style="list-style-type: none"> <li>- Información que proporcionan empresas, anunciantes y otros socios publicitarios sobre las actividades que se realizan dentro y fuera de la plataforma: compras, anuncios que se ven, interacciones con enlaces, páginas visitadas, etc.</li> </ul>

Tabla 2. Políticas de datos. Tipo de datos recopilados por las plataformas sociales

De conformidad con el Reglamento General de Protección de Datos, en las políticas de datos de estas redes sociales se expone la base legal para la recopilación y el tratamiento de estos datos. Como finalidad de la recogida de estos datos señalan: la oferta de contenidos personalizados (puede incluir anuncios en internet y otros formatos de marketing); desarrollo de nuevos productos y funciones; mediciones, análisis y otros servicios empresariales y para fomentar la seguridad, integridad y protección. Así mismo se informa al usuario sobre el ejercicio de sus derechos al acceso, rectificación, eliminación y portabilidad de sus datos.

Como primera observación, se puede señalar que muchos de los datos recopilados en cada una de estas categorías constituyen datos de carácter sensible, supuestamente protegidos por la ley. Junto a los datos personales facilitados para utilizar estas plataformas (nombre y apellidos, correo electrónico, fotografías, etc.), los usuarios crean perfiles de los que se recopilan otros muchos datos de las interacciones con los contenidos, servicios y contactos, que tienen consideración de sensibles como son gustos y preferencias.

En la categoría de datos sobre redes, conexiones y dispositivos de acceso a la plataforma, aparentemente de carácter técnico, también subyacen datos personales que pueden tener consideración de sensibles. Es el caso de las direcciones IP, que reciben la consideración de datos personales en la nueva normativa, y que permiten situar geográficamente un usuario conectado a Internet así como el dispositivo desde el que se conecta con el fin de contextualizar los contenidos y la publicidad. Este hecho podría considerarse como una intromisión en las rutinas del usuario, por tanto, en su intimidad, según un estudio del Instituto Nacional de Tecnologías de la Comunicación (Inteco, 2009: 75).

Los datos de actividad con terceros (por ejemplo, páginas visitadas, experiencia e interacciones con anunciantes, empresas y aplicaciones) y que son recopilados con fines analíticos para extraer patrones y conocimiento para las empresas también puede tener consecuencias para la privacidad y libertad de los usuarios. Estos, entre otros aspectos son los principales contenidos de las Condiciones de uso y Políticas de Privacidad de las redes sociales que se analizan, comentan y comparan a continuación.

### **3.1 Facebook**

El acceso se encuentra en el margen inferior de la pantalla, donde aparecen un total de treinta etiquetas, entre las que se encuentran “Condiciones” y “Privacidad”. El primer caso remite a condiciones y políticas de Facebook, que permite el acceso directo a Condiciones del Servicio, Política de Datos y Normas Comunitarias. Las condiciones que rigen el uso de la plataforma y los servicios establecen una serie de compromisos para el registro y mantenimiento de la seguridad. El texto se estructura en cinco secciones.<sup>4</sup> El límite mínimo de edad para usar el servicio sube hasta los 14 años. Conviene saber que si la configuración del perfil es público, cualquier persona -incluso aquellas que no forman parte de la plataforma- puede acceder a esta información, utilizarla y asociarla al nombre y foto del perfil de uno mismo.

En relación con el contenido que se encuentra protegido por derechos de propiedad intelectual (como fotos o vídeos) que se crean, publican y comparten en los productos Facebook, cuando aceptamos las condiciones y políticas de la plataforma, concedemos a Facebook una licencia mundial, no exclusiva, transferible, sublicenciable y libre de pago por derechos de autor para alojar, usar, distribuir, modificar, mantener, reproducir, mostrar o comunicar públicamente y traducir nuestro contenido, así como para crear contenido derivado (de conformidad con nuestra configuración de privacidad y de la aplicación).

De igual modo, cuando aceptamos las condiciones de servicio estamos dando permiso para utilizar nuestro nombre, foto del perfil e información sobre las acciones que realizamos en anuncios y contenido comercial, patrocinado o asociado, que publique la plataforma. Esto significa que autorizamos que una empresa u otra entidad pague a Facebook por mostrar nuestro nombre y/o foto del perfil y nuestro contenido o información sin recibir compensación de ningún tipo. Esto hace referencia, entre otras cosas, a la publicidad que aparece en los márgenes laterales o intercalada entre las publicaciones con el nombre de “publicación sugerida” o “páginas sugeridas”.

En cuanto a la Política de Datos (información recopilada, uso de los datos y gestión de los mismos) el texto se estructura en once secciones,<sup>5</sup> formuladas a modo de pregunta en un claro ejercicio de comunicación directa y cercana con el usuario.

### 3.2 Twitter

La entrada a las condiciones de acceso y políticas de privacidad se encuentra en el margen inferior de la pantalla. Bajo la etiqueta "Condiciones" se accede a los **Términos de Servicio**, cuyo texto se estructura en seis apartados<sup>6</sup> y permite la descarga en formato pdf. Para el registro y uso de los servicios se establece como requisito la edad de 13 años. En relación con el contenido e información publicada, cuando aceptamos los Términos de Servicio estamos otorgando una licencia mundial, no exclusiva, libre de pago de derechos (con derecho a sublicencia) para usar, copiar, reproducir, procesar, adaptar, modificar, publicar, transmitir, mostrar y distribuir ese contenido en todos los medios de comunicación o métodos de distribución actualmente conocidos o desarrollados con posterioridad. En definitiva, con esta licencia autorizamos a poner nuestro contenido a disposición del resto del mundo y a permitir que otros hagan lo mismo.

La etiqueta "Política de Privacidad" da acceso al texto que informa sobre el tratamiento de los datos personales del usuario. Se estructura en siete secciones numeradas<sup>7</sup> y claramente diferenciadas por colores, con una tipografía destacada, subrayados en aspectos clave y enlaces para facilitar información adicional e incluye navegación local para desplazarse por los contenidos de cada una de las secciones.

En la Política de Privacidad quedan recogidos los derechos del usuario contemplados en el RGPD como son el acceso o rectificación de sus datos personales, su eliminación, oposición al tratamiento, limitar o retirar el consentimiento y la portabilidad o descarga de los datos. Asimismo, para la asistencia y consultas sobre la Política de Privacidad de usuarios residentes en la Unión Europea o en algún Estado de la Asociación Europea de Libre Comercio (AELC), se incluye la figura del Delegado de Protección de Datos, con el que se puede contactar a través de un formulario en el que se deben hacer constar nuestros datos de contacto y la consulta con posibilidad de adjuntar documentos. Una vez enviada, el usuario recibe una clave para el seguimiento y tramitación de la solicitud.

### 3.3 Instagram

El acceso a las Condiciones y Políticas de Privacidad se encuentran en el margen inferior de la pantalla, bajo las etiquetas “Condiciones” y “Privacidad”, entre un total de once. Instagram fue adquirido por Facebook en septiembre de 2012, por lo que ambas plataformas pueden compartir información. No obstante, desde Instagram se informa de que el usuario sigue teniendo el control sobre quién ve sus fotos y si las publica o no Facebook.

Las Condiciones de Uso establecen en 13 años el límite mínimo de edad para usar el servicio. Al igual que en los casos anteriores, Instagram no reclama la propiedad sobre el contenido que publiquemos en el servicio o a través de él. En su lugar concedemos a la plataforma una licencia mundial, no exclusiva, transferible, sublicenciable y libre de pago por derechos de autor para alojar, usar, distribuir, modificar, mantener, reproducir, mostrar o comunicar públicamente y traducir el contenido que se suba, así como para crear contenido derivado (de conformidad con la configuración de privacidad de la persona y de la aplicación). Es posible elegir qué personas pueden ver nuestro contenido y actividades, incluidas las fotografías. De igual modo, aceptamos que Instagram puede insertar anuncios y promociones sobre, acerca de o junto con nuestro contenido. Esto significa que autorizamos que una empresa pague a Instagram por usar nuestro nombre de usuario, foto del perfil e información sobre nuestras relaciones y las acciones que realizamos sin compensación alguna.

En cuanto a la Política de Datos, entendemos y aceptamos que proporcionan una plataforma para publicar contenido, incluyendo fotos, comentarios y otros materiales para compartirlo públicamente. Esto significa que otros usuarios pueden buscar, ver, utilizar o compartir cualquier contenido que hagamos público a través de la plataforma. Cualquier información o contenido que se publique voluntariamente adquiere un carácter público, si bien es cierto que se puede controlar mediante la configuración de privacidad que establezca el usuario. Instagram recopila la siguiente información de sus usuarios:

### 3.4 YouTube

El acceso a las Condiciones y Políticas de Privacidad se realiza desde el menú disponible en el margen izquierdo de la pantalla. Los avisos legales se encuentran en la parte inferior, por lo que es necesario desplazar el *scroll* para ver las etiquetas “Términos” y “Privacidad” que dan acceso a las políticas de información de la plataforma.

La primera etiqueta enlaza con el documento de Términos y Condiciones del Servicio que el usuario deberá aceptar previamente. En el propio documento se informa de que el usuario puede aceptar los Términos y Condiciones mediante la simple utilización de los Servicios. Hace constar, además, que el usuario reconoce y acepta que YouTube considerará que su uso de los Servicios constituye la aceptación de los Términos y Condiciones a partir del inicio de dicha utilización. El documento incluye, además, que el usuario acepta que su inobservancia de cualquiera de estas condiciones constituirá un incumplimiento por su parte de Términos y Condiciones y recomiendan al usuario que imprima o guarde en sus archivos una copia de dicho documento.

En cuanto al contenido que se crea y publica, el usuario seguirá siendo el titular de los derechos, si bien deberá otorgar unos derechos de licencia limitados a favor de YouTube y otros usuarios de los Servicios.

- a. A favor de YouTube, el usuario otorga una licencia mundial, no exclusiva, exenta de *royalties* y transferible (con derecho de sub-licencia) para utilizar, reproducir, distribuir, realizar obras derivadas de, mostrar y ejecutar, ese contenido en relación con la prestación de los Servicios y con el funcionamiento y la actividad de YouTube, incluyendo sin limitación alguna, a efectos de promoción y redistribución de la totalidad o de una parte del Servicio (y de sus obras derivadas) en cualquier formato y a través de cualquier canal de comunicación.
- b. A favor de cada usuario del Servicio, el usuario otorga una licencia mundial, no exclusiva y exenta de *royalties* para acceder a su contenido a través del Servicio, y para utilizar, reproducir, distribuir, realizar obras derivadas de, mostrar y ejecutar, este contenido en la medida de lo permitido por la funcionalidad del Servicio y con arreglo a los Términos y Condiciones, que se rigen por las leyes de España.

La Política de Privacidad -accesible desde la etiqueta "Privacidad"- informa al usuario sobre qué datos recoge la plataforma, por qué los recopila y cómo puede actualizarlos, gestionarlos, exportarlos y eliminarlos. Para facilitar al usuario la comprensión de este documento se añaden ejemplo, videos explicativos y definiciones de los términos clave.

El tipo de información que recoge [Google/YouTube] y cómo se utiliza esa información depende del uso de los servicios que realice el usuario y de cómo administre los controles de privacidad. En la Política de Privacidad señala que no muestran anuncios personalizados basados en categorías sensibles como, por ejemplo, la raza, la religión, la orientación sexual o la salud. Tampoco comparten información que identifique al usuario (nuestro nombre o nuestra dirección de correo electrónico) con los anunciantes, a menos que el usuario lo solicite.

Además proporciona información sobre los controles de privacidad que puede aplicar el usuario, y que le permite gestionar, revisar y elegir las opciones más importantes (controles de actividad, configuración de anuncios, información que comparte, información personal que ven otros usuarios) así como exportar, retirar y eliminar su información (contenidos específicos vinculados a servicios y productos concretos, o eliminar su cuenta por completo).

### 3.5 WhatsApp

En 2014 WhatsApp se unió a las empresas del grupo Facebook, por lo que recibe información de estas empresas y comparte información con ellas. No obstante, WhatsApp señala que los mensajes del usuario se mantienen privados y no se compartirán en Facebook. De hecho, Facebook no usará los mensajes de WhatsApp para ningún otro propósito distinto al de ayudar a operar y proveer los Servicios de WhatsApp. No permite publicidad por parte de terceros en la aplicación (política de cero anuncios *banner* de terceros).

Al igual que en Facebook, el requisito mínimo de edad son 13 años para poder usar la aplicación (o la edad mínima requerida en cada país). Una vez que uno se une a WhatsApp les proporciona regularmente los números de teléfono de todos los contactos de que uno dispone en la libreta de direcciones del móvil, usen o no esta aplicación. Al utilizar WhatsApp aceptamos la recopilación, utilización, procesamiento y uso compartido de nuestra información, así como la transferencia y el procesamiento de nuestros datos en los Estados Unidos y otros países donde tengan instalaciones, proveedores de servicios o socios. Además otorgamos a WhatsApp una licencia para usar, reproducir, distribuir, crear obras derivadas, mostrar y ejecutar la información (incluido el contenido) que subimos, presentamos, almacenamos, enviamos o recibimos a través de WhatsApp, con el propósito limitado de operar y proveer sus servicios.

Debemos destacar que la Política de Privacidad de WhatsApp establece que los mensajes pertenecen a cada usuario y que ellos no pueden leerlos, ni tampoco almacenar nuestros mensajes una vez que son entregados.

### 3.6 Análisis comparativo

El estudio comparativo de las condiciones de uso de las redes sociales seleccionadas pone de relieve las principales diferencias con respecto a los requisitos del servicio, la facilidad de acceso al texto con las condiciones así como la claridad y estructura de los contenidos (Tabla 3).

Twitter e Instagram establecen como requisito la edad mínima de 13 años para el uso del servicio; Youtube y Facebook la elevan a 14 años, y WhatsApp establece 16, al igual que alguna de las aplicaciones de Twitter, como Periscope. En todos los casos el usuario se compromete a hacer un uso responsable del servicio, respetar las condiciones de la plataforma y no realizar actividades fraudulentas o que infrinjan los derechos de otras personas, incluidos los de propiedad intelectual.

CONDICIONES DE SERVICIO		PLATAFORMAS				
		Facebook	Twitter	Instagram	Youtube	WhatsApp
Requisitos	Edad	14 años	13 años	13 años	14 años	16 años
	Uso legal y responsable	SI	SI	SI	SI	SI
Acceso y Estructura	Enlace	SI	SI	SI	SI	SI
	Visibilidad	Baja	Alta	Media	Media	Alta
	Etiqueta	Condiciones	Términos y condiciones	Condiciones	Términos	Privacidad y condiciones
	Secciones	SI (5)	SI (5)	NO	NO	NO
	Navegación	SI	SI	NO	NO	NO
Contenido	Claridad	SI	SI	SI	SI	SI
	Enlaces	SI	SI	SI	SI	SI
	Idiomas	SI (48)	SI (9)	SI (48)	SI (80)	SI (60)
	Actualización	SI 31/07/2019	SI 25/05/2018	SI 19/04/2018	SI 22/07/2019	SI 24/04/2018

Tabla 3. Comparativa requisitos de acceso, estructura y contenido de las Condiciones de Servicio

*Fuente: Elaboración propia*

El acceso se facilita en todas las plataformas a través de un enlace ubicado en el margen inferior de la pantalla bajo las etiquetas Condiciones (Facebook e Instagram) y Términos (Youtube), bien de forma independiente o combinada (Twitter). En el caso de WhatsApp, el mismo enlace facilita el acceso a las condiciones de uso y las políticas de privacidad, empleando en este caso la etiqueta Privacidad y Condiciones. La visibilidad del enlace es especialmente subrayada en el caso de WhatsApp, apareciendo como única etiqueta, destacada en una franja independiente, seguido de Twitter donde aparece junto a otras tres etiquetas. A medida que se incrementa el número de etiquetas que aparecen en el margen inferior de la pantalla, también se reduce el tamaño de la tipografía, por lo que la visibilidad de este enlace con información clave para el usuario se pierde considerablemente. Es el caso de Youtube e Instagram, donde el enlace aparece entre un total de 11 etiquetas. El nivel de visibilidad más bajo lo presenta Facebook, donde el enlace a las Condiciones se pierde en un total de 30 etiquetas.

Los textos referidos a las Condiciones de Uso suelen ser amplios, por lo que una buena estructura puede facilitar al usuario la identificación de las categorías de la información contenida y dirigir la consulta a las secciones de interés. Las mejores prácticas en este sentido las ofrecen Facebook y Twitter, que estructuran el texto en cinco secciones y facilitan su navegación a través de las mismas, pudiendo acceder de forma directa a cada una de ellas. Mejorables son los casos de Instagram, Youtube y WhatsApp, donde el texto de Condiciones se presenta de forma continua y sin secciones, lo que obliga a manejar la barra lateral o *scroll* para la lectura del texto, una práctica desaconsejada a efectos de usabilidad web.

El esfuerzo más destacado en todos los casos se aprecia en el interés por facilitar la comprensión del texto, evitando terminología específica a favor de un lenguaje más claro y cercano al usuario. En todos los casos se incluyen además enlaces con información adicional y se ofrece la posibilidad de traducción del texto a varios idiomas a través de listados y desplegables, desde las 9 opciones de Twitter, las 48 de Facebook e Instagram, hasta los más completos como WhatsApp (60) y Youtube (80), con un amplio abanico de posibilidades.

La entrada en vigor del RGPD en mayo de 2018 obligó a las plataformas a revisar y actualizar sus condiciones de uso, por lo que en todos los casos las fechas de revisión y entrada en vigor se corresponden con esta fecha. Las últimas revisiones y actualizaciones han sido efectuadas por Facebook y Youtube en julio de 2019.

En cuanto a las Políticas de Datos o Políticas de Privacidad (Tabla 4), el acceso se facilita en todas las plataformas a través de un enlace ubicado en el margen inferior de la pantalla bajo la etiqueta Privacidad. En el caso de WhatsApp, el mismo enlace facilita el acceso a las condiciones de uso y las políticas de privacidad, empleando en este caso la etiqueta Privacidad y Condiciones. Como ya comentamos anteriormente, el nivel de visibilidad más alto corresponde a WhatsApp y Twitter, seguido de Youtube e Instagram, donde el enlace aparece entre un total de 11 etiquetas. El nivel de visibilidad más bajo lo presenta nuevamente Facebook, donde el enlace a las Políticas de Privacidad queda diluido entre un total de 30 etiquetas.

POLÍTICA DE DATOS		PLATAFORMAS				
		Facebook	Twitter	Instagram	Youtube	WhatsApp
Acceso y Estructura	Enlace	SI	SI	SI	SI	SI
	Visibilidad	Baja	Alta	Media	Media	Alta
	Etiquetas	Privacidad	Privacidad	Privacidad	Privacidad	Privacidad y condiciones
	Secciones	SI (11)	SI (7)	NO	SI (10)	SI (9)
	Navegación	SI	SI	NO	SI	SI
Contenido	Claridad	SI	SI	SI	SI	SI
	Enlaces	SI	SI	SI	SI	SI
	Idiomas	SI (48)	SI (9)	SI (48)	SI (80)	SI (60)
	Actualización	SI 19/04/2019	SI 25/05/2018	SI 19/04/2018	SI 22/01/2019	SI 24/04/2018

Tabla 4. Comparativa acceso, estructura y contenidos sobre las Políticas de Datos.

*Fuente: Elaboración propia*

El contenido de las Políticas de privacidad es complejo y extenso, por lo que la estructura del texto y su presentación es especialmente importante de cara al usuario. En este sentido hay que señalar que en todos los casos se encuentra organizado en secciones con posibilidad de

navegación y acceso directo a cada una de ellas, a excepción de Instagram, que presenta el texto de forma continua obligando a manejar la barra lateral para la lectura del texto.

El nuevo RGPD es especialmente exigente con la claridad y el detalle de las políticas de datos. De ahí que sea en este punto donde más se aprecia la voluntad por facilitar al usuario de los servicios la comprensión de los contenidos y la fácil identificación de los temas clave de obligado cumplimiento en la normativa como son: la base legal de los datos recopilados, el periodo de conservación de los datos, la gestión de la información personal, la transferencia de datos a terceros, la elaboración de perfiles, el contacto del Delegado de Protección de Datos y la gestión de las reclamaciones. En todos los casos se aprecia un claro ejercicio de comunicación directa y cercana con el usuario, siendo especialmente destacables Facebook, que formula los enunciados a modo de preguntas; Youtube, que acompaña cada sección con ejemplo, vídeos explicativos y definiciones de los términos clave, y Twitter, cuyas secciones aparecen numeradas y claramente diferenciadas por colores, tipografía destacada y subrayados en aspectos clave.

La necesidad de consentimiento expreso para el tratamiento de los datos también se pone de manifiesto en la redacción del texto, en los que se subraya la importancia de leer el texto de las políticas de datos en su totalidad, se incluyen fórmulas de consentimiento expreso para diferentes finalidades, e incluso se insiste en imprimir y conservar el documento, ofreciendo la opción de descarga en formato pdf, como es el caso de Twitter y Youtube.

Al igual que las Condiciones de Uso, las Políticas de Datos incluyen en todos los casos enlaces con información adicional y numerosas opciones de traducción del texto a otros idiomas. Las fechas de revisión y actualización de las Políticas de Datos son coincidentes con las señaladas en las Condiciones de Uso.

#### **4. La privacidad como oportunidad de negocio**

Los avances tecnológicos y el abaratamiento del almacenamiento junto con el desarrollo de las técnicas estadísticas están permitiendo extraer conocimiento derivado del análisis de datos masivos procedentes de distintas fuentes -en su mayoría datos personales- asociados a las operaciones que los consumidores llevan a cabo en cualquier sector, con un coste mucho menor, con mayor exactitud y con mayor riqueza para la toma de decisiones. Nos encontramos inmersos en la economía del dato y términos como *Big Data* o Inteligencia Artificial se han vuelto cotidianos en los planes estratégicos de cualquier organización, independientemente de la industria de la que se trate.

Las redes sociales tienen capacidad para construir una identidad digital de los usuarios a partir de sus datos personales (nombre y apellidos, lugar de residencia, centro de estudios o estado civil, lugar de trabajo y red profesional de contactos, círculos de amigos y familiares, ideología política, creencias religiosas, etc.) y sus datos de actividad (tráfico web, transacciones en tiendas online, sensores en *wearables* y móviles, geoposicionamiento, datos científicos, financieros, de salud o los de las ciudades inteligentes o *smartcities*, etc.). Además, con sus datos

de uso, las personas desvelan sus necesidades, gustos y preferencias, cómo utilizan productos y servicios, patrones de compra o de comportamiento y anticipan los posibles cambios en la demanda. En suma, el perfil de usuario en redes sociales permite realizar un retrato bastante preciso resultado de una gran cantidad de información, aparentemente no sensible, que configura una identidad digital en constante evolución. Con la analítica de estos *Big Data* las empresas pueden optimizar la toma de decisiones, sus estrategias de *marketing*, su eficiencia interna y adaptar sus productos y servicios a los gustos y necesidades de perfiles de consumidores.

Sin embargo, la retención masiva de datos de carácter socioeconómico, demográfico, financiero y de comportamiento con propósitos analíticos puede tener graves consecuencias para la privacidad y libertad individual de los consumidores. Desde una perspectiva de seguridad y privacidad, la normativa reguladora, la tecnología que sustenta las plataformas y las empresas se enfrentan al reto de garantizar que los usuarios tengan el suficiente control sobre sus datos para prevenir un uso indiscriminado a la vez que se mantiene su utilidad para extraer conocimiento, patrones y, en suma, valor como activo empresarial.

La economía digital es relativamente nueva pero hay un hecho constatable: la base de todas las relaciones duraderas y fructíferas es la confianza, y el procedimiento de obtención de los datos de los clientes y el modo de utilizarlos son la base de esa confianza. La protección de datos personales no debe estar motivado por el deseo de evitar las cuantiosas sanciones por incumplimiento del RGPD, sino porque la protección de los clientes, usuarios, colaboradores o empleados es, además de una responsabilidad, un importante factor de competitividad y fidelización.

#### **4. Conclusiones**

Las redes sociales, por su carácter abierto y divulgativo, están sujetas a condiciones de uso y políticas de privacidad que deben informar al usuario de manera clara y directa la finalidad del uso y tratamiento de los datos y contenidos que publica y comparte.

El análisis realizado permite afirmar que entre las categorías de datos recopilados por las redes sociales, los más abundantes son datos sensibles, compartidos por el usuario en sus interacciones con la plataforma, con sus contactos y con las empresas y anunciantes que usan dichas redes sociales. Más allá de revelar nombre, apellidos o correo electrónico, o incluso de publicar fotografías, los usuarios crean perfiles en las redes sociales con detalles de sus gustos, preferencias y todo aquello que, supuestamente, está protegido por la ley y se considera sensible. Aunque a ojos de los usuarios se trate de datos inconexos, aparentemente irrelevantes y dispersos en varias plataformas, las actuales técnicas de agregación de datos y elaboración de perfiles a través de Internet permiten crear una imagen muy precisa de las personas. De ahí la importancia de conocer el uso que estas plataformas hacen de los datos de los usuarios, la existencia de decisiones automatizadas o elaboración de perfiles, cómo gestionar los controles de privacidad y cómo los interesados pueden ejercer sus derechos.

La entrada en vigor de la nueva normativa ha obligado a las plataformas a la revisión y actualización de sus Condiciones de Uso y Políticas de Datos, para adaptarlas a los nuevos requisitos. El análisis constata que los servicios de redes sociales han hecho un importante ejercicio de comunicación y transparencia en la información de los avisos legales, cuya redacción presenta un estilo directo y un lenguaje mucho más próximo al usuario. La incorporación de índices y menús de navegación por estos contenidos y el acceso directo a la información clave para el usuario, haciendo uso del sistema de información por capas que señala el RGPD, son otras de las adaptaciones y mejoras incorporadas a las Condiciones de Uso y Políticas de Datos, a lo que hay que sumar las opciones de traducción de los textos a varios idiomas, y en algunos casos, la posibilidad de descarga de los avisos legales en formato pdf.

Sin embargo, el esfuerzo por la revisión y adaptación de los contenidos de estas políticas a las obligaciones de la nueva normativa contrasta con el escaso interés por mejorar la accesibilidad a estos contenidos en los servicios de redes sociales. Tratándose de una información clave para las empresas -y sus obligaciones legales- y para los intereses del usuario - la protección de sus datos personales e intimidad- el acceso a estas políticas sigue sin privilegiarse. La ubicación de los avisos legales en el margen inferior de la página y el tamaño de la tipografía empleada en las etiquetas -en algunos casos inferior a nueve puntos- no facilitan su localización. Por las razones señaladas, sería deseable mejorar la accesibilidad y visibilidad a estos contenidos, bien en el menú principal o en una sección específica, diferenciada y visible en la página principal.

Por otro lado, el sistema de etiquetas utilizado en las secciones del menú, en ocasiones, resulta inconsistente y no facilita la identificación de esta información. Por ejemplo, en Facebook e Instagram se aprecia cierta inconsistencia cuando incluyen en el menú la etiqueta "Privacidad" y el contenido aparece rotulado como "Políticas de Datos". Esta misma inconsistencia se encuentra en Twitter, cuando la sección del menú se denomina "Términos" y el contenido se rotula "Condiciones de Servicio".

En un mercado competitivo donde la personalización es la clave - y no es posible personalizar sin datos personales- el empleo de las tecnologías (redes sociales, aplicaciones móviles, e-commerce, etc.) y la interacción con los clientes es condición indispensable para el éxito y la estrategia empresarial. Sin embargo, el mismo usuario que demanda personalización de productos y servicios se escandaliza si las empresas le *trackean*<sup>8</sup> para ofrecerle la personalización que él mismo solicita y lo que resulta aún más grave, sigue reconociendo que no lee las políticas de privacidad.

El cliente espera recibir un servicio personalizado, pero con frecuencia desconoce la tecnología que hay detrás, lo que constituye un primer obstáculo para comprender el uso y tratamiento que se hace de sus datos. No solo se trata de una cuestión de privacidad, es cuestión de confianza, y esta hay que ganarla. Las empresas tienen una oportunidad para transformar esta situación en una ventaja competitiva. El reto está en poner al cliente en el centro, definir cómo se entiende la relación con él y sus datos personales y trazar una estrategia

Antonia Salvador Benítez:

Entre la privacidad y el negocio. Condiciones de uso y política de datos en redes sociales,  
[www.derecom.com](http://www.derecom.com), ISSN 1988-2629, pgs. 139-161.

en consonancia con la normativa para lograr un impacto social no solo económico. El reto está en construir la relación con los clientes a largo plazo, definir el objetivo y minimizar los datos solicitados. El nuevo Reglamento ya apunta en esta dirección cuando indica que solo podrán solicitarse los datos exclusivamente necesarios para prestar el servicio y/o producto, evitando así que se puedan pedir más bajo la misma firma. La visibilidad, transparencia de la información y minimización de los datos constituyen aspectos clave, que se traducen en una mejora de la usabilidad, la comunicación y claridad de las políticas de privacidad para que el usuario comprenda las implicaciones de la cesión de sus datos.

---

<sup>1</sup> Disponible en: <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

<sup>2</sup> AEPD. *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD* <https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>.

La Autoridad Catalana de Protección de Datos proporciona un modelo sencillo para crear y mantener el registro de las actividades de tratamiento en entidades pequeñas: *Instrucciones de uso del registro de actividades de tratamiento*.

Disponible en:

[http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament general de proteccio de dades/documents/instrucciones-de-uso-del-registro-de-las-actividades-de-tratamiento-CAST.pdf](http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament%20general%20de%20proteccio%20de%20dades/documents/instrucciones-de-uso-del-registro-de-las-actividades-de-tratamiento-CAST.pdf)

<sup>3</sup> La privacidad por diseño es la que se incorpora desde que se concibe un servicio hasta su despliegue de medidas tecnológicas para preservar la privacidad de los usuarios. La privacidad por defecto protege los datos del usuario en los ajustes por defecto. En este caso el diseñador de los servicios, bien por su construcción, bien en los parámetros configurables por el usuario, seleccionará los más respetuosos con la privacidad.

<sup>4</sup> 1) Nuestros Servicios; 2) Nuestra Política de Datos y Tus Opciones de Privacidad; 3) Tus Compromisos con Facebook y Nuestra Comunidad; 4) Disposiciones Adicionales; y 5) Otras Condiciones y Políticas que Pueden Aplicarse en Tu Caso.

<sup>5</sup> Las secciones de la Política de Datos son las siguientes: ¿Qué tipo de información recopilamos?; ¿Cómo utilizamos esta información?; ¿Cómo se comparte esta información?; ¿Cuál es la dinámica de trabajo conjunto de las empresas de Facebook?; ¿Cuáles son los fundamentos legales en los que nos basamos para tratar los datos?; ¿Cómo puedo ejercer mis derechos en virtud del RGPD?; Retención de datos, desactivación y eliminación de cuentas; ¿Cómo respondemos a requerimientos legales o evitamos que se produzcan daños?; ¿Cómo operamos y transferimos datos como parte de nuestros servicios internacionales?; ¿Cómo notificaremos los cambios que se produzcan en esta política?; Cómo remitir tus dudas a Facebook.

<sup>6</sup> Dichas secciones son: Quien puede hacer uso de los Servicios; Privacidad; Contenido de los Servicios; Uso de los Servicios; Limitaciones de Responsabilidad y General.

<sup>7</sup> Las secciones son las siguientes: Información que comparte con nosotros; Información adicional que recibimos sobre usted; Información que compartimos y revelamos; Gestionar nuestra información personal sobre usted; Los menores y nuestros servicios; Nuestras operaciones globales y escudo de privacidad; y Cambios a esta Política de Privacidad.

<sup>8</sup> El término se refiere básicamente a seguir puntualmente los “movimientos” de los usuarios. Google con sus analíticas agrega este elemento denominado Heatmaps.

## Referencias bibliográficas

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS (2018). *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetos al RGPD*. Disponible en: <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>

CABELLO, A. (2013). *Los derechos de las fotografías y las redes sociales*. *Af.es*, 9, p.66-71.

DÍAZ BUCK, A.V (2013). “La autorregulación en redes sociales como forma de garantizar los derechos de intimidad, privacidad y protección de datos personales”, *Derecom*, 13, p. 125-143.

FERRÉ PAVIA, C. (Ed.) (2014). *El uso de las redes sociales: ciudadanía, política y comunicación. La investigación en España y Brasil*. Universitat Autònoma de Barcelona: Institut de la Comunicació.

IAB Spain-Elogia. *Estudio Anual de Redes Sociales 2018*. Disponible en: [https://iabspain.es/wp-content/uploads/estudio-redes-sociales-2018\\_vreducida.pdf](https://iabspain.es/wp-content/uploads/estudio-redes-sociales-2018_vreducida.pdf)

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN; AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Disponible en: <https://www.csirtcv.gva.es/es/descargas/inteco-estudio-sobre-la-privacidad-de-los-datos-personales-y-la-seguridad-de-la-informaci%C3%B3>

ROURA, E; FERRE PAVIA, C. (2014). “Aspectos legales de las redes sociales: protección de datos y uso consciente de la tecnología”, en FERRÉ PAVIA, C. (Ed.) (2014). *El uso de las redes sociales: ciudadanía, política y comunicación. La investigación en España y Brasil*. Universitat Autònoma de Barcelona: Institut de la Comunicació, p.92-115.

SALVADOR BENÍTEZ, A; GUTIERREZ DAVID, E. (2010). *Redes sociales y medios de comunicación. Desafíos legales*, *El Profesional de la Información*, 19, 6, p. 667-674.

SALVADOR BENÍTEZ, A; OLIVERA ZALDUA, M; SÁNCHEZ VIGIL, J.M (2014). *Redes sociales y medios de comunicación. Políticas de uso de contenidos audiovisuales*, en SIERRA SÁNCHEZ, J; GARCÍA GARCÍA, F. *Tecnología y narrativa audiovisual*. Madrid: Fragua, p. 717-735.

## Legislación

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales. BOE, núm. 294, de 6 de diciembre, p. 119788-119857. <https://www.boe.es/eli/es/lo/2018/12/05/3>

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE, núm. 119, de 4 de mayo de 2016, 88p. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

### **Redes sociales – Condiciones de Uso y Políticas de Privacidad**

Facebook. Condiciones y Políticas <<https://es-es.facebook.com/policies?ref=pf>>

Instagram. Política de Datos <<https://help.instagram.com/519522125107875>>

Instagram. Condiciones de Uso <<https://help.instagram.com/581066165581870>>

Twitter. Términos de Servicio <<https://twitter.com/es/tos>>

Twitter. Política de Privacidad <<https://twitter.com/es/privacy>>

WhatsApp. Privacidad y Condiciones <<https://www.whatsapp.com/legal>>

Youtube. Términos y Condiciones del Servicio <<https://www.youtube.com/t/terms>>

Youtube. Política de Privacidad <<https://policies.google.com/privacy?hl=es&gl=es>>