UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja

Privacidad e Intimidad en las Redes Sociales

Trabajo fin de máster presentado por:	Andrea B. Romero Robredo
Titulación:	Máster
Línea de investigación:	Propiedad Intelectual y Nuevas Tecnologías
Director:	Prof. Dr. Luis Miguel González de la Garza

Madrid
27 de septiembre de 2017
Firmado por:

ROMERO ROBREDO ANDREA BEATRIZ - 44732659M

Digitally signed by ROMERO ROBREDO ANDREA BEATRIZ - 44732659M
DN: c=ES, serialNumber=44732659M, sn=ROMERO ROBREDO, givenName=ANDREA BEATRIZ, cn=ROMERO ROBREDO ANDREA BEATRIZ - 44732659M
Reason: I am the author of this document
Date: 2017.09.27 21:38:42 +02'00'

Resumen

Internet ha cambiado drásticamente cómo se comunican e interactúan las personas entre sí y nuestra presencia virtual se ha convertido en un reflejo de nuestras personalidades como consecuencia de la popularidad y uso extendido de las redes sociales. Existe un desconocimiento abrumador respecto del tipo, cantidad y frecuencia de la información que se recolecta y se comparte y los operadores de las redes sociales deberían asumir un rol más activo en la protección de la privacidad de sus usuarios a través de sus políticas de privacidad, lo que permitiría a los usuarios adoptar una decisión formada sobre la transmisión de sus datos. En este trabajo se hace un análisis de las políticas de privacidad en el marco de las redes sociales, la herramienta legal más importante para informar a los usuarios sobre el uso de sus datos personales, usando como referencia las tres redes sociales más populares en España.

Palabras clave:

privacidad online, internet, redes sociales, protección de datos

Abstract

Internet has drastically changed how people communicate and interact amongst each other and, as a result of the social networks' popularity and extended use, our virtual presence has become an actual reflection of our personalities. There is an overwhelming lack of information with respect to the type, quantity and frequency of the information that is shared and recollected online and social networks should adopt a more active role in the protection of its users' privacy through their privacy policies, which would allow their users to make an informed decision over the transmission of their personal data. In this study, the privacy policies of the three most popular social networks in Spain are analysed, as these are the most important tool to inform the users of the use that is given to their personal data.

Key words:

online privacy, internet, social networks, data protection

I. Índice

II. Introducción

En el mundo de la información digital, si no estás pagando por un producto, eres el producto. Si las empresas continúan incrementando la cantidad de datos que almacenan sobre los individuos, los datos en sí se convierten en un producto a la venta y, si los individuos no comienzan a protegerse a sí mismos y la información digital que divulgan, corren el riesgo de que sus datos personales se agrupen y se vendan al mejor postor[1].

La cantidad de datos que las empresas recolectan sobre los individuos en el mundo digital es impresionante, sólo en Facebook se generan diariamente 10.000 millones de mensajes, los usuarios comparten 350 millones de fotografías y vídeos y 4.500 millones de páginas al día se señalan con el icono "me gusta". Lo cierto es que en esta sociedad moderna, la mayoría de las personas dependen de sus *smartphones*, portátiles y *tablets* para interactuar con otras personas y empresas en todo el mundo. Son dispositivos que se usan para jugar, en el colegio, para trabajar, etc. Usamos Google para buscar un restaurante, WhatsApp para enviar mensajes a nuestros amigos sobre los planes de cena esa noche, Instagram para hacer un reportaje fotográfico del menú y también Facebook para compartir la velada con nuestros amigos. Mientras vamos pasando de una red social a otra por cada una de las aplicaciones de estas grandes empresas, van a ir rastreando cada una de nuestras interacciones que hemos realizado *online* a través del hardware y el software de nuestros dispositivos. Registran lo que nos gusta y lo que no nos gusta, curiosidades y hasta ubicaciones[2].

Indudablemente, Internet ha cambiado drásticamente cómo se comunican e interactúan las personas entre sí y nuestra presencia virtual se ha convertido en un reflejo de nuestras personalidades, intereses e identidades. Nuestros teléfonos, portátiles y cómo los usamos no son ya únicamente un reflejo de las comunicaciones que hacemos entre nosotros sino que son un puro reflejo de nuestras vidas al completo[3].

Detrás de la "seguridad" que les da una pantalla de ordenador, muchos de los usuarios anónimos revelan más información sobre sí mismos en el mundo digital de lo que jamás compartirían en la vida real. Mientras es expresan libremente a través de sus teclados, desconocen el número de operadores de redes sociales que están almacenando la información que comparten. Un comentario escrito en un momento de rabia o frustración, una fotografía desafortunada que suben sin pensarlo dos veces, se almacenan en los servidores de estos operadores para la eternidad, incluso si se borran inmediatamente[4].

Como consecuencia de esta popularidad y uso extendido de *smartphones*, aplicaciones y los servicios que prestan las redes sociales, los expertos temen que

[1] Rosenberg, M. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 1.
[2] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 1.
[3] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 1.
[4] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 10

se haya expuesto demasiada información. Aún hoy no tenemos certeza de cómo usan exactamente estos operadores los datos que recolectan ni cómo pretenden utilizarlos en el futuro[5].

Las empresas han descubierto el poder de la información aparentemente irrelevante que, cuando se combina y pone en relación con otra información almacenada en sus bases de datos, contribuyen a crear una identidad completa de los individuos. Las empresas ya cuentan con múltiples servicios con los que interactuar los usuarios. Solo Google ofrece servicios de correo electrónico (Gmail), un navegador (Google Chrome), un buscador (Google), servicios de vídeo, música y voces (YouTube, Google Play y Google Voice), mapas y servicios de GPS (Google Maps) y todo un sistema operativo en los smartphones Android. A través de todos estos servicios, Google puede supuestamente seguir el rastro del comportamiento de un usuario en un 88% de los dominios de Internet. Cada acto insignificante, como enviar un email o hacer una búsqueda en Internet, una vez asociada, permite a Google crear algo que no se aleja nada de un retrato detallado de nuestras vidas e intereses[6].

Ya son más de 3.000 millones las personas que utilizan las redes sociales en todo el mundo[7] y estas personas se ven inmersas en la vida social online que prefieren, crean un enmarañamiento entre sus identidades reales y virtuales. Al igual que existen múltiples perfiles de usuarios de redes sociales, hay otros tantos motivos por los que no deberían sobre-exponer su información en la red. La razón más evidente siendo, sin duda, que los usuarios suelen infravalorar o no comprender debidamente los riesgos asociados a su uso[8].

Esta realidad se ha convertido en un problema actual en el que los internautas se basan en la asunción – falsa – de que la información marcada como "privada" no será difundida en la red. Si bien es cierto que rara vez van a traicionar la confianza de sus usuarios, ningún mecanismo de seguridad es perfecto. Las redes sociales a menudo usan sistemas de seguridad estándares que pueden ser accedidos en cualquier momento por un *hacker*. La combinación de información privada de carácter sensible manejada por usuarios que no son conscientes de que la seguridad en este ámbito no está protegido herméticamente y que es, por tanto, una fuente segura de filtración de información personal o, incluso, de robos de identidad[9].

La creencia generalizada de que la privacidad se protege en las redes sociales nos lleva a la preocupante realidad de que la información está al alcance de más empresas y personas de las que se cree. En primer lugar, si se conserva un perfil público estará nuestra información personal al alcance de cualquiera. En segundo lugar y, en todo caso, el operador de la red social dispondrá de toda la información

[5] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 11.
[6] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 12-13.
[7] Estudio de We Are Social y Hootsuite. (2017)
[8] Leenes, R. (2011) "Context Is Everything Sociality and Privacy in Online Social Network Sites". Página 10.
[9] Altshuler, Y.; Elovici, Y.; Armin B.; Nadav, C. [eds.] (2013). "*Security and Privacy in Social Networks*." Página 14.

depositada en la cuenta aunque la configuración sea privada. Por otro lado, lo más común es que empresas de publicidad que colaboran con las redes sociales tengan acceso a la misma información. Por último, de nuevo en función de la configuración de la cuenta, lo normal es que los amigos-de-amigos puedan acceder a la información compartida en tu cuenta con tus amigos. La pregunta que se hacen los expertos, por tanto, es en qué momento una información publicada tiene el derecho a optar a las garantías asociadas a la privacidad. El hecho de que un individuo elija compartir información con otros usuarios no debería necesariamente destruir su expectativa razonable de que se respete la privacidad respecto de terceros[10].

Dado que muchas personas confían en los operadores digitales para que protejan su privacidad digital, la solución más evidente está en el mercado digital en sí mismo. Si existe un desconocimiento abrumador respecto del tipo, cantidad y frecuencia de la información que se recolecta y se comparte para fines lucrativos, los operadores en sí deberían asumir un rol más activo en la protección de la privacidad de sus usuarios a través de sus políticas de privacidad. Esto permitiría que los usuarios puedan adoptar una decisión formada y una elección deliberada sobre la transmisión de los datos a estas empresas desde un principio[11].

La herramienta legal más importante a la hora de informar a los usuarios sobre el uso que se hace de sus datos personales es la política de privacidad. Si bien ahora lo encontramos ahora de forma generalizada en los sitios web en Internet, eran virtualmente inexistentes antes de 1998. El auge de las políticas de privacidad comenzó como un esfuerzo por parte de la industria de autorregular este aspecto y evitar escrutinios regulatorios. El rápido crecimiento de las políticas de privacidad es un mero reflejo del exponencial crecimiento de Internet y de los problemas relativos a la privacidad que lo acompañan[12].

En este trabajo se hace un exhaustivo análisis de las políticas de privacidad en el marco de las redes sociales, usando como referencias las redes sociales más populares en España. En primer lugar, se presentará el contexto necesario para entender el concepto de privacidad y la importancia de su protección. A continuación, en el aparado IV de este trabajo se llevará a cabo un estudio de las políticas de privacidad de las redes sociales Facebook, WhatsApp y YouTube (Google), para finalmente llegar a la conclusión de los riesgos principales identificados y puntos de mejora por parte de los operadores de las redes sociales y de los propios usuarios. Veremos que los problemas de privacidad no son una consecuencia de incompetencia o de malas intenciones, sino más bien las consecuencias naturales del uso entusiasta – en exceso –que se hace de las redes sociales.

[10] Argento, Z. (2013) "*Whose Social Network Account? A trade Secret Approach to Allocating Rights*". Michigan Telecommunications and Technology Law Review. Vol 19(3). Página 235-236.
[11] Op. Cit. (2016) "*The Price of Privacy: How access to digital privacy is slowly becoming divided by class*". UCLA Journal of Law & Technology. Página 29.
[12] Kim, N. (2014) "Three's A Crowd: Towards Contextual Integrity In Third-Party Data Sharing". *Harvard Journal of Law & Technology*. Vol 28 (1). Página 328.

III. Concepto de "intimidad" y "privacidad"

Históricamente, la protección de los datos personales y el respeto a la vida privada son reconocidos como derechos fundamentales y de especial importancia. En concreto en España, el artículo 18.1 de la Constitución española no garantiza sin más la "intimidad", sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público (Sentencia del Tribunal Constitucional 144/1999, de 22 de julio). La intimidad, en cuanto derivación de la dignidad de la persona que reconoce el art. 10 CE, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (Sentencias del Tribunal Constitucional 209/1988, 231/1988, 197/1991, 94/1994, 143/1994, 207/1996, etc.). Este es el criterio mantenido por el Tribunal Constitucional desde el inicio de su actividad y, jurisprudencialmente, el concepto de intimidad es el más extenso al afectar a todas las facetas de la persona[13].

Asimismo, en el marco de la Unión Europea se ha tratado siempre de encontrar un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada[14]. Así, en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) se establece en su artículo 16.1 que "*toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*".

En este sentido, los principales instrumentos en materia de protección de datos siempre han reconocido el respeto de la vida privada y la protección de los datos de carácter personal como derechos fundamentales. Así lo establece la Carta de los Derechos Fundamentales de la Unión Europea en los artículos 7 y 8 o el artículo 8 del Convenio Europea para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), de 4 de noviembre, que consagra el derecho al respeto de la vida privada y familiar: "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*"[15].

En España, el nivel de concienciación respecto a la protección de derecho a la intimidad y a la protección de datos personales ha ido en aumento. Prueba de ello, es la publicación de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE) al considerar la nueva realidad social que ha supuesto el uso de las TIC en general e Internet en particular, y disponer las bases normativas para una regulación de Internet y sus servicios, de manera completa, íntegra y efectiva[16].

[13] García, C. (2003) "*El derecho a la intimidad y dignidad del Tribunal Constitucional*". Colección Estudios de Derecho. Página 188.
[14] Milt, K. *Fichas Técnicas sobre la Unión Europea (La protección de datos personales).* Unión Europea. Junio 2017. Página 1.
[15] Op. Cit. *Fichas Técnicas sobre la Unión Europea (La protección de datos personales).* Unión Europea. Junio 2017. Página 2.
[16] INTECO y AEPD (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Página 10.

Asimismo, en la actualidad, la reforma de la protección de datos de la Unión Europea busca fortalecer los derechos de los ciudadanos, dotándoles de un mayor control de sus datos y garantizando a su vez que su privacidad sigue protegida en la era digital. Este es, al fin y al cabo, uno de los principales objetivos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 que entra en vigor en mayo de 2018 y por el que se deroga la actual Directiva 95/46CE (el "**Reglamento General de Protección de Datos**" o "**RGPD**"). Con esta reforma, por tanto, se pretende aumentar el control de los datos por parte de los usuarios teniendo en cuenta los avances tecnológicos y la globalización que, sin lugar a dudas, han tenido un profundo impacto en los métodos de recogida, acceso y uso de los datos.

El RGPD nos ofrece en su artículo 4 una definición de lo que se entiende por "datos personales", esto es, toda aquella información sobre una persona identificada o identificable. Se considera que será identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador concreto (un nombre, número de identificación, localización) o a través de varios elementos propios de su identidad (por ejemplo, identidad física, fisiológica, económica, cultural o social)[17].

Por otro lado, el término privacidad al que hacemos referencia a lo largo de esta exposición podría parecer un anglicismo de la palabra "*privacy*" y es, por este motivo, frecuentemente rechazado. En general, se opta por referirse a la "intimidad" o la "vida privada", sin embargo, el concepto de privacidad tiene una connotación que no coincide enteramente con la de intimidad. A efectos del presente análisis, se emplearán ambos conceptos de forma equivalente pues de una forma u otra estamos ante un derecho que es reconocido hoy en la práctica totalidad de los ordenamientos, internacional y nacional, lo cual va más allá del plano estrictamente jurídico[18].

A pesar de que la privacidad es actualmente uno de los temas más debatidos, debido a la complejidad de los elementos que la componen, no existe una definición exacta y unánime respecto a lo que se entiende por privacidad[19]. Ahora bien, se viene entendiendo más amplio el concepto de "privacidad" que el de "intimidad". De forma que si el concepto de intimidad busca proteger la esfera en que se desarrollan las facetas más singularmente reservadas de las personas – por ejemplo, el domicilio donde realiza su vida cotidiana – la privacidad, por el contrario, constituye un conjunto más amplio, más global, de facetas de la personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que,

[17] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 que entra en vigor en mayo de 2018 y por el que se deroga la actual Directiva 95/46CE (Reglamento General de Protección de Datos).
[18] Arce, A. *"El Derecho a la Intimidad" de Samuel D. Warren y Louis D. Brandeis*. Revista Española de Derecho Constitucional. Año 16, núm 47. Mayo-Agosto 1996. Página 369.
[19] Patil, S., Kobsa, A. "*The Challenges in Preserving Privacy in Awareness Systems*" University of California, Irvine. Página 3.

coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado[20].

En un esfuerzo común por dar forma al concepto de privacidad, el libro "*Security and Privacy in Social Networks*" en su capítulo segundo trata aspectos fundamentales de la seguridad y privacidad en las redes sociales[21]. Con este propósito, se introducen tres perspectivas principales desde el que analizar la privacidad[22] [23]:

1. **Perspectiva Legal**: Este aspecto se centra en las leyes y políticas de protección del individuo por parte de empresas, gobiernos y otros individuos. Por ejemplo, el RGPD que busca promover y asegurar el derecho del individuo a controlar la recogida y uso de sus datos.
2. **Perspectiva Técnica**: Este aspecto transfiere las normas y códigos en especificaciones técnicas. La norma P3P (plataforma de preferencias de privacidad) es un claro ejemplo del esfuerzo por aumentar la capacidad del individuo de controlar la información que se divulga por medios técnicos.
3. **Perspectiva Social**: Este aspecto se centra en la gestión de las relaciones sociales y los límites entre la vida pública y la privada. Así, Nissenbaum describe la privacidad como la integridad contextualizada, argumentando que la información personal se publica respecto de un entorno social claramente definido. Existirá violación de la privacidad desde el momento en que dicha información está disponible fuera del entorno al que estaba destinado.

Tomando como referencias estas tres perspectivas, se ponen en relación con las notas características de la privacidad – *data sovereignty*, *data transience*, *audience segregation*, *privacy awareness*, *transparency* y *enforcement* – tal y como se analizará en los apartados III.1 y III.2 del presente trabajo desde el punto de vista de las relaciones entre usuarios y desde el punto de vista de las relaciones entre operadores y usuarios, respectivamente.

[20] Op. Cit. (2003) "*El derecho a la intimidad y dignidad del Tribunal Constitucional*". Colección Estudios de Derecho. Página 285.
[21] Netter, N.; Herbst, S.; Pernul, G. 2013. "*Interdisciplinary Impact Analysis of Privacy in Social Networks*". Altshuler, Y.; Elovici, Y.; Cremers, A.B.; Aharony, N.; Pentland, A. (Editores). "*Security and Privacy in Social Networks*". Páginas 14-33.
[22] Patil, S.; Kobsa, A. (2009) *Privacy considerations in awareness systems: designing with privacy in mind*. Markopoulos, P.; Mackay, W.; Ruyter, B. (Editores) Página 4.
[23] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 19.

III.1. Concepto de Privacidad entre Usuarios

Desde el punto de vista de las relaciones entre usuarios de las redes sociales, nos permite hacernos una idea del impacto que puede llegar a tener cada uno de los aspectos legales, técnicos o sociales sobre la privacidad de cada individuo[24][25].

III.1.1. Control sobre los datos personales ("Data Sovereignty")

Para que una información de un usuario se considere privada debe existir un estricto control sobre su procesamiento. En este sentido, los datos personales en las redes sociales se suelen incluir de una forma sistematizada que pone en peligro la privacidad del usuario al perder control sobre sus datos que pueden ser copiados o transferidos. Evidentemente, en el marco de un mundo digital no se cuentan con las barreras propias de un mundo físico y real que limita en mayor medida el flujo de información que se transmite.

Desde la perspectiva legal, las leyes y políticas de privacidad que aplican respecto del intercambio y flujo de datos personales a día de hoy no son muy relevantes y, por tanto, no se considera que sea un factor determinante que contribuya a afianzar el control sobre los datos personales.

Desde la perspectiva técnica, en cambio, sí se puede considerar un medio efectivo para reforzar dicho control sobre los datos personal aunque el impacto global es menor precisamente por limitarse a un carácter de soporte.

Desde la perspectiva social, el control sobre los datos personales se ve amenazado desde el momento en que la información personal se extrae del entorno al que estaba destinado. Etiquetar a personas en fotos, algo tan común en las redes sociales, es un claro ejemplo de cómo se pierde el control del flujo de los datos personales. Las normas sociales podrían reforzar el control de los usuarios sobre sus datos personales si se trasladasen al mundo digital las mismas normas que aplican en las relaciones del mundo real. Se podrían describir los lazos sociales que se encuentran en el mundo real como lazos fuertes que reflejan la confianza que se genera entre dos personas que se conocen bien y, cualquier abuso de esa confianza terminaría por tener un impacto negativo en los lazos existentes de la relación[26]. Mientras que hay estudios que indican que los usuarios de las redes sociales cada vez tienen lazos más débiles entre ellos en dicho contexto que se alejan de la estabilidad y confianza del mundo real[27] [28] [29]. Donde cualquier individuo pasa a ser un "contacto" o a llamarse incluso "amigo". De forma que para considerar que el aspecto social podría tener un impacto relevante en el contexto

[24] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". (2013) Páginas 4-5.
[25] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". (2013) Páginas 20-25.
[26] Donath, J.; Boyd, D. (2004) "Public displays of connection*". BT Technology Journal*. Vol. 22(4). Páginas 71–82.
[27] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". (2013) Página 21.
[28] Boyd, D. (2004) *Friendster and publicly articulated social networking*. Páginas 2 y 4.
[29] Gross, R.; Acquisti, A. (2005) "*Information revelation and privacy in online social networks (The Facebook Case)"*. Página 3.

del control de los datos personales podríamos concluir que tiene el potencial suficiente para incrementar dicho control pero está aún lejos de ser efectivo. Por eso se concluye que el impacto que tiene el aspecto social sobre el control que ejerce un usuario sobre los datos personales en el contexto digital es medio – tal y como se muestra en la **Figura 1.1** – debido a que los lazos que se crean en las redes sociales son aún demasiado débiles y no están a la altura de aquellos lazos que se crean en la vida real[30].

III.1.2. La fugacidad de los datos ("Data Transience")

La fugacidad de los datos se refiere a la pérdida de información personal con el paso del tiempo que es característico del mundo real. Por el contrario, en el mundo digital, el almacenamiento de la información personal resulta ser permanente. Siempre nos hemos caracterizado en la vida por olvidar más de lo que recordamos pero con la ayuda de la tecnología el olvido ha pasado a convertirse en la excepción y recordar en la regla general. Este es uno de los principales obstáculos con el que se encuentra la privacidad de nuestros días en que un usuario se ve imposibilitado a construirse una nueva identidad debido a la cantidad de información contradictoria que existiría en el mundo *online*.

La comunicación tal y como se lleva a cabo en el mundo digital, en consecuencia, difiere notablemente de cómo se comunica uno en el mundo real, pues se añade el factor de permanencia, rastreabilidad, replicabilidad y escalabilidad[31].

Sin embargo, los usuarios de las redes sociales no se pueden ver obligados legalmente a eliminar información personal que ha sido compartida voluntariamente pasado el tiempo de la divulgación. Por este motivo, respecto de la fugacidad de los datos, la influencia legal es nula, tal y como se aprecia en la **Figura 1.1**.

Desde un punto de vista técnico, fijar una fecha de caducidad a la información publicada es difícil porque en cualquier caso la información ya divulgada puede ser replicada y fácilmente copiada, lo que impide eliminar información del mundo digital. Aunque ya existen iniciativas para tratar de hacer posible tecnológicamente la fugacidad de los datos[32], implementen políticas de trazabilidad más eficientes basadas en agentes que tutelen los flujos informativos de la información privada de los individuos, que es a lo que se tiende en el futuro aunque de momento no tienen un impacto significativo.

Por otro lado, desde la perspectiva social, la permanencia de la información personal en las redes sociales supone un reto significativo. El claro desconocimiento de los usuarios de las redes sociales respecto de las políticas de

[30] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 21.
[31] Boyd, D. (2008) "*Taken out of context: American teen sociality in networked publics*". Ph.D. thesis, University of California, Berkeley. Páginas 16, 26 y 40.
[32] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 21-23.

períodos de preservación de los datos[33] implica que las normas sociales no puedan suponer un factor relevante a la hora de promover la fugacidad de los datos.

III.1.3. Segregación del público ("Audience Segregation")

Se trata de un concepto originalmente desarrollado por Goffman[34], según el cual la segregación del público permite que un individuo efectúe, en su día a día, diferentes roles en un principio contradictorios. Debiendo por tanto segregar los públicos dependiendo del rol de forma que un público de un rol determinado no vislumbre cómo juega un papel y le vea actuar de una forma que no corresponde con ese contexto, manteniendo con ello la imagen y privacidad que le corresponde. En las redes sociales todos los contactos se clasifican a menudo como "amigos" sin diferenciarse adecuadamente dichos públicos y dificultando con ello la posibilidad de distinguir la información que se comparte con uno y otro grupo. La privacidad se ve con ello amenazada permitiendo a un gran público indiferenciado acceder a una gran cantidad de información personal.

El gestionar cómo se presenta uno ante distintos públicos en su rutina diaria no es competencia ni se regula por el ámbito legal, no teniendo por tanto impacto alguno la ley sobre la segregación del público.

En lo que se refiere a la perspectiva técnica, en muchas redes sociales nos encontramos con que ya se han implementado medidas para facilitar la segregación de grupos. Así, el papel tecnológico en este caso tiene un impacto medio y se prevé que vaya en aumento con el crecimiento de los adelantos tecnológicos.

Desde un punto de vista social, la segregación de públicos no se encuentra respaldada en las actuales redes sociales siendo los propios usuarios los que deben establecer una estrategia para canalizar las comunicaciones usando distintas formas de comunicación – por ejemplo, a través de mensajes privados –

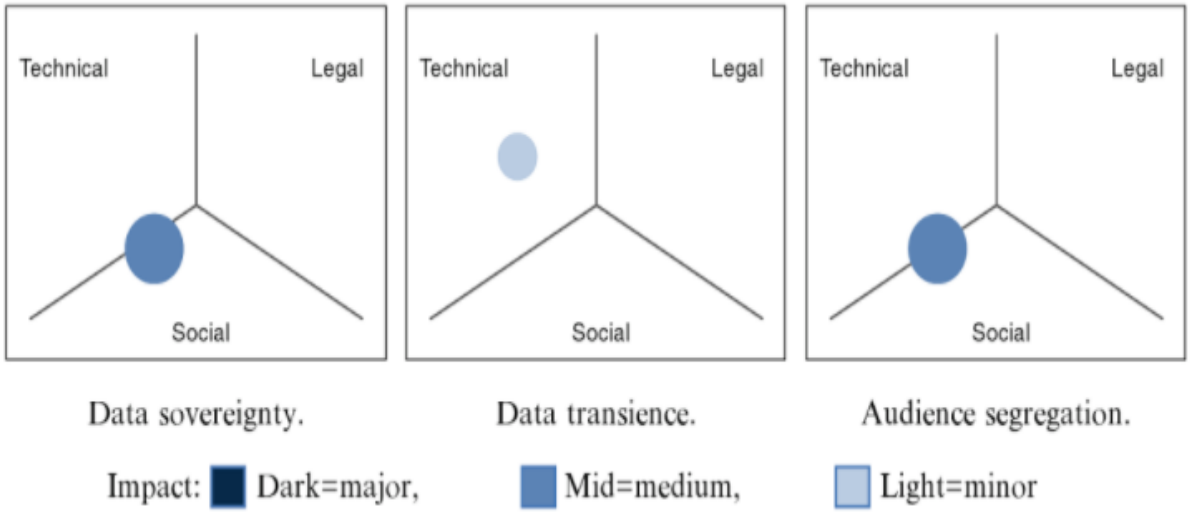


Figura 1.1 - Concepto de Privacidad entre Usuarios

[33] Op. Cit. (2005) "*Information revelation and privacy in online social networks (The Facebook Case)"*. Página 3.
[34] Goffman, E. (1959) "*Presentation of Self in Everyday Life*". Nueva York: Anchor.

y a través de estrategias mentales – autocensura – [35]. No obstante, los estudios demuestran que el gestionar diferentes públicos en el mundo digital resulta una carga y rara vez se lleva a cabo[36]. Por esto, sólo se le atribuye al aspecto social un impacto medio en la protección de la privacidad en lo que se refiere a la segregación de públicos[37].

III.1.4. Conciencia de privacidad ("Privacy Awareness")

La toma de conciencia respecto a la privacidad abarca la atención, percepción y conocimiento de la información personal que otros han recibido y cómo dicha información es o debe ser procesada. Sin duda, la conciencia del individuo respecto del riesgo que amenaza a su propia privacidad es absolutamente necesario para permitir encontrar una conducta que permita proteger su privacidad.

Una vez más, el aspecto legal no tiene ningún impacto sobre la conciencia de privacidad puesto que la legislación no puede imponer a un usuario dicha percatación del riesgo que recae sobre su privacidad.

A su vez, los medios técnicos en este sentido únicamente tienen una naturaleza de apoyo por el que pueden contribuir a facilitar dicha conciencia de privacidad y llamar la atención respecto de los posibles riesgos de su violación pero que significa que el impacto en este caso es mínimo, tal y como se aprecia en la **Figura 1.2**[38].

De manera que la conciencia de privacidad es principalmente un concepto en el que se puede hallar una amplia brecha entre la conciencia teórica y práctica[39]. Al respecto se encuentran estudios que respaldan el hecho de que los usuarios a menudo subestiman los riesgos hacia la privacidad y rara vez emplean los ajustes de privacidad que están a su disposición[40] [41]. Se considera que ello se debe a que la gratificación que supone una publicación a corto plazo pesa más que el beneficio a largo plazo, lo que supone una visión distorsionada del usuario a la hora de evaluar el riesgo en que pone su privacidad[42]. Por lo que esa brecha que

[35] Lampinen, A.; Tamminen, S.; Oulasvirta, A. (2009) "*All my people right here, right now: management of group co-presence on a social networking site*". Proceedings of the ACM 2009 international conference on supporting group work. Páginas 281-290.
[36] DiMicco, J.M.; Millen, D.R. (2007) "*Identity management: multiple presentations of self in Facebook*".
[37] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 22.
[38] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013
[39] Op. Cit. (2004) "*Public displays of connection"*. BT Technology Journal 22(4):71–82
[39] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". (2013) Páginas 71–82
[40] Op. Cit. (2004) "*Friendster and publicly articulated social networking*".
[41] Op. Cit. (2005) "*Information revelation and privacy in online social networks (The Facebook Case)"*.
[42] Acquisti, A. (2004) "*Privacy in electronic commerce and the economics of immediate gratification*". Página 4.

identificamos entre la teoría y la práctica lleva a concluir que el impacto social en crear una conciencia de protección de la privacidad es de nivel medio[43].

III.1.5. Transparencia ("Transparency")

En relación con los prestadores de servicios de redes sociales, la transparencia se refiere a la capacidad del usuario de estar informado respecto de las prácticas de procesamiento y divulgación y de entender las implicaciones del flujo de la información personal dentro de las redes sociales para poder conocer y distinguir los límites que garantizan la integridad contextual de los datos personales.

Aunque inicialmente pueda asociarse con la conciencia de privacidad que ya hemos analizado, la transparencia tiene por objetivo realzar la comprensión de los usuarios respecto de la difusión de sus datos personales dentro de las redes sociales para proteger de forma más efectiva el uso no autorizado a su información personal.

Desde la perspectiva legal, el individuo cuenta con escasos medios para obligar a otros usuarios a revelar de forma transparente la difusión que hacen de la información ajena puesto que no existe normativa aplicable que lo regule o imponga.

Desde un punto de vista técnico, se conocen ya acercamientos que buscan reforzar la transparencia en las redes sociales, centrándose en un análisis retrospectivo de la difusión de los datos personales[44]. No obstante, en la práctica, los lazos débiles que caracterizan la forma imprecisa en que se divulga la información - "amigos de amigos" - conllevan que se cree una red de contactos excesivamente amplia que hace inevitable que la información se propague de una forma nada transparente[45]. Por lo que la efectividad de las aproximaciones tecnológicas para asegurar la transparencia del flujo de información depende en gran medida de los prestadores de servicios de las redes sociales y la programación que hacen de sus interfaces (APIs). De acuerdo con este razonamiento, sólo se le podría atribuir un nivel medio – tal y como se aprecia en la **Figura 1.2**[46] – de impacto del aspecto técnico a la efectividad de la transparencia en las redes sociales[47].

De forma similar a como ocurre con el aspecto legal, la difusión de información personal por otros usuarios de las redes sociales no está habitualmente gobernada por las normas sociales, lo que supone que no hay impacto alguno desde una

[43] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 23.
[44] Kolter, J.; Netter, M.; Pernul, G. (2010) "*Visualizing past personal data disclosures*".
[45] Op. Cit. (2005) "*Information revelation and privacy in online social networks (The Facebook Case)".* Página 3.
[46] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013.
[47] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 23.

perspectiva social sobre la transparencia de los datos personales en las redes sociales[48].

III.1.6. Ejecución ("Enforcement")

La ejecución se refiere a los medios con que cuenta un individuo para hacer efectivas sus preferencias de privacidad. Es decir, hasta qué punto el usuario puede controlar la adhesión a una política de privacidad impuesta por las redes sociales y gestionar sus limitaciones.
La imposición de la normativa legal es una nota inherente a cualquier sistema jurídico. En el marco de la privacidad en las redes sociales un individuo podrá interponer una medida cautelar si se divulga información que atenta contra su reputación o dignidad. Sin embargo, dichas acciones legales no son universalmente aplicables en el mundo digital. Tal y como lo establece el Tribunal de Justicia Europeo (TJUE), la protección legal requiere que la información personal que se pretende proteger estuviese originariamente limitada a un grupo privado y cerrado de amigos y familia para poder imponerse medidas legales, que rara vez es el caso de por sí en las redes sociales[49]. Asimismo, las acciones legales a disposición del usuario únicamente entran en juego una vez producido una violación de la privacidad y, por tanto, juega un papel menor y resulta en un impacto poco relevante cuando lo que se pretende es precisamente proteger dicha privacidad y tratar de evitar que se atente contra la misma.

Precisamente los medios técnicos de rectificación podrían tener un impacto positivo en la ejecución de medidas legales. Sin embargo, de momento no existe uniformidad en la forma en que las redes sociales ofrecen herramientas para enfrentarse a estos problemas – por ejemplo, el *cyber-bullying* –[50] y se limita de nuevo a una función secundaria de apoyo que apenas tiene un impacto en la efectividad de la ejecución de las medidas a disposición del usuario.

[48] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Páginas 23-24.
[49] Dix, A. (2010) Daten- "Personlichkeitsschutz im Web 2.0". Klumpp, D.; Kubicek, H.; Nagel A.; Schulz, W. (eds) *Netzwelt-Wege, Werte, Wandel*. Berlin/Heidelberg : Springer. Páginas 195–210.
[50] Bonneau, J., Preibusch, S. (2009) "*The privacy jungle: on the market for data protection in social networks*". Página 21.

En cuanto al aspecto social, como ya hemos visto anteriormente, los lazos en las relaciones que se crean en las redes sociales son demasiado débiles[51] como para que puedan permitir que las normas sociales puedan producir un efecto significativo sin que la presión que se ejercen los usuarios entre sí tenga un impacto relevante a la hora de garantizar la ejecución y efectividad de la privacidad en la red[52].

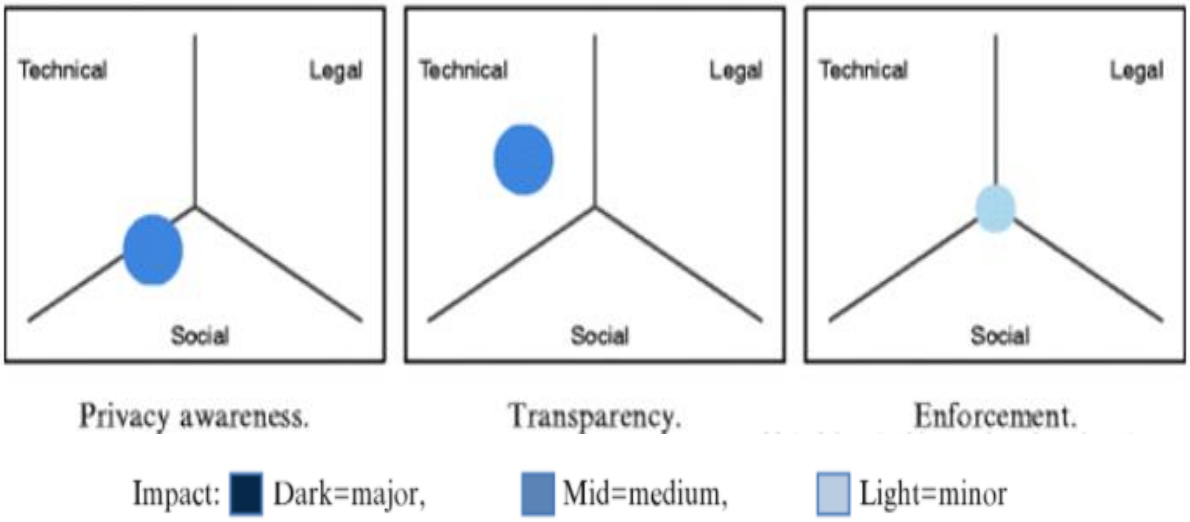


Figura 1.2 - Concepto de Privacidad entre Usuarios.

III.1.7. Resumen

La **Tabla 1**[53] muestra que las conclusiones alcanzadas una vez analizadas las características del control sobre los datos, la fugacidad de los datos, la segregación de los públicos, la conciencia de privacidad, la transparencia y la ejecución en el marco de las redes sociales desde unas perspectivas legales, técnicas y sociales se puede concluir que la protección de la privacidad y del uso que hacen otras personas en las redes sociales de tu información está principalmente cubierta por las normas sociales. Lo cual se corresponde con el mundo real donde los usuarios dependen en gran medida de esa difusión selectiva de sus datos personales y de las relaciones especialmente construidas sobre la base de confianza para poder garantizar su privacidad.

La función técnica y los acercamientos tecnológicos por tratar de proteger la privacidad de los usuarios en el mundo digital finalmente se ven reducidos de momento a un papel secundario de soporte para hacer efectivas las normas impuestas socialmente en la red pero que se prevé que siga en aumento en el futuro en la medida en que las reglas sociales se vayan imponiendo en el entorno digital.

Por el contrario, las medidas legales juegan un rol residual y son, en todo caso, un último remedio que únicamente puede tratar de subsanar una situación una vez se

[51] Op. Cit. (2005) *Information revelation and privacy in online social networks (The Facebook Case)*. Página 3.
[52] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Páginas 24-25.
[53] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 25.

ha producido ya la violación de privacidad de una persona, con el daño que ello conlleva. Al respecto, hay autores que afirman que la ley hace poco por dar forma a las expectativas de privacidad de las personas[54].

En cualquier caso, el carácter intervenido de las redes sociales con su almacenamiento de la información y rastreabilidad de los datos personales no hace sino añadir capas complejas que afectan a la privacidad de las personas en tanto en cuanto el entorno de información de las redes sociales es contradictorio con las normas que rigen en el mundo real respecto de la misma información[55].

	Data sovereignty	Data transience	Audience segregation	Privacy awareness	Transparency	Enforcement
Legal						
Technical						
Social						

Impact: Dark = major, Mid = medium, Light = minor

Tabla 1 - Concepto de Privacidad entre Usuarios. Resumen.

[54] Strahilevitz, L. (2005) "A social networks theory of privacy". *University Chicago Law School Review* 72(3). Páginas 919–988

[55] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 25.

III.2. Concepto de Privacidad para los Prestadores de Servicios de Internet

Al igual que hemos realizado un análisis del concepto de privacidad en el marco de las relaciones de los usuarios, a continuación procederemos a estudiar el impacto que tienen los prestadores de servicios sobre los temas que afectan a la privacidad de los usuarios para poder contar con una visión global de la privacidad en el mundo digital.

III.2.1. Control sobre los datos personales ("Data Sovereignty")

Con el objetivo de garantizar el control sobre los datos personales, se han promulgado normas legales para controlar la explotación que hacen los prestadores de servicios de los datos personales recolectados en las redes sociales. Por ejemplo, en España la Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI) y la Ley Orgánica de Protección de Datos (LOPD) o en Alemania la equivalente Ley de Teleservicios y Ley Federal de Protección de Datos, que exigen – al igual que el próximo RGPD en vigor en mayo de 2018 – el consentimiento expreso del usuario para poder usar los datos personales con fines promocionales. Además, las exigencias legales que se imponen a los prestadores de servicios de las redes sociales requieren que se almacene la información de forma segura evitando cualquier clase de indexación por defecto que permita hacer que la información sea fácilmente localizable e identificable. De forma que en este contexto, el papel legal adquiere una importancia significativa y conlleva un impacto alto a la hora de reforzar la seguridad y el control sobre los datos personales del individuo.

Desde un punto de vista técnico, se han presentado ya numerosas propuestas[56] [57] que permiten asegurar el control sobre los datos personales del individuo en las redes sociales siendo las principales los métodos criptográficos y esteganográficos que resultan ser medios efectivos de proteger los datos personales al limitar el acceso de los prestadores de servicios. Aunque estos métodos podrían integrarse fácilmente en las redes sociales, el caso es que la realidad implica que actualmente supondría una violación de las condiciones generales de las redes sociales pues, al fin y al cabo, su negocio recae en ese libre acceso del que disponen los prestadores de servicios a los datos personales de sus usuarios. Por lo que aun siendo teóricamente fácilmente construible, las dificultades que se presentan en la práctica suponen que el impacto real del aspecto tecnológico en este caso sea medio, véase la **Figura 2.1**[58].

Por otro lado, dado que los prestadores de servicios no tienen una relación social directa con los usuarios de las redes sociales, el individuo no debe confiar en las normas sociales para asegurarse de que el prestador de servicio cumplirá con una

[56] Guha, S.; Tang, K.; Francis, P. (2008) "*NOYB: privacy in online social networks*".
[57] Baden, R.; Bender, A.; Spring, N.; Bhattacharjee, B.; Starin, D. (2009) "*Persona: an online social network with user-defined privacy*".
[58] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013.

obligación social de garantizar el control de los datos personales. Por lo que desde una dimensión social, el impacto es inexistente[59].

III.2.2. La fugacidad de los datos ("Data Transience")

Al igual que ocurre con el control de los datos personales, el ámbito legal cubre con sus normas la fugacidad de los datos que han de respetar los prestadores de servicios de forma que los usuarios tienen derecho a solicitar que se borren todos sus datos personales almacenados en un determinado perfil creado en sus redes sociales y cancelar su suscripción[60]. Además, yendo un paso más allá, la normativa europea les impone a los prestadores de servicios la obligación de eliminar todos aquellos datos que ya no sean necesarios para el fin para el que fueron recolectados[61]. Esto sitúa al usuario en una posición de fuerza y supone un alto impacto del aspecto legal a la hora de garantizar la fugacidad de los datos y proteger con ello en mayor medida la privacidad de los usuarios en la red.

En cambio, las aproximaciones que se han hecho[62] desde un punto de vista técnico han tenido un impacto menor pues las redes sociales en sus condiciones generales prohíben el uso de herramientas que pongan restricciones al acceso de los datos personales.

Asimismo, como ya hemos visto, la falta de relación social entre los usuarios y los prestadores de servicios hace que sea inexistente el impacto social sobre la fugacidad de los datos en el mundo digital[63].

III.2.3. Protección contra la elaboración de perfiles ("profiling")

La protección contra la elaboración de perfiles no es sino la capacidad que tiene un individuo para evitar que otra persona recabe, agregue y vincule sus datos personales con el fin de crear un dossier digital sobre el mismo. El peligro de *profiling* se ve incrementado desde el momento en que se pueden conectar los datos de geolocalización (a través de los dispositivos móviles) y los registros de conexión a las redes sociales existentes. La relevancia de esta amenaza se ve acentuada por las implicaciones que conlleva, que abarca peligros desde el robo de identidades hasta la publicidad personalizada.

[59] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Páginas 26-27.
[60] Op. Cit. (2010) "*Daten- und Personlichkeitsschutz im Web 2.0*". In: Klumpp D, Kubicek H, Rob Nagel A, Schulz W (eds) Netzwelt-Wege, Werte, Wandel. Springer, Berlin/Heidelberg, páginas 195–210.
[61] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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 (Directiva 95/46/CE).
[62] Federrath, H.; Fuchs, K.P.; Herrmann, D.; Maier, D.; Scheuer, F.; Wagner, K. (2011) „*Grenzen des digitalen Radiergummis*". Datenschutz und Datensicherheit – DuD 35(6): Páginas 403–407
[63] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Páginas 26-27.

Tanto la OCDE[64] y la regulación europea[65] coinciden en que los retos a los que se enfrentan los principios de privacidad provienen en gran medida de los prestadores de servicios de las redes sociales y establecen que la reducción de los datos recolectados es una de las claves para evitar que los prestadores de servicios vinculen la información personal de la que disponen para elaborar dossiers digitales de sus usuarios. Ello se enfrenta, no obstante, al hecho de que la esencia del negocio de las redes sociales es precisamente el uso de los datos personales para fines promocionales de forma que siempre van a exigir ciertos atributos personales a la hora de registrarse un usuario y hay estudios que indican que solo 3 de 29 redes sociales permite el uso de pseudónimos al registrarse[66]. Esto denota que a pesar de existir normativas legales que lo regulan, en la práctica el impacto legal se considera menor.

Tecnológicamente, los mismos métodos criptográficos y esteganográficos que ya hemos visto podrían emplearse para evitar la elaboración de perfiles y hay otros estudios que proponen medidas alternativas pero, en general, el impacto ha sido menor en la protección contra el *profiling*, una vez más, porque las condiciones generales de las redes sociales lo prohíben.

Aquí, como en los supuestos anteriores, las normas sociales no tienen ningún impacto, tal y como se muestra en la **Figura 2.1**[67].

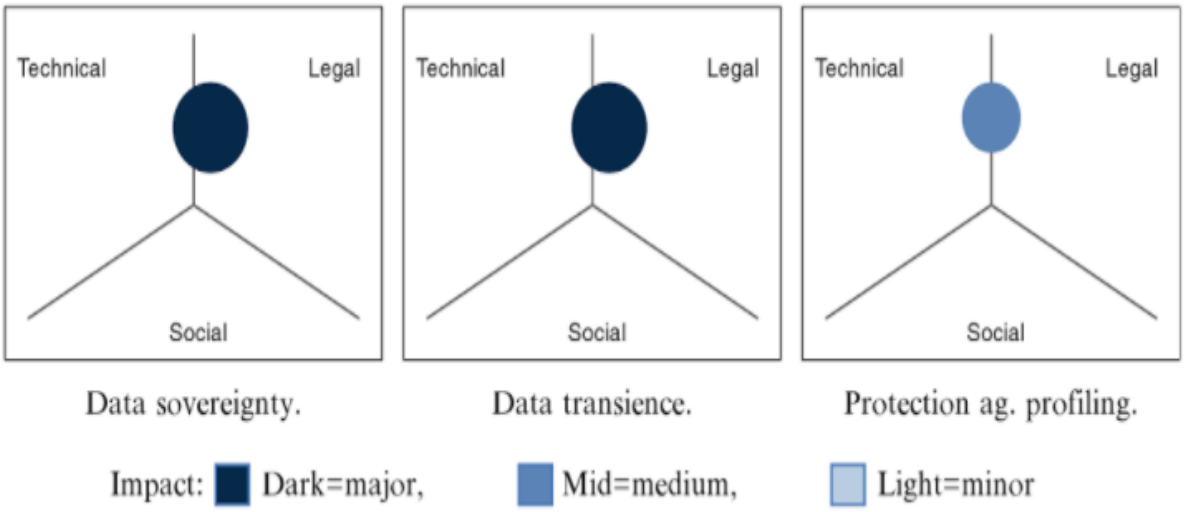


Figura 2.1 - Concepto de Privacidad entre Prestadores de Servicios.

III.2.4. Conciencia de privacidad ("Privacy Awareness")

[64] Organización para la Cooperación y el Desarrollo Económicos (OCDE). (1981) *Guidelines on the protection of privacy and transborder flows of personal data*, vol 11. Organisation for Economic Cooperation and Development, Paris.
[65] Directiva 95/46/CE.
[66] Op. Cit. (2009) "*The privacy jungle: on the market for data protection in social networks*". Página 16.
[67] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 27.

En este caso el impacto se asemeja al caso de la relación entre usuarios por el que la conciencia de privacidad está principalmente influenciada por el aspecto social mientras que las dimensiones legales y técnicas no contribuyen en absoluto.

Así, existen estudios que revelan que los usuarios de Facebook depositan más confianza en Facebook como prestador de servicios que en la media de usuarios de Facebook[68]. O estudios que muestran que el 56% de los usuarios de Facebook creen que Facebook no comparte información personal con terceros y el 70% cree que Facebook no combina la información que recolecta de otras fuentes. Un número menor a uno de cada cuatro usuarios dice haberse leído la política de privacidad de Facebook. De forma que mientras que los riesgos sobre la privacidad tienden a mantenerse invisibles[69] un incremento en la conciencia de privacidad supone un obstáculo demasiado grande en el crecimiento de los beneficios de los prestadores de servicios a través de las redes sociales[70]. Por lo que aunque los riesgos siguen existiendo de forma invisible y van en aumento, el hecho de que los usuarios de las redes sociales se hayan acostumbrado a este tipo de riesgo conlleva que el impacto social únicamente se puede considerar medio – tal y como se muestra en la **Figura 2.2**[71] – por insuficiente[72].

III.2.5. Transparencia (“Transparency”)

La primera fuente de información para evaluar el impacto legal sobre la transparencia de los prestadores de servicio no es otra que su política de privacidad. Tal y como han hecho ya otros estudios[73], veremos en detalle en el apartado IV las políticas de privacidad en relación con las redes sociales. Así, son muchos los defectos que se encuentran en las políticas de privacidad, partiendo de una falta de accesibilidad técnica – por ejemplo, requiriéndose JavaScript – hasta un uso extenso de complejos términos jurídicos que dificultan su comprensión por un usuario medio. Entre otros problemas que se han identificado, como que no se incluya la ley aplicable o el país donde se procesan o almacenan los datos[74]. Un estudio similar sobre la transparencia de los operadores de las redes sociales revela que los usuarios a menudo son incapaces de determinar la cantidad de datos personales que se requieren antes del registro[75]. Este mismo estudio muestra que incluso a peticiones realizadas por correo electrónico los operadores no proporcionan el apoyo adecuado para incrementar la transparencia respecto de cómo tratan los datos recabados. Por lo que, a pesar de la existencia

[68] Acquisti, A.; Gross, R. (2006) “*Imagined communities: awareness, information sharing, and privacy on the Facebook*”. Página 13.
[69] Debatin, B.; Lovejoy, J.P.; Horn, A.K.; Hughes, B.N. (2009) “Facebook and online privacy: attitudes, behaviors, and unintended consequences”. *Journal of Computer-Mediated Communication*, Vol. 15(1). Páginas 83–108.
[70] Ziegele, M.; Quiring, O. (2011) “Privacy in social network sites”. *Privacy online. Perspectives on privacy and self-disclosure in the social web*. Springer. Páginas 175-189.
[71] Op. Cit. “Interdisciplinary Impact Analysis of Privacy in Social Networks”. “*Security and Privacy in Social Networks*”. 2013.
[72] Op. Cit. “Interdisciplinary Impact Analysis of Privacy in Social Networks”. “*Security and Privacy in Social Networks*”. 2013. Página 27.
[73] Op. Cit. (2009) “*Persona: an online social network with user-defined privacy*”.
[74] Op.Cit. (2009) “*The privacy jungle: on the market for data protection in social networks*”. Página 23.
[75] Op. Cit. (2004) “Public displays of connection”. *BT Technology Journal.* Vol. 22(4). Páginas 71–82

de políticas de privacidad como instrumento valioso, únicamente se aprecia un impacto medio debido a las restricciones que hemos visto recaen sobre su aplicación en la práctica.

Desde un punto de vista técnico ya existen sistemas que permiten total transparencia. Un claro ejemplo de ello es la norma P3P [76] que requiere que los prestadores de servicios publiquen una política de privacidad interpretable por una máquina que contrasta las preferencias del usuario con las que vienen por defecto en las redes sociales. Sin embargo, los prestadores de servicios siguen reticentes a publicar dichas versiones de sus políticas de privacidad, haciendo que el sistema propuesta sea inaplicable. Igualmente, el definir las preferencias de privacidad no está al alcance de cualquier usuario puesto que requiere de conocimientos tecnológicos que le permitan elaborarlo. Teniendo todo ello en cuenta, la realidad es que el impacto tecnológico respecto de la transparencia del uso que se da a los datos personales es menor.

En lo que se refiere al aspecto social, podría jugar un rol importante la cobertura en los medios al difundir las prácticas de los prestadores de servicios de internet pero es raro encontrarse con un análisis exhaustivo al respecto principalmente debido a la falta de conciencia de protección de privacidad que ya hemos analizado. Por lo que tampoco la dimensión social tiene aquí un gran impacto[77].

III.2.6. Ejecución (“Enforcement”)

El principio general de ejecución que ya hemos visto en el apartado III.1.6 aplica igualmente en las relaciones entre usuarios y prestadores de servicios y hemos visto también el papel dominante en este contexto de la importancia de la normativa jurídica. En cualquier caso, las redes sociales suelen aplicar el enfoque de privacidad por política – “*privacy-by-policy”* – notificando y obteniendo de los usuarios el consentimiento a su política de privacidad con carácter previo al registro manteniendo con ello el impacto elevado del aspecto legal en este caso.

En relación con la dimensión técnica, a pesar de existir medidas que permiten hacer imponibles las preferencias de privacidad de los usuarios, ya hemos visto que las mismas no son efectivas y, por tanto, en este sentido, la perspectiva técnica en cuanto a su ejecución es baja teniendo en cuenta que dichas medidas están a menudo prohibidas por las condiciones generales de las redes sociales.

[76] Cranor, L.; Dobbs, B.; Egelman, S. (2006) “*The platform for privacy preferences 1.1 (P3P1.1) specification*”.
[77] Op. Cit. “Interdisciplinary Impact Analysis of Privacy in Social Networks”. “*Security and Privacy in Social Networks*”. 2013. Páginas 27-28.

En el caso de hacer imponer las normas sociales, al no existir relación social entre

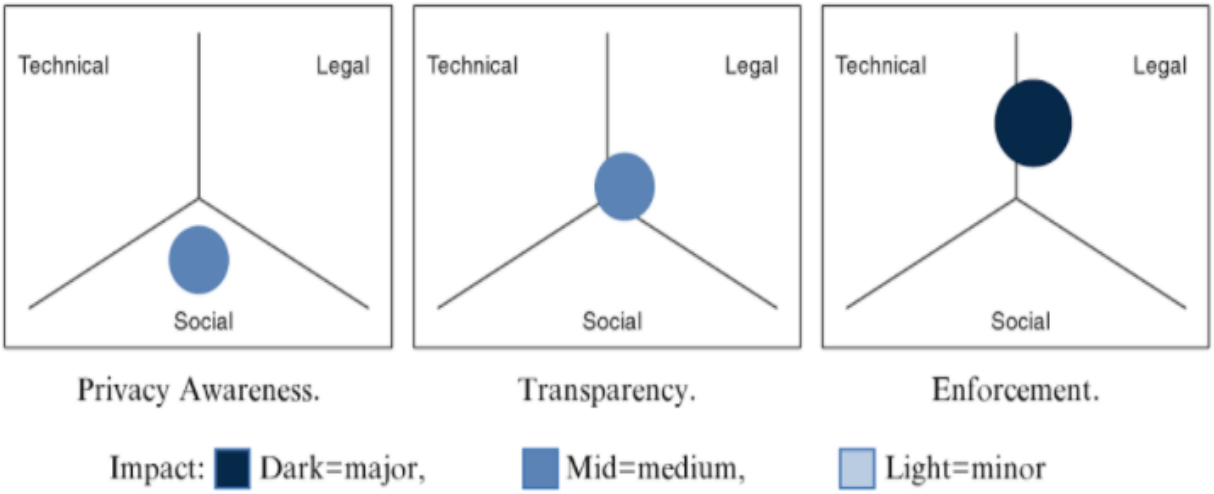


Figura 2.2 - Concepto de Privacidad entre Prestadores de Servicios.

los prestadores de servicios de las redes sociales y sus usuarios, no son ejecutables los intereses de protección de la privacidad a los prestadores de servicios y el impacto es nulo[78].

III.2.7. Resumen

Del análisis que hemos abordado en este apartado, podemos obtener dos conclusiones principales. En primer lugar, que hay un desplazamiento del impacto que tenía el aspecto social en el contexto de las relaciones entre usuarios que se ve sustituido por un papel más significativo de la perspectiva legal. En segundo lugar, se ve un incremento general en la relevancia de los impactos de todas las dimensiones. Especialmente relevante desde el punto de vista legal pues es indicativo de que los legisladores se han dado cuenta de que existe un desequilibrio de poderes entre los prestadores de servicios y los usuarios tratando, en consecuencia, de dotar al usuario de una posición de mayor fuerza. Todo ello queda reflejado en la **Tabla 2**[79].

Asimismo, el impacto menor que tienen las normas sociales en este contexto se puede justificar por la difusión de responsabilidades donde ni siquiera existe una relación social entre los jugadores principales – los prestadores de servicios y los propios usuarios de las redes sociales – no aplicándose las normas sociales en absoluto. Por último, al igual que ocurría en el marco de la privacidad entre usuarios, el aspecto técnico se ve limitado y constreñido a una función secundaria y de apoyo.

[78] Op. Cit. “Interdisciplinary Impact Analysis of Privacy in Social Networks”. “*Security and Privacy in Social Networks*”. 2013. Páginas 28-29.
[79] Op. Cit. “Interdisciplinary Impact Analysis of Privacy in Social Networks”. “*Security and Privacy in Social Networks*”. 2013.

Llaman la atención, en todo caso, las importantes limitaciones que existen respecto a la protección contra la elaboración de perfiles de los usuarios de las redes sociales, encontrándose una sólida negativa por parte de los prestadores de servicios en ceder al respecto por constituir una parte demasiado esencial en su modelo de negocio.

	Data sovereignty	Data transience	Protection ag. Profiling	Privacy awareness	Transparency	Enforcement
Legal						
Technical						
Social						

Tabla 2 - Concepto de Privacidad entre Prestadores de Servicios. Resumen.

IV. Redes Sociales y Políticas de Privacidad

Tal y como muestra la **Figura 3**[80], el término "privacidad" adquiere un nuevo significado en el contexto de las redes sociales, donde privacidad no significa sencillamente ocultar información sino que supone el legítimo control sobre la información personal de uno[81].

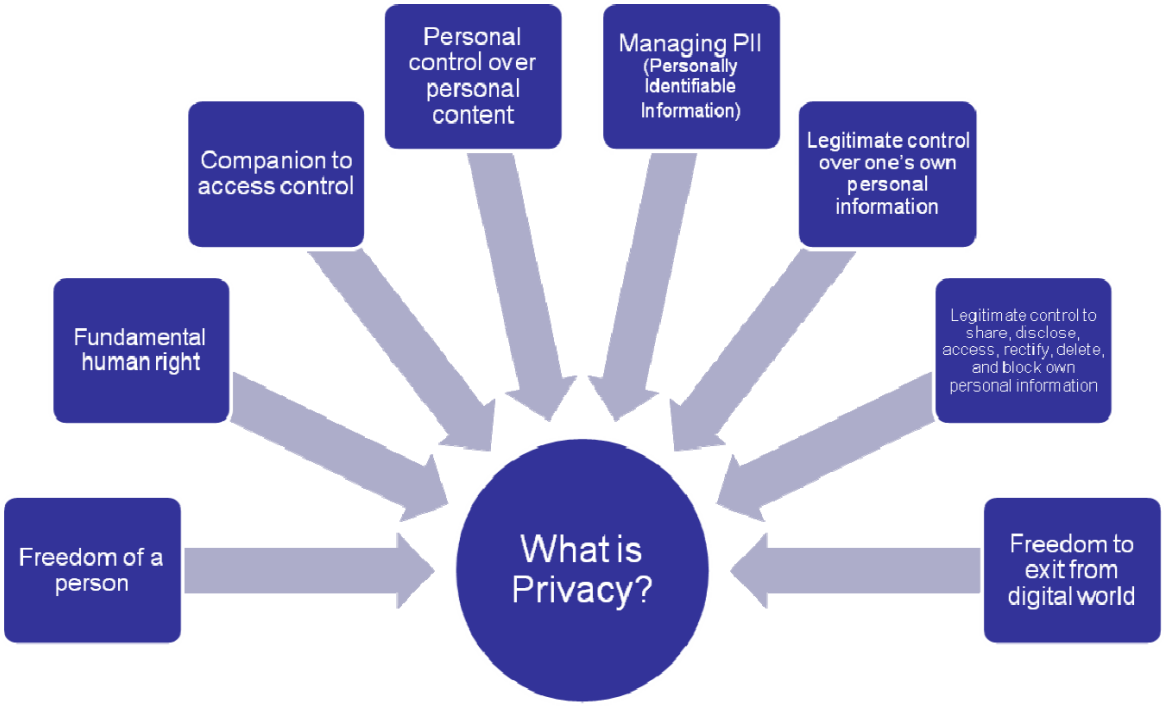


Figura 3 – ¿Qué es la privacidad?

En un sentido amplio, una red social es una estructura social formada por personas o entidades conectadas y unidas entre sí por algún tipo de relación o interés común. El término se atribuye a los antropólogos británicos Alfred Radcliffe-Brown y John Bames. Asimismo, podemos definir las redes sociales *online* como estructuras sociales compuestas por un grupo de personas con que compartes un interés común, relación o actividad a través de Internet, donde tienen lugar los encuentros sociales y se muestran las preferencias de consumo y de información mediante la comunicación en tiempo real, aunque también puede darse la comunicación diferida. La Real Academia Española la define, a su vez, como aquélla plataforma digital de comunicación global que pone en contacto a gran número de usuarios[82].

En España, un 86% de los internautas de entre 16-65 años utilizan redes sociales, lo que representa más de 19 millones de usuarios en nuestro país[83]. De los cuales un 77,5% se conecta a Internet todos los días y en un 64,4% se conecta a Internet para participar en redes sociales[84].

[80] Islam, M.B.; Iannella, R. (2010) "*Privacy by Design: Does It Matter For Social Networks*?" IFIP Advances in Information and Communication Technology, vol. 375.
[81] Op. Cit. (2010) "*Privacy by Design: Does It Matter For Social Networks*?" IFIP Advances in Information and Communication Technology, vol. 375. Página 3.
[82] Estudio Anual Redes Sociales. (2017). Página 17.
[83] Estudio Anual Redes Sociales. (2017). Página 9.
[84] CIS. Barómetro Febrero (2017). Pregunta 21a. Página 14.

En el presente estudio vamos a realizar un estudio de tres redes sociales seleccionadas en base a su uso en España, tal y como se muestra en la **Imagen 1**[85] – Facebook, WhatsApp y YouTube – y analizaremos cómo cada una de ellas tienen en cuenta la privacidad de sus usuarios accediendo a sus políticas de privacidad para comprender el uso que hacen de los datos de sus usuarios y, sobre todo, cómo se les informa sobre ello a los mismos.

Imagen 1 – Tres redes sociales más usadas en España.

Así, en lo que se refiere al uso o visita de las redes sociales, Facebook se mantiene como la red social por excelencia, seguida de WhatsApp y YouTube[86]. El uso principal que se hace de las redes sociales continúa siendo "social", es decir, chatear, enviar mensajes, ver qué hacen otros contactos, así como ver vídeos y escuchar música siguen siendo una actividad destacada debido a la fuerza de YouTube[87].

En estos momentos, en España nos encontramos con que existe un alto grado de concienciación en lo que respecta a la protección de datos personales y el posible uso de información personal por otras personas, donde según estudios recientes un 38,2% de los encuestados se preocupan mucho por este tema y un 37,8% se preocupa bastante[88]. Encuentran los encuestados, además, en un 80,5% que es muy probable o bastante probable que sus datos puedan ser utilizados sin su conocimiento[89] y el 96,9% de los españoles está de acuerdo o bastante de acuerdo con la necesidad de que las redes sociales no deberían comunicar datos personales a terceros sin autorización previa[90]. En general, se desconfía mucho de que las redes sociales cuiden de la seguridad de los datos personales de sus usuarios. De hecho, es alarmantemente abrumador (76,6%) el sentimiento de los usuarios de que no pueden controlar quién ve la información que se introduce en el perfil[91] y uno de cada cinco españoles (21,2%) se ha arrepentido alguna vez de

[85] Estudio Anual Redes Sociales. (2017). Página 21.
[86] Estudio Anual Redes Sociales. (2017). Página 21.
[87] Estudio Anual Redes Sociales. (2017). Página 30.
[88] CIS. Barómetro de Febrero de 2017. Pregunta 9. Página 11.
[89] CIS. Barómetro de Febrero de 2017. Pregunta 12. Página 11.
[90] CIS. Barómetro de Febrero de 2017. Pregunta 21g. Página 17.
[91] CIS. Barómetro de Febrero de 2017. Pregunta 21g. Página 17.

haber publicado un comentario, una foto o un vídeo en una red social[92] de los cuales el 8,8% ha tenido problemas por haberlo hecho[93].

La mayoría de los usuarios no son conscientes de la cantidad de información que se recolecta sobre ellos de forma encubierta a partir de las redes sociales, información que es recolectada, analizada y monetizada por los prestadores de servicios. La forma de recabar nuestra información comenzó siendo bastante discreta – preguntándonos si queremos que se recuerde la contraseña o el número de la tarjeta en una página web en concreto – pero poco a poco han ido recolectando información de las compras, búsquedas y hábitos a través de *cookies*, *web beacons*, *data scraping*, etc. Inevitablemente, las redes sociales han acabado por jugar un papel importante en las vidas públicas y privadas pero este avance de la tecnología no debe restringir la protección del consumidor, el poder del gobierno o la protección de los derechos del individuo[94].

Únicamente un 14,6% de los usuarios en Internet leen siempre o casi siempre las políticas de privacidad que les aplican[95] y casi a uno de cada dos usuarios (46%) admite que le importa más acceder a los servicios que le prestan los sitios web que la privacidad de sus datos[96].

En los que se refiere a las políticas de privacidad que rigen las redes sociales, además de ser contratos legalmente vinculantes entre el operador de la red social y sus usuarios, se trata de la única fuente directa en la que un potencial usuario puede basarse para dar un **consentimiento informado** respecto de los datos personales que se recaban, tal y como se requiere bajo la normativa europea. Por tanto, es esencial que las redes sociales publiquen dichos documentos de forma accesible tanto técnica como lingüísticamente.

En este sentido, nuestra Ley Orgánica de Protección de Datos (LOPD) en su artículo 6 dispone, en su apartado 1, que *"[e]l tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado*" y en su artículo 3.h) la LOPD define el consentimiento del interesado como "*toda manifestación de voluntad, libre, inequívoca, específica, informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*", de lo cual se desprende la necesaria concurrencia de los cuatro requisitos enumerados en dicho precepto para que el consentimiento pueda ser considerado conforme a derecho. Asimismo, así lo ha señalado la Audiencia Nacional en su Sentencia de 10 de mayo de 2007:

> *"El apartado h) del artículo 3 LOPD nos dice que el consentimiento del interesado es toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. De esta definición se desprende que es necesario que concurran cuatro requisitos para que el consentimiento sea válido a los efectos de legitimar un tratamiento de datos personales. En*

[92] CIS. Barómetro de Febrero de 2017. Pregunta 21h. Página 17.
[93] CIS. Barómetro de Febrero de 2017. Pregunta 21i. Página 17.
[94] Andrews, L. 2012. "*I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*". Nueva York: Free Press. Página 35.
[95] CIS. Barómetro de Febrero de 2017. Pregunta 21d. Página 16.
[96] CIS. Barómetro de Febrero de 2017. Pregunta 21e. Página 16.

> *primer lugar que el consentimiento se preste libremente lo que supone que el mismo ha de obtenerse libre de vicios del consentimiento en los términos regulados en el Código Civil (violencia, intimidación, error...). En segundo lugar que el consentimiento venga referido a una determinada operación de tratamiento y para una finalidad determinada y legítima del responsable del tratamiento. No son posibles los consentimientos genéricos o inespecíficos. En tercer lugar, el consentimiento ha de ser informado lo que significa que el afectado o interesado conoce que se va a realizar un tratamiento con sus datos y cuál va a ser el alcance de ese tratamiento. Esta información debe ser expresa, precisa e inequívoca en relación a la existencia del fichero o tratamiento, a la finalidad perseguida por la recogida de los datos y los destinatarios de la información, del carácter obligatorio o facultativo de las respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, así como de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Así lo expresa el artículo 5 al fijar el contenido del derecho de información en la recogida de datos. En cuarto lugar, el consentimiento ha de ser inequívoco lo que excluye el consentimiento presunto, aquel que debe deducirse de los actos realizados por el afectado."*

En cuanto a la necesidad de que el consentimiento sea específico, se puede citar el Dictamen 15/2011 del Grupo de Protección de Datos del artículo 29, sobre la definición de consentimiento, que contempla las condiciones generales de validez del consentimiento y determina, en cuanto a la necesidad de que el consentimiento se manifieste a través de una manifestación de voluntad específica, que:

> *"para ser válido, el consentimiento debe ser específico. En otras palabras, el consentimiento indiscriminado sin especificar la finalidad exacta del tratamiento no es admisible.*
> *Para ser específico, el consentimiento debe ser comprensible: referirse de manera clara y precisa al alcance y las consecuencias de tratamiento de datos. No puede referirse a un conjunto indefinido de actividades de tratamiento. Esto significa, en otras palabras, que el consentimiento se aplica en un contexto limitado*.
> *El consentimiento debe darse en relación con los diversos aspectos del tratamiento, claramente identificados. Esto implica saber cuáles son los datos y los motivos del tratamiento. Este conocimiento debería basarse en las expectativas razonables de las partes. Por tanto, el "consentimiento específico" está intrínsecamente relacionado con el hecho de que el consentimiento debe estar informado. Existe un requisito de precisión del consentimiento con respecto a los diferentes elementos del tratamiento de datos: no puede pretenderse que abarque "todos los fines legítimos" perseguidos por el responsable del tratamiento. El consentimiento debe referirse al tratamiento que es razonable y necesario en relación con la finalidad…"*

El consentimiento prestado requiere que la información sea expresa, precisa e inequívoca no sólo en relación con la existencia del fichero o tratamiento sino también en relación con la finalidad específica perseguida con la recogida de datos. El tratamiento de datos sin consentimiento de los afectados constituye un límite al

derecho fundamental a la protección de datos (Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000). Para que el consentimiento sea válido, por tanto, debe ser inequívoco, aparte de informado y específico, como ya se ha razonado, de forma que pueda considerarse que el interesado lo ha prestado de forma indubitada y sin haber sido o podido ser inducido a error. Con ello se asegura al afectado un efectivo poder sobre sus datos y se le garantiza la toma de decisiones acerca de su disposición[97].

La calidad de una política de privacidad no debe confundirse con la calidad de los estándares de protección de los datos personales que se implementen. Por el contrario, como herramienta para facilitar el consentimiento informado, una política de privacidad debe proporcionar toda la información relevante respecto de las prácticas de la red social sin perjuicio de que las mismas sean beneficiosas o perjudiciales para el usuario. En este sentido, una página web que exponga de forma abierta y clara un uso terrible de su recopilación de datos, el uso inapropiado que se hace de los mismos y su transmisión a terceros tendrá una mejor política de privacidad que una página web que ofrece un contenido ambiguo y sin mencionar condiciones esenciales como la transmisión o no de los datos recabados a terceros[98].

A continuación se procederá al análisis de las políticas de privacidad de las redes sociales seleccionadas, en particular estudiando los siguientes aspectos:

a) Su accesibilidad técnica: si la política de privacidad es accesible desde la página web principal de la red social en cuestión e incluso desde los dispositivos móviles a través de su App.
b) Su accesibilidad lingüística: aspectos como la extensión del documento en sí y los términos que se emplean en el mismo, pues una política excesivamente extensa o el uso de palabras ambiguas o complejas – ya sea técnica o legalmente – puede tener como objeto o, al menos como efecto, el disuadir al usuario de su completa lectura.
c) Su carácter legal: la política de privacidad debe verse como un contrato jurídico entre el operador de la red social y el usuario. Por ello, resulta esencial que la misma disponga de un contenido legal mínimo que regula la relación jurídica que se crea entre ambos. Por ejemplo, fecha, notificaciones, ley aplicable y jurisdicción, etc.
d) Su uso de los datos: uno de los aspectos más importantes a evaluar cuando se analiza una política de privacidad es la información que se transmite al usuario respecto del uso que se va a hacer de sus datos personales. Por ejemplo, una buena política de privacidad explicará claramente por cuánto tiempo se retienen los datos, si se transmiten a terceros y, en tal caso, a quién, cómo y con qué objeto.

En función de estos aspectos podremos determinar si las políticas de privacidad de las redes sociales objeto de este estudio, están a la altura de las garantías de los usuarios que busca salvaguardar la normativa de protección de datos.

[97] Agencia Española de Protección de Datos (AEPD). Procedimiento núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017.
[98] Op. Cit. (2009) "*The Privacy Jungle: On the Market for Data Protection in Social Networks.*" Universidad de Cambridge. Página 21.

IV.1. Facebook

Facebook es una de las redes sociales más populares en la red y, tanto es así, que su sitio web está posicionado como el número 3 a nivel global atendiendo al número de visitas diarias según el *ranking* de ALEXA[99]. Una empresa que al cierre del ejercicio 2016 sus ingresos se situaron en los 25.668 millones de euros, de los que 24.968 millones correspondieron sólo a sus ventas por publicidad, con un incremento del 57% respecto al año anterior[100]. En general, Facebook tiene una gran capacidad de agregar información de sus usuarios, desde sus "*likes*" a los artículos que leen a las páginas web que visitan. De hecho, Facebook ya ha sido criticado duramente por seguir rastreando las actividades de sus usuarios incluso una vez fuera de la red social[101].

La cantidad de información publicada por los usuarios en esta red social a través de sus "*likes*", fotos, enlaces a artículos y páginas, compartiendo su ubicación etc. les permite crear una "identidad de Facebook" donde esa versión virtual de ellos mismos refleja su historia personal y de su personalidad que se reducen a datos esenciales sobre los que los anunciantes encuentran tanto atractivo – edad, nivel de educación, estructura familiar, ubicación geográfica, preferencias de productos, inclinaciones políticas – mientras anulan información que no tiene valor comercial tales como los principios morales o patrones emocionales[102].

Dado el valor elevado de estos datos, Facebook ha podido continuar siendo un servicio gratuito utilizando la publicidad como fuente de ingresos. Sin embargo, la política de privacidad de Facebook y la forma en que recolecta y procesa los datos de sus usuarios históricamente ha enfurecido a los usuarios y sufrido duras críticas por los expertos en la materia[103].

Tal y como se aprecia en la **Imagen 2**[104]**,** en el caso de Facebook la política de privacidad se presenta en el momento de registro como un breve aviso legal con un tipo de letra de tamaño inferior y sin destacar que dice "*Al hacer clic en Terminado, aceptas nuestras Condiciones y reconoces haber leído nuestra* Política de datos*, incluido nuestro Uso de cookies. Es posible que recibas notificaciones de Facebook por SMS, pero puedes desactivarlas en cualquier momento";* apareciendo las palabras subrayadas en un color distinto, azul, y no en negrilla, y siendo enlaces a las páginas que contienen las condiciones de servicio, la política de privacidad, denominada "*Política de datos*", así como la denominada "*Uso de*

[99] ALEXA, Website Traffic, Statistics, and Analytics. Site info on Facebook.com [consultado el 1 de Septiembre de 2017] Disponible en: *https://www.alexa.com/siteinfo/facebook.com*

[100] EL MUNDO. [consultado el 1 de Septiembre de 2017] Disponible en: *http://www.elmundo.es/economia/2017/02/01/589266c622601d790e8b45b7.htmlhttp://www.elmundo.es/economia/2017/02/01/589266c622601d790e8b45b7.html*

[101] Hans, G.S. (2012) "Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era". *Michigan Telecommunications and Technology Law Review*, University of Michigan Law School. Vol. 19(1). Páginas 183-184.

[102] Op. Cit. (2012) "Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era". *Michigan Telecommunications and Technology Law Review*, University of Michigan Law School. Vol. 19(1). Página 184.

[103] Op. Cit. (2012) "Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era". *Michigan Telecommunications and Technology Law Review*, University of Michigan Law School. Vol. 19(1). Página 184.

[104] FACEBOOK. Página principal. [Consultado en Agosto de 2017]. Disponible en: "http://www.facebook.com"

cookies". Debajo de este párrafo, destacado y en un tipo de letra mucho mayor – tal y como se aprecia en la **Imagen 2** – aparece un botón en fondo verde etiquetado como "*Terminado*", sin que sea obligatorio acceder a la política de privacidad – "Política de Datos" – para continuar el proceso de registro[105]. No se exige que se marque una casilla de aceptación expresa para el uso de datos y, sin embargo, ya se considera desde el momento del registro que dicha política de privacidad es un acuerdo legal y vinculante entre el operador y el usuario por el que este último acepta que Facebook recolecte, procese y ceda a terceros sus datos, tal y como analizaremos en los siguientes sub-apartados.

Imagen 2 – Aceptación de la Política de Privacidad de Facebook en el momento de registro.

IV.1.1. Accesibilidad técnica

Es esencial que la política de privacidad esté en todo momento accesible para el usuario durante el uso de la red social, ya sea desde su ordenador personal o desde cualquier dispositivo móvil. En el caso de Facebook, en la **Imagen 3** se puede apreciar que desde la página principal – en este caso, desde el *News Feed* – se muestra un enlace a la política de privacidad, al igual que en el momento del registro, con letra pequeña y junto con otros avisos legales de forma casi desapercibida que, al fin y al cabo, únicamente resulta fácil de encontrar para el que lo busque y no siempre se encuentra visible, dependiendo de la actividad que realice el usuario en la misma ventana y de si se desplaza hacia arriba o abajo en la misma.

Aunque no aparece en el tipo de fuente azul que caracteriza a los hipervínculos, se trata de un enlace al documento legal que Facebook denomina "*Política de*

[105] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 59.

Datos". Ahora bien, en el momento de clicar en dicho enlace, no se abre una nueva ventana sino que interrumpe la actividad del usuario y eso podría conllevar a que el mismo desista, por inconveniente, de su lectura. Tampoco se ofrece en esta ventana actualizada donde se presenta al usuario la Política de Datos una versión imprimible o archivable para que el usuario pueda elegir proceder a su lectura en un momento posterior.

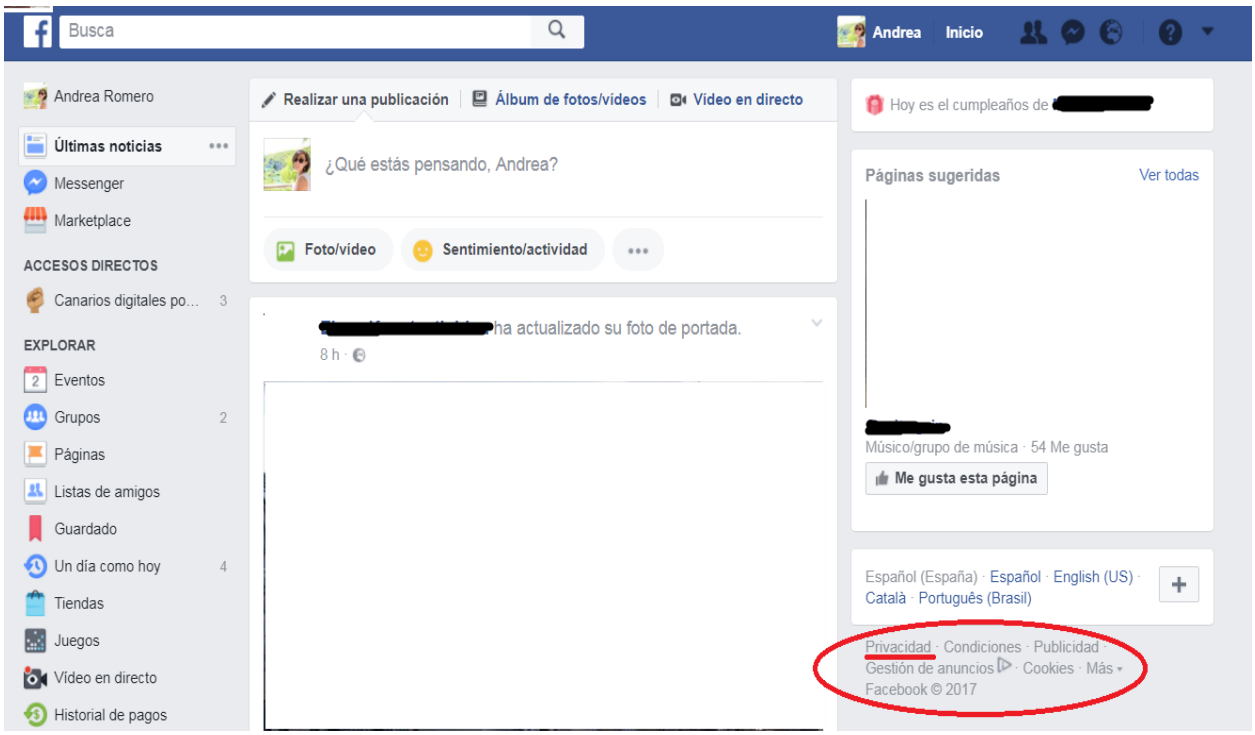


Imagen 3 – Accesibilidad Técnica a la Política de Privacidad de Facebook desde la Página Principal.

Por otro lado, en lo que se refiere a la accesibilidad desde los dispositivos desde su aplicación – "App" – para móviles veremos que Facebook no pone a disposición del usuario su política de privacidad de forma práctica. Tal y como muestra la **Figura 4**[106], son muchos los pasos que ha de realizar un usuario de Facebook en la aplicación para poder acceder a la misma.

En primer lugar, debe clicar sobre el icono de "Menú", y tras desplazarse a lo largo de las diferentes opciones que se le presentan (14 en total) antes de poder llegar a la sección de "CONFIGURACIÓN" – por lo que no aparece a primera vista para el usuario, sino que solo lo ve si continúa desplazándose hasta el final – entonces podrá acceder a "*Aspectos básicos de la privacidad*". En esta nueva ventana que se le aparece al usuario se le explica de forma gráfica aspectos básicos de cómo está configurada la privacidad de su cuenta aunque las imágenes aparecen cortadas y no parece estar configurado para el tamaño de una pantalla móvil. Incluso en esta ventana, no aparece todavía la opción para acceder a la política de datos, al menos no a simple vista.

El siguiente paso es acceder a un nuevo botón de "Menú" que inicialmente aparece oculto detrás de un aviso legal respecto al uso de las cookies y únicamente si el

[106] FACEBOOK APP. [Consultado en Septiembre de 2017].

usuario se desplaza hacia abajo se le aparecerá este botón que, si bien entonces está visible, aparece el texto superpuesto, mezclándose la palabra “menú” con “privacidad”, lo que nuevamente lleva a pensar que no esté este apartado de la aplicación bien adaptado para su uso desde el móvil. A estas alturas, se induce a error al usuario que podría pensar que el apartado de “*Aspectos básicos de la privacidad*” es todo cuanto necesita saber respecto de la privacidad de su cuenta puesto que realmente esta es la información que se le presta de forma relativamente accesible. Nada indica al usuario que el botón de Menú que aparece medio oculto sea la clave para acceder a la política de privacidad completa de Facebook, lo cual resulta ser, de hecho, lo que ocurre. Siendo este, finalmente, el último paso para poder acceder a la “Política de Datos” de Facebook desde la aplicación móvil que, ahora sí, remite a la página web principal de Facebook, de forma que contiene exactamente la misma información y formato que veíamos era accesible desde la página web. Sin embargo, esto significa que técnicamente la Política de Privacidad no está disponible para su lectura desde la aplicación móvil, siendo necesario la conexión a la misma a través del sitio web.

Figura 4 – Pasos para acceder a la Política de Datos de Facebook desde la aplicación del móvil (App).

Contamos, en definitiva, un total de 6 pasos, poco claros y nada intuitivos, a seguir desde el móvil para poder consultar la política de privacidad desde la aplicación de Facebook por lo que, no cabe duda de que sería impreciso describir la accesibilidad técnica en este caso de satisfactoria. Sería fácilmente mejorable con incluir un enlace directo a la Política de Datos – habilitando su lectura desde la aplicación y sin necesidad de acudir al sitio web – desde que el usuario accede al Menú principal.

En definitiva, la accesibilidad técnica de la página web se podría mejorar sencillamente habilitando que el enlace se redirija a una nueva ventana sin interrumpir la actividad del usuario y, desde el dispositivo móvil, haciendo que se pueda acceder a la Política de Datos a través del Menú principal y directamente desde la aplicación.

IV.1.2. Accesibilidad lingüística

En el caso de la accesibilidad lingüística de la política de privacidad de Facebook llama la atención en primer lugar el término "*Política de Datos*" que se le ha otorgado a la misma, evitando identificar correctamente lo que se debería titular como "Política de Privacidad" o de "Protección de Datos Personales"[107].

En lo que respecta a la extensión de la Política de Datos, en total cuenta con 2.990 palabras, lo cual constituye una extensión razonable que, añadido a la forma de presentación de la misma, contribuye a hacer su accesibilidad lingüística óptima de forma que el usuario no se sienta abrumado por la extensión de la misma. Además, desde el primer momento en que se accede a la Política de Datos se presenta al lector con la información distribuida en un formato muy claro y sencillo de seguir, distribuido en distintos apartado de preguntas - *¿Qué tipo de información recopilamos? / ¿Cómo utilizamos esta información? / ¿Cómo se comparte esta información? / ¿Cómo puedo administrar o eliminar información sobre mí? / ¿Cómo respondemos a requerimientos legales o evitamos que se produzcan daños?* – entre otras categorías adicionales de información. Inicialmente parece que el lenguaje que se emplea es sencillo, sin emplear términos técnicos o legales complejos que puedan impedir la correcta comprensión por parte del usuario del mensaje que se le transmite, independientemente de la formación o edad del mismo.

Sin embargo, al continuar con una lectura en profundidad de la política de privacidad se puede observar el uso de términos ambiguos y poco claros, empleándose ejemplos pero sin enumerar una lista de los datos efectivamente recogidos. Así, indican: "*Recopilamos información sobre las personas y los grupos a los que estás conectado y cómo interactúas con ellos […]*" o "*Recopilamos información cuando visitas o utilizas sitios web*" o "*Utilizamos la información de la que disponemos para mejorar nuestros sistemas de publicidad […]*" pero en ningún momento se enumera con precisión qué información se recoge o con qué finalidad.

Con todo ello, en cuanto al método lingüístico y la presentación se refiere, resulta muy efectiva la forma en que Facebook ha logrado presentar la información,

[107] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Páginas 78-79.

facilitando la lectura del usuario y contribuyendo a hacer accesible la Política de Datos a sus usuarios pero las expresiones empleadas únicamente logran crear un contexto de falsa sensación de información con términos vacíos de contenido, imprecisos en cuanto que su lectura no lleva al lector a conocer de forma inequívoca los datos que se recogen ni el uso que se da a los mismos.

IV.1.3. Aspectos Legales

Es esencial la valoración de la política de privacidad pues este es, al fin y al cabo, el acuerdo jurídico por el que el usuario se informa y consiente al uso que va a hacer el operador de la red social de su información personal y, para que dicho consentimiento sea indiscutiblemente válido, resulta indispensable que la política contenga los requisitos mínimos para hacer vinculante y eficaz un contrato de esta naturaleza.

En el caso de la Política de Datos de Facebook no se ofrece una fecha contractual en el momento del registro aunque sí se indica la fecha de actualización. Resulta sorprendente, no obstante, que no se otorgue acceso a las actualizaciones anteriores.

Más positivo resulta, en cambio, la política de notificaciones que se incluye en la Política de Datos – ver **Imagen 4**[108] –, según la cual Facebook se compromete a notificar al usuario de cualquier actualización de las condiciones dando tiempo suficiente al usuario para consultar la misma e, incluso, hacer comentarios antes de decidirse a continuar disfrutando de los servicios.

Imagen 4 – Notificación de Cambios en la Política de Datos de Facebook.

Asimismo, como marco legal debería establecerse en la Política de Datos claramente cuál es la Ley Aplicable y Jurisdicción, con más razón teniendo en consideración el contexto global que caracteriza al mundo digital que es Internet, en general, y el alcance mundial que tiene Facebook, en particular. Luego cobra especial relevancia este aspecto legal si se tiene en cuenta la discrepancia que existe en la mayoría de los casos entre la ubicación geográfica del domicilio social del operador y el domicilio del usuario, así como el lugar donde efectivamente se lleva a cabo el procesamiento de los datos.

[108] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"

Imagen 5 - Referencia al Privacy Shield.

Facebook no se pronuncia al respecto de la ley aplicable o resolución de conflictos en la Política de Datos pero sí encontramos al margen de la misma página de la Política de Datos un enlace con información adicional – "*Más Recursos*" tal y como se aprecia en la **Imagen 5**[109] – en donde se hace referencia al Escudo de la Privacidad Unión Europea-Estados Unidos. Al seguir dicho enlace y visitando la página web oficial de Privacy Shield podemos comprobar que Facebook está incluido dentro del listado del *EU-US and Swiss-US Privacy Shield Frameworks*[110].

Después de que el Tribunal Europeo de Justicia derogase el 6 de octubre de 2015 el conocido como el acuerdo Safe Harbor[111], se redactó rápidamente el denominado "Privacy Shield" para evitar, en palabras del presidente de la Cámara de Comercio de EE.UU. en España, "*una gran inseguridad jurídica en el ámbito de transferencia de datos entre los principales bloques de comercio a nivel mundial*". El Privacy Shield, por tanto, busca garantizar la transferencia de datos conforme a las exigencias del RGPD y a partir del mismo, pone a disposición de las empresas de la Unión Europea una serie de recursos como un sistema de arbitraje paritario, gratuito para las empresas miembros del nuevo acuerdo en el que las reclamaciones podrán efectuare en la lengua propia del que las realiza y los afectados dispondrán de acciones eficaces y prácticas cuando consideren que sus derechos han sido vulnerados entre otros aspectos[112].

FACEBOOK INC. Y EL ESCUDO DE LA PRIVACIDAD UNIÓN EUROPEA-ESTADOS UNIDOS

Facebook Inc. ("Facebook") ha obtenido la certificación del marco Escudo de la privacidad Unión Europea-Estados Unidos emitida por el Departamento de Comercio de Estados Unidos en lo que concierne a la recopilación y el procesamiento de datos personales de nuestros anunciantes, clientes o socios comerciales en la Unión Europea ("Socios"), con relación a los productos y servicios descritos en la sección "Alcance" incluida más adelante y en nuestra certificación. Para obtener más información sobre el programa Escudo de la privacidad, visita www.privacyshield.gov.

Imagen 6 – Extracto tras seguir el enlace "*Aviso sobre el Escudo de la privacidad Unión Europea–Estados Unidos*".

Ahora bien, tal y como se observa en la **Imagen 6**, la adhesión al Privacy Shield que consta en la página web de Facebook está referida a la información que

[109] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation

[110] Privacy Shield Framework. [Consultado el: 3 de septiembre de 2017]. Disponible en: *https://www.privacyshield.gov/participant_search*

[111] Tribunal de Justicia de la Unión Europea. Petición de decisión prejudicial planteada por la High Court (Irlanda). Caso Maximillian Schrems y Data Protection Commissioner (C-362/14). Sentencia de 6 Octubre 2015.

[112] Cámara de Comercio de EE.UU. en España. 2016. "*Privacy Shield y el impacto de la privacidad y la ciberseguridad en las relaciones transatlánticas*".

intercambia con sus "Socios", no la relativa a los datos personales de los usuarios de la red social y ello únicamente se descubre si se sigue el enlace que aparece en la **Imagen 5**, lo cual podría llevar erróneamente al usuario a considerar que la transferencia de datos está garantizada por el Privacy Shield sin ser ello cierto. No quedando de ninguna otra manera expresada en la política de privacidad de Facebook la ley aplicable o resolución de conflictos en relación con los datos del usuario.

Asimismo, tampoco es determinante la política de privacidad de Facebook respecto del período de retención indicando únicamente que la información se almacenará el tiempo suficiente para proporcionar los productos y servicios, y aquellos necesarios para cumplir con los requerimientos legales[113].

Finalmente, se indica en la Política de Datos los datos de contacto por los que cualquier usuario se puede poner en contacto con Facebook para hacer llegar sus dudas. En este sentido, se incluye el correo postal y, a falta de un correo electrónico, se habilita un enlace para ponerse en contacto a través de Internet, tal y como se muestra en la **Imagen 7**[114].

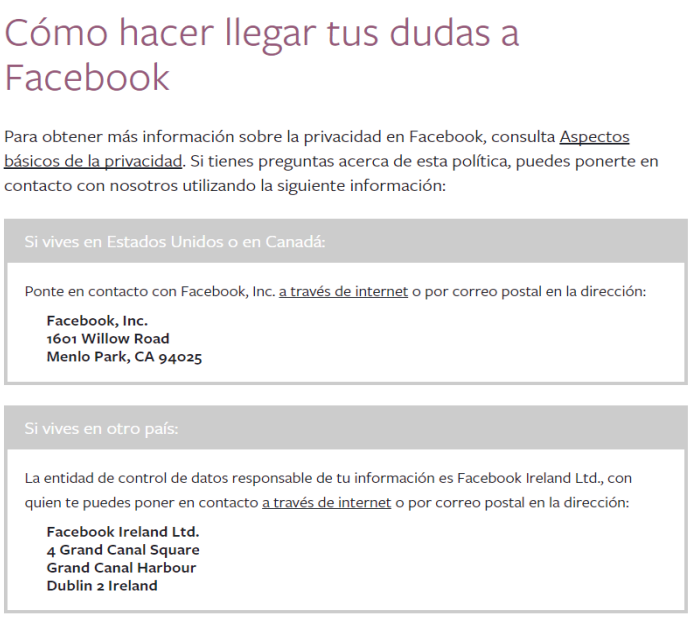


Imagen 7 – Apartado "*Cómo hacer llegar tus dudas a Facebook*" en la Política de Datos de Facebook.

Un buen canal de comunicación y consultas podría salvar muchos obstáculos o carencias en la política de privacidad que pudieran surgir al hacer uso de la red social. Sin embargo, no es la posición del usuario el indagar a fondo para conocer toda la información sino que la normativa de protección de datos personales establece que corresponde al responsable o titular del fichero de datos el deber de informar debidamente a los afectados en el momento de obtener un consentimiento válido de los mismos.

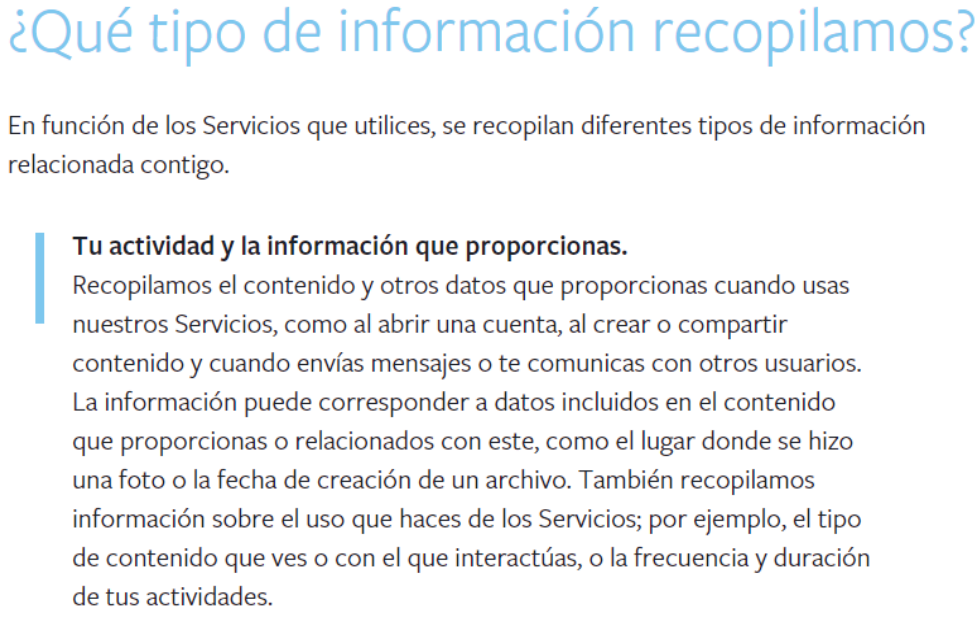
IV.1.4. Uso de los datos

Respecto del uso de los datos, Facebook dedica en su Política de Datos los dos primeros apartados – *¿Qué tipo de información recopilamos?* y *¿Cómo utilizamos esta información?* – para definir los datos que se recolectan a través de la actividad de sus usuarios y el fin de los mismos. Como ya hemos observado en el apartado IV.1.2. (Accesibilidad Lingüística) la forma de presentar las condiciones facilita en

[113] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 49.
[114] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"

gran medida la lectura de estas condiciones por parte del usuario. Ahora bien, en su Política de Datos, Facebook clasifica en diferentes sub-apartados el tipo de información que recolecta seguido de una breve descripción, complementado en cada caso con ejemplos de forma general y sin enumerar una lista de los datos recogidos lo que impide una presentación completa y exacta de la información recabada.

En el primer apartado dentro de "*¿Qué tipo de información recopilamos?"* Facebook hace referencia a los diferentes tipos de información que recopilan sobre cada usuario pero, como hemos visto, en ningún momento enumera una lista de datos y se limita a dar unos ejemplos, es el caso que vemos en la **Imagen 8**[115] como menciona que se recaban los datos al "*abrir una cuenta, al crear o compartir contenido y cuando envías mensajes o te comunicas con otros usuarios*" pero no enumera exactamente qué datos son los que han recabado en estos caso que muestra como ejemplo, así, por ejemplo, no sabe el usuario exactamente la información que ha proporcionado al registrarse – "*abrir una cuenta*" – ni se menciona que también se recaban otros datos a través de la red social como es el alarmante caso del perfil del usuario que durante su configuración en el apartado "*Información básica y de contacto*" existe la posibilidad de indicar en el campo de "*Intereses*" valores que permiten discriminar en función de creencias religiosas, ideologías políticas, vida sexual o salud, todos ellos considerados datos especialmente protegidos. Sin embargo no se mencionan en la política de privacidad y en ningún momento durante la configuración del perfil al seleccionar dichos "intereses" se establece un régimen de preferencias de publicación especial – siendo por defecto Amigos-de-Amigos – ni se solicita el consentimiento a priori y expreso para utilizar dicha información o se informa de la finalidad con que se puede utilizar en su tratamiento, sino que – también por defecto – se tratan todos los datos personales para mostrar anuncios. No se señala en ningún momento en la política de privacidad de Facebook – sin necesidad de navegar más



¿Qué tipo de información recopilamos?

En función de los Servicios que utilices, se recopilan diferentes tipos de información relacionada contigo.

Tu actividad y la información que proporcionas.
Recopilamos el contenido y otros datos que proporcionas cuando usas nuestros Servicios, como al abrir una cuenta, al crear o compartir contenido y cuando envías mensajes o te comunicas con otros usuarios. La información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con este, como el lugar donde se hizo una foto o la fecha de creación de un archivo. También recopilamos información sobre el uso que haces de los Servicios; por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y duración de tus actividades.

Imagen 8 – Extracto del apartado *¿Qué tipo de información recopilamos?*

[115] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"

profundamente en el conjunto de enlaces que se proporcionan – que se recogen datos especialmente protegidos ni se recaba consentimiento expreso para tratar datos especialmente protegidos[116].

Ahora bien, a pesar de que la forma en que se explica la información que se recolecta desde la red social es ordenada y clara, no es completa y resultan alarmantes ciertos datos que Facebook puede recolectar a través del uso de su red social. En este sentido, Facebook reconoce que recopila datos sobre los datos de pago cuando se efectúan transacciones desde su plataforma, y ello incluye el número de la tarjeta de débito o crédito y "*otra información sobre la tarjeta, así como otros datos sobre la cuenta y sobre autenticación*".

Igualmente preocupante es el hecho de que Facebook recopila información de "*socios externos*", lo que en la práctica conlleva que podrán seguir rastreando tu actividad aunque no sea dentro de la red social – "*dentro y fuera de Facebook*" – tal y como se observa en la **Imagen 9**[117].

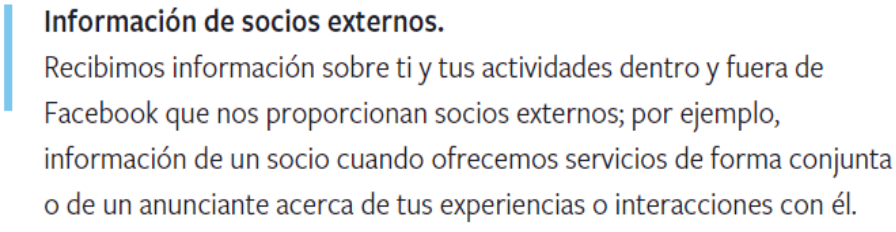


Imagen 9 – Información sobre socios externos.

Al respecto de la recopilación de datos fuera de la red social, resulta especialmente relevante una sentencia reciente en los Tribunales de California al respecto que ha resuelto que no hay violación del derecho a la intimidad de los usuarios por este seguimiento de sus actividades al no haberse probado que tuvieran los usuarios una expectativa de privacidad razonable o que hubiesen sufrido ningún daño o pérdida realista. Ello choca de frente con la interpretación que hace la AEPD de la recopilación de datos que hace Facebook en páginas web de terceros resolviendo que "*los usuarios no son informados de que se tratará su información, mediante el uso de cookies, algunos de uso específico publicitario y alguna de uso secreto, cuando navegan por páginas que no son páginas de FACEBOOK (páginas de terceros) y que contienen el botón "Me gusta". Que esto se produce incluso cuando los usuarios no están registrados en FACEBOOK, pero han visitado alguna vez una de sus páginas. Que también ocurre en usuarios registrados pero que navegan por páginas de terceros, incluso si no tienen sesión iniciada en FACEBOOK, añadiendo la información recogida de dichas páginas a la asociada a su cuenta de FACEBOOOK"*[118].

[116] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 29.
[117] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"
[118] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 78.

A pesar de considerarse la recopilación de estos datos significativamente preocupantes desde el punto de vista del usuario, lo cierto es que Facebook no es completamente transparente al respecto y, tal y como hemos analizado en el Apartado III.1.5. (Transparencia), la transparencia se refiere a la capacidad del usuario de estar informado respecto de las prácticas de procesamiento y divulgación y de entender las implicaciones del flujo de la información personal dentro de las redes sociales para poder conocer y distinguir los límites que garantizan la integridad contextual de los datos personales[119]. De forma que es preferible una Política de Datos escandalosamente verdadera y exacta por medio de la cual el usuario puede alcanzar a comprender el impacto de su consentimiento al uso de sus datos a una que oculta la información que realmente recopila de su red social.

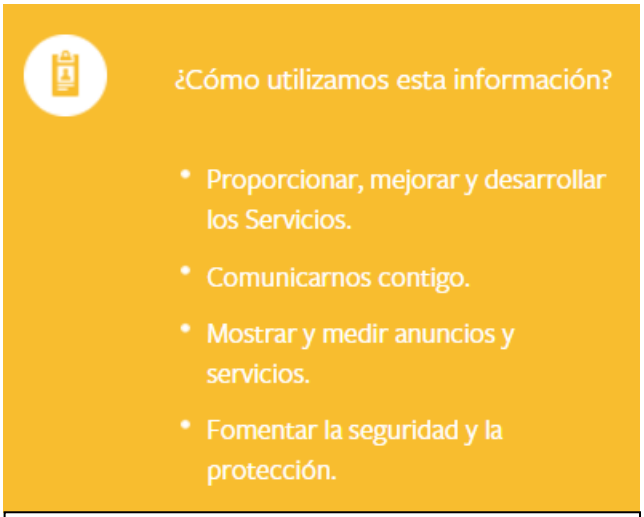


Imagen 10 – Cómo utilizan la información en Facebook.

En lo que respecta al cómo utilizan la información que recopilan, en la Política de Datos Facebook clasifica cuatro fines, tal y como se muestra en la **Imagen 10**[120]. En dichos apartados se incluyen enlaces relevantes para complementar la información pero lo esencial es que, de nuevo, a pesar de que Facebook trata de ser transparente respecto de sus usos no se enumera la correspondiente lista de qué datos son recogidos y se limita a dar algunos ejemplos[121].

Principalmente llama la atención que dediquen un apartado completo para explicar cómo emplean los datos recabados para "*mostrar y medir anuncios*", indicando al lector que no comparten "*información mediante la que se te [al usuario] puede identificar […] con socios de publicidad, medición ni análisis, a menos que nos des permiso para ello*" pero sin precisar cómo y cuándo se recaba dicho consentimiento. También se pone a disposición del usuario un enlace desde el que se le permite ajustar sus preferencias de los anuncios pero esta herramienta únicamente permite controlar los anuncios que se ven fuera de Facebook y otros dispositivos – tal y como se aprecia en la **Imagen 11**[122] – pero no evita que continúen apareciendo anuncios en la red social o que continúen recopilando datos. Se despliegan, por tanto, tres opciones que por defecto – en la **Imagen 11** aparecen ya configurados por el usuario – están activadas con "*Sí*" o para compartir con "*Mis amigos*". Se hace notar en la **Imagen 11** que en el segundo sector de la configuración el texto explicativo aparece – sin ningún motivo – en inglés, lo que

[119] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Páginas 19-20.
[120] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"
[121] Agencia Española de Protección de Datos (AEPD). Procedimiento N`PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Páginas 16,30 y 62.
[122] FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"

sin duda limita, a su vez, la total comprensión de un usuario medio que no tiene por qué conocer dicha lengua, las consecuencias e implicaciones que pueda tener desactivar o no esa opción en concreto.

Imagen 11 – Configuración de anuncios en página web de Facebook.

En consecuencia, se crea una apariencia de control y, en cierta medida, sí se le ofrece información y capacidad para ajustar las preferencias del usuario pero podría ser mucho más precisa. Las opciones de configuración que se ponen a disposición del usuario permiten que Facebook no muestre anuncios basados en su perfil, pero esto no implica que Facebook no recoja ni trate la información para crear un perfil asociado al usuario y que conserve de forma indefinida[123].

IV.1.5. Resumen

Teniendo en cuenta lo dispuesto en los apartados anteriores, tal y como ha quedado acreditado, a través de su actual política de privacidad, Facebook no ha recabado un consentimiento inequívoco y la misma induce a error acerca del tratamiento en un usuario con un conocimiento medio de las nuevas tecnologías.

En lo que se refiere a la accesibilidad técnica de la Política de Datos desde la página web de Facebook, no se habilita el enlace de forma que redirija a la política de privacidad de una forma más visible y que conduzca a una nueva ventana sin interrumpir la actividad del usuario. Mientras que, desde el dispositivo móvil, se podría configurar el acceso a la misma a través del Menú principal y directamente desde la aplicación sin necesidad de redirigirse a un navegador web, evitando los búsquedas innecesarias de una sección a otra y asegurando que la lectura sea compatible con el dispositivo de que se trata. Se incluyen, además, enlaces a información adicional, de forma que no se presenta al usuario con toda la información de una lectura de la política de privacidad sin necesidad de navegar más profundamente en el conjunto de enlaces que se proporcionan.

Asimismo, ya hemos visto que a la hora de registrarse en Facebook proporcionando los datos personales básicos, el botón sobre el que hay que

[123] Agencia Española de Protección de Datos (AEPD). Procedimiento N`PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 29.

presionar se ha denominado "*Terminado*", y no se obliga en ningún momento al nuevo usuario a leer las condiciones de uso a pesar de que existen medios fácilmente configurables como que se abra una ventana emergente con la política de privacidad donde hacer clic en "*Aceptar*" tras su efectiva lectura, lo cual sería una forma de registrar la aceptación sin dejar lugar a duda. Presentar un enlace en el momento de registro cuya consulta no es obligada y no impide continuar con el proceso de alta de un usuario nuevo y que la obtención del consentimiento informado se lleve a cabo con un simple *clic* en el recuadro de "*Terminado*" no es suficiente para que el consentimiento sea válido, en tanto que informado y específico.[124]

Desde la perspectiva de accesibilidad lingüística, en cuanto a la presentación se refiere, resulta muy efectiva la forma en que Facebook ha logrado mostrar la información, facilitando la lectura del usuario y contribuyendo a hacer accesible la Política de Datos a sus usuarios pero las expresiones empleadas únicamente logran crear un contexto de falsa sensación de información con términos vacíos de contenido, imprecisos en cuanto que su lectura no lleva al lector a conocer de forma inequívoca los datos que se recogen ni el uso que se da a los mismos. El usuario de Facebook no llega a ser consciente de la recogida de sus datos, de su almacenamiento o posterior tratamiento ni tampoco de las finalidades a las que se destinarán dichos datos.

En lo que se refiere a los aspectos legales de la Política de Datos, Facebook claramente suspende al no aportar datos especialmente relevantes como la ubicación de los servidores, la ley aplicable y jurisdicción, fecha vinculante o el período por el que se almacenan los datos.

Finalmente, en cuanto al uso que se hace de los datos, la Política de Datos de Facebook contiene referencias a una serie de finalidades caracterizadas por su imprecisión, sin especificar los servicios y datos personales que se asocian a las mismas, a través de términos inconcretos de los que no cabe deducir, sin duda o equivocación, la finalidad para la cual van a ser tratados los datos, lo que impide que el interesado pueda conocer a qué uso se están destinando o poder oponerse a esos usos. Estamos ante una política de privacidad indeterminada considerando las expresiones genéricas y poco claras que se emplean.

En definitiva, la política de privacidad debería representar una herramienta para obtener un consentimiento válido del afectado y para ello se requiere que se trate de un consentimiento inequívoco, de modo que sea evidente sin que admita duda o equivocación, y que permita al usuario ejercer un control efectivo sobre sus datos, garantizando con ello su poder de disposición respecto de los mismos. En este sentido la Política de Datos de Facebook no cumple las exigencias mínimas requeridas por la normativa de protección de datos para garantizar la privacidad de sus usuarios.

[124] Agencia Española de Protección de Datos (AEPD). Procedimiento Núm. PS/00082/2017. Inspección de oficio de la AEPD ante la red social de FACEBOOK. 2017. Página 81-83.

IV.2. WhatsApp

WhatsApp es en España la segunda red social más usada después de Facebook, principalmente por usuarios de entre 16 y 30 años y es considerada la red social más valorada – con una puntuación de 8,3 – liderando también en frecuencia de uso, con aproximadamente 5 horas de uso al día de promedio[125]. Por todo ello, WhatsApp se considera actualmente la red social preferida por los usuarios[126].

Tras su lanzamiento inicial en 2009, WhatsApp fue adquirido por Facebook en 2014 pero no sin estar en el punto de mira de la Comisión Europea que terminó por imponer una multa a Facebook de 110 millones de euros (122 millones de dólares). El motivo de esta multa fue porque, contrariamente a lo que había declarado Facebook en el momento de la compra, se había habilitado en 2016 la posibilidad de vincular técnica y automáticamente los datos existentes entre usuarios de Facebook y WhatsApp[127].

Asimismo, la forma en que se actualizó la política de privacidad de WhatsApp en el año 2016 para habilitar que los datos recopilados de sus usuarios fuesen compartidos con las empresas de Facebook tampoco estuvo libre de debate al venir una casilla pre-marcada autorizando dicha transferencia de datos, tal y como se muestra en la **Imagen 12**[128].

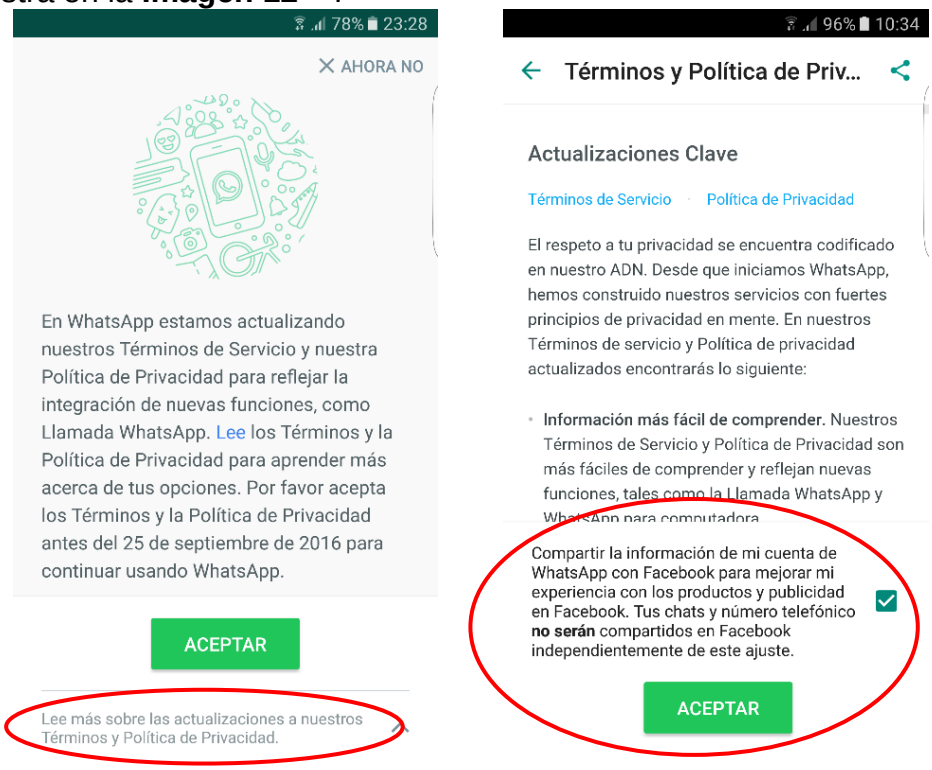


Imagen 12 – Actualización Política de Privacidad de WhatsApp en 2016.

[125] Estudio Anual Redes Sociales. (2017). Páginas 21-28.
[126] Estudio Anual Redes Sociales. (2017). Páginas 56.
[127] REUTERS. http://www.reuters.com/article/us-eu-facebook-antitrust/eu-fines-facebook-110-million-euros-over-whatsapp-deal-idUSKCN18E0LA . Consultado el 6 de Septiembre de 2017.
[128] BLOG Samuel Parra. "La casilla premarcada de Whatsapp para ceder datos a Facebook es legal". [Consultado el: 27 de septiembre de 2017]. Disponible en:

Sin embargo, la Agencia Española de Protección de Datos ha resuelto recientemente que el empleo de dicha casilla es conforme con la normativa de protección de datos como mecanismo de obtención de consentimiento por parte de los usuarios de WhatsApp[129]. En este sentido, establece en dicha Resolución que el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD)[130] únicamente prohíbe el uso de casilla pre-marcadas "*durante el proceso de formación de una contrato*", y dado que esta opción sólo aparecía en los términos de uso de usuarios que ya tenían instalada la aplicación (no para nuevos registros), considera la AEPD que el hecho no se ajusta a los presupuestos del artículo 15 del RLOPD.

En definitiva, WhatsApp, además de haberla actualizado en 2016, ha mantenido su política de privacidad en lugar de adoptar la propia de Facebook tras la operación de compraventa. Así, tal y como se muestra en la **Imagen 13**[131], la Política de Privacidad de WhatsApp se presenta al usuario – a través de un enlace – y se da por aceptada en el momento de descarga de la aplicación. Sin exigirse en ningún momento que se marque expresamente una casilla, que se haya leído la Política de Privacidad o, al menos, requerir que se acceda a la misma antes de darla por aceptada y considerarse un acuerdo vinculante entre usuario y operador.

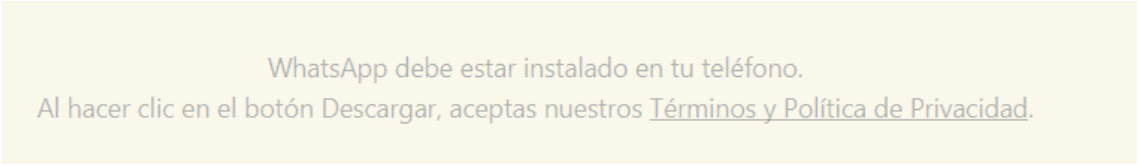


Imagen 13 – Momento de Aceptación de la Política de Privacidad de WhatsApp.

IV.2.1. Accesibilidad Técnica

Dado que WhatsApp es una red social a la que se accede principalmente desde los dispositivos móviles inteligentes – *smartphones* – vamos a comenzar el análisis de su accesibilidad técnica desde la App. Tal y como se nos muestra en la **Figura 5**, son cuatro en total los pasos que hay que dar para acceder a la Política de Privacidad de WhatsApp desde su aplicación móvil. En primer lugar, se accede al apartado de "*Configuración*" donde se le muestra al usuario en una única pantalla (no hay necesidad de desplazarse) un total de ocho sub-apartados a los que acceder. El siguiente paso es acceder específicamente al sub-apartado relativo a "*Ayuda*", lo cual puede resultar poco intuitivo dado que tal apartado se suele asociar más a una sección relativa a problemas técnicos que pueda sufrir un usuario en el uso de la aplicación, si bien es cierto que aparece el signo comúnmente conocido de "*información*". A continuación, aparecen cuatro secciones entre las cuales aparece la de "*Términos y Privacidad*" a la que puede acceder el usuario y a partir de la cual se le presenta un enlace directo a la Política de Privacidad pero que se

https://www.samuelparra.com/2017/09/04/la-casilla-premarcada-de-whatsapp-para-ceder-datos-a-facebook-es-legal/

[129] Agencia Española de Protección de Datos. Expediente Núm. E/04948/2016. Resolución de archivo de actuaciones.

[130] Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, aprobado por Real Decreto 1720/2008 (RLOPD).

[131] WHATSAPP. Página Principal. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com

abre en una ventana nueva en el navegador en lugar de estar disponible directamente desde la App.

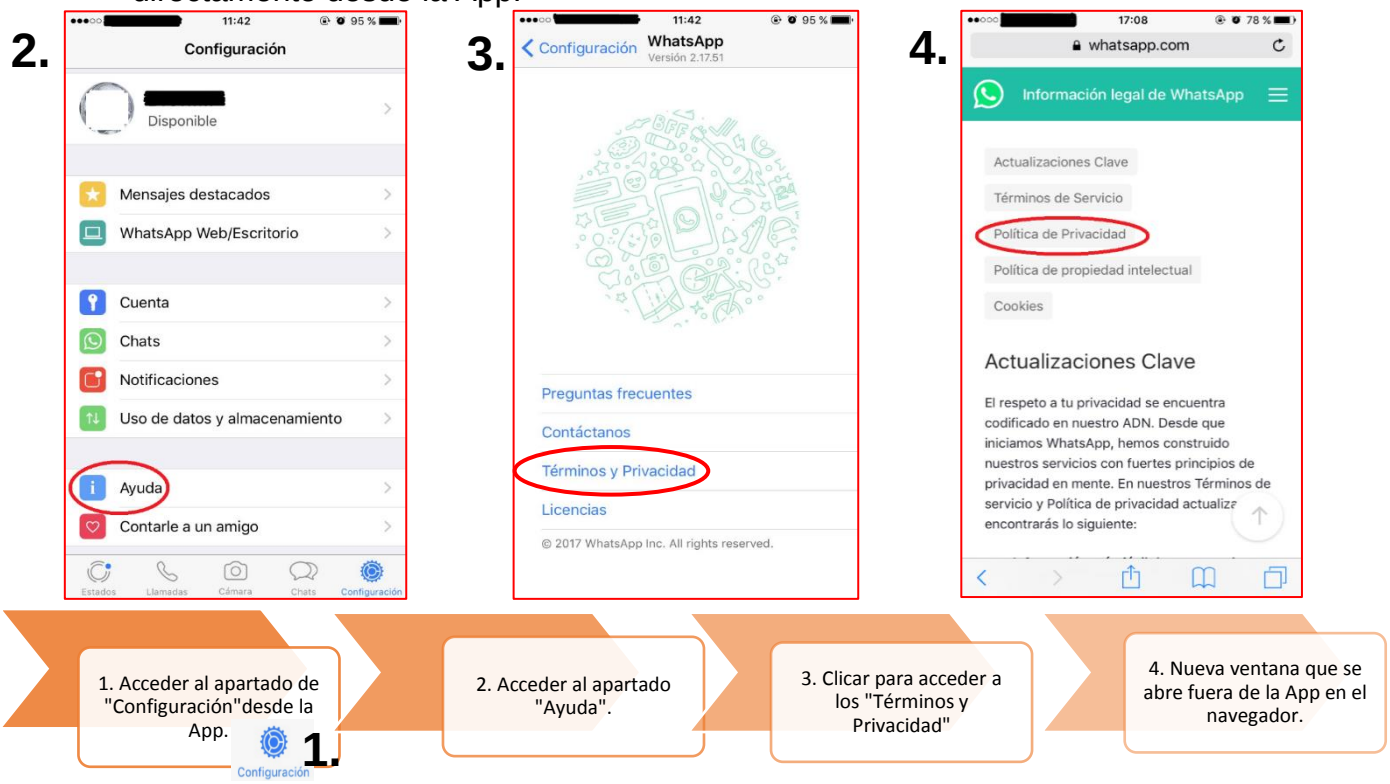


Figura 5 – Pasos para acceder a la Política de Privacidad de WhatsApp desde la App.

De forma que, estrictamente hablando, aunque se puede terminar accediendo a la Política de Privacidad a través de la App, no podemos decir que la misma esté técnicamente disponible dentro de la misma, siendo necesario tener acceso a la red y que se abra la nueva ventana en el navegador para poder acceder a la misma.

Una vez accedemos a la Política de Privacidad de WhatsApp, estamos ante la misma ventana a la que accederíamos desde el sitio web de WhatsApp. Ahora bien, para acceder a ella desde la página principal en el navegador – esto es, sin

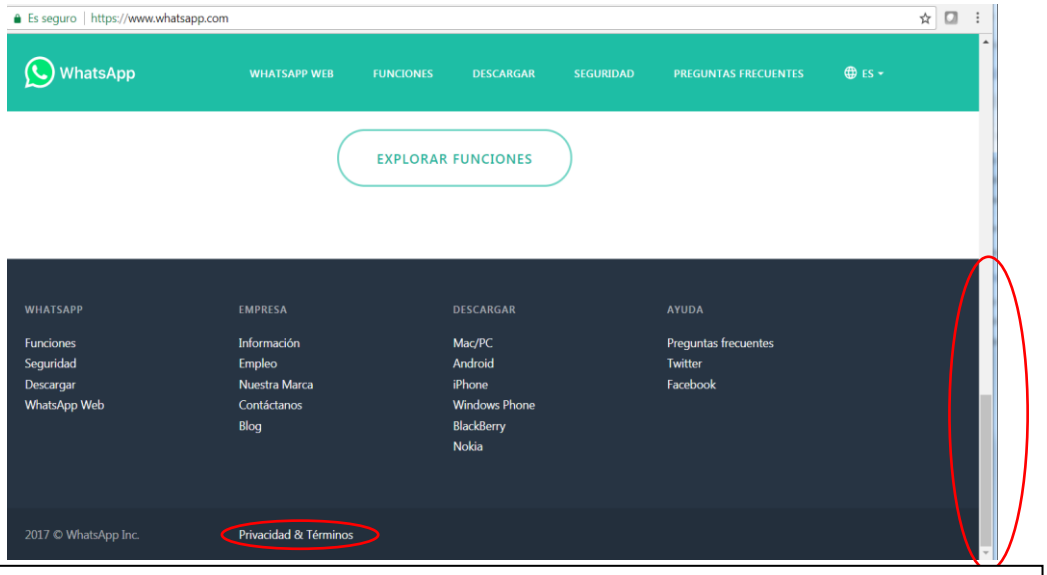


Imagen 14 – Accesibilidad Técnica desde la página principal de WhatsApp.

ser redirigido desde la App –, el usuario debe desplazarse hasta el final de la ventana para que, finalmente, aparezca un enlace a la "*Privacidad y Términos*" de WhatsApp. De forma que no está siempre accesible al usuario – sólo aparece si llega hasta el final de la ventana, tal y como muestra la **Imagen 14**[132] – y, en caso de que se acceda al enlace, no se abre en una ventana nueva sino que interrumpe cualquier otra actividad del usuario en la página principal.

Tanto desde la App como desde la página principal, la ventana que se abre es la de "*Información Legal*", por lo que no se encuentra disponible un documento específico para la Política de Privacidad, apareciendo ésta como un apartado dentro del marco global de aspectos legales que se despliega en la ventana, tal y como se muestra en la **Imagen 15**[133]. Además, no solo no se ofrece en ningún momento la opción de archivar, descargar o imprimir la Política de Privacidad – o cualquier otra sección – sino que, además, al imprimir directamente desde la página web las páginas aparecen cortadas, no siendo legibles las cláusulas al completo en papel impreso.[134]

Imagen 15 – Información Legal de WhatsApp.

Por lo que no podemos concluir que la Política de Privacidad, en este caso, esté fácilmente accesible para el usuario desde la App o la página principal del sitio web. Como aspectos a mejorar debe señalarse que podría incluirse un apartado específico dentro de sección de "*Configuración*" de la App desde donde el usuario pueda leer la Política de Privacidad en cualquier momento y sin necesidad de acudir a demasiados sub-apartados ni al navegador y, desde la página principal, habilitar el enlace para que esté visible en todo momento, que se abra en una nueva ventana y que ofrezca al usuario la posibilidad de descargar una copia de la Política de Privacidad.

IV.2.2. Accesibilidad Lingüística

Si nos centramos únicamente en el apartado de "Política de Privacidad" dentro del marco de "Información Legal" que ofrece WhatsApp al acceder al enlace "Privacidad y Términos" – tal y como hemos observado en el apartado anterior –

[132] WHATSAPP. Página Principal. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com
[133] WHATSAPP. Página Principal. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com
[134] WHATSAPP. Página Principal. *Información Legal*. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com

se puede apreciar que se ofrece al lector una estructura bien organizada y accesible por medio de enlaces a los distintos sub-apartados que se muestran en la **Imagen 15**, sin embargo, dicha estructura organizada se enmarca dentro del marco de "Información Legal" en lugar de ponerse a disposición del usuario un documento específico para la política de privacidad.

Por otro lado, nos encontramos en seguida con el uso de frases superfluas en la política de privacidad que nada aportan desde una perspectiva legal. Es el caso de la primera frase en el apartado que nos interesa: "*El respeto a tu privacidad forma parte de nuestro ADN*"[135]. Este es un claro ejemplo del uso de un lenguaje que, sin duda, busca crear apariencia de seriedad a pesar de que ya hemos visto que lo realmente importante en la accesibilidad lingüística y, en general, en la naturaleza misma de una política de privacidad no son los estándares de la empresa respecto de lo que ellos entienden por privacidad sino el contenido e información que logran transmitir al usuario a través de ella respecto del uso que se hace de sus datos. Asimismo, al igual que ocurría en el caso de Facebook, a lo largo de la política de privacidad se emplean expresiones como "*Recopilamos información relacionada con el rendimiento, diagnóstico y servicio*" o "*Recopilamos información sobre tus cambios de mensaje de estado*" y "*podemos recibir información*", pero sin especificar en ningún momento un listado concreto de qué datos se están recabando ni cuál es el uso que se les va a dar.

Es preferible una política de datos transparente – aunque la información que exponga sea alarmante – que una que emplea un texto ambiguo y confuso que omite la información verdaderamente relevante[136] y, por ello, el uso de frases como las anteriormente citadas debería evitarse en este tipo de políticas. Además, son esta clase de expresiones las que contribuyen a crear una falsa percepción de seguridad y que ponen en duda si el consentimiento otorgado es verdaderamente informado e inequívoco.

Por lo demás, se puede apreciar en la Política de Privacidad de WhatsApp que, se hace uso de un lenguaje sencillo y claro a la hora de exponer la información, no empleándose términos jurídicos o técnicos demasiado complejos y su extensión – valorada independientemente del resto de secciones de la Información Legal disponibles – es razonable, ocupando 2.737 palabras. De forma que resulta, desde esta perspectiva lingüística, fácilmente accesible al usuario en cuanto a su presentación aunque indudablemente mejorable si se excluyesen las frases superfluas y vacías de información en su contenido.

IV.2.3. Aspectos Legales

En primer lugar, al consultar la política de privacidad de WhatsApp, no podemos descargar una copia – tal y como hemos visto en el apartado IV. 2.1. (Accesibilidad Técnica) – y, aunque sí se indica la fecha de última modificación como la de 25 de agosto de 2016, en ningún momento aparece de forma clara la fecha en que la misma es vinculante para con el usuario. Si bien aparece un enlace a "*versiones*

[135] WHATSAPP. Página Principal. *Información Legal*. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com
[136] Op. Cit. (2009) "*The privacy jungle: on the market for data protection in social networks*". Página 21.

antiguas" al clicar sobre el mismo remite a otra página – tal y como se muestra en la **Imagen 16**[137] – que únicamente presenta una versión anterior de la política de WhatsApp (de fecha 7 de julio de 2012) pero que sólo está disponible en inglés – a pesar de que la página principal sigue estando en presentación en lengua española – lo cual limita aún más la efectividad de la puesta a disposición de versiones anteriores.

En lo que se refiere a la ley aplicable y resolución de conflictos, no viene definido dentro de la Política de Privacidad pero sí dentro del apartado "*Términos de Servicio*" recogido bajo la misma página con la "*Información Legal*" de WhatsApp. Sería conveniente, para mayor claridad, incluir dicha información también dentro de la política de privacidad aunque sea de una forma más resumida y con un enlace que conduzca, aunque sea por referencia, a dicha cláusula para que el interesado

Imagen 16 – Actualizaciones: Política de privacidad de WhatsApp.

conozca las condiciones en que se han de resolver los posibles los conflictos.

Dentro de los Términos de Servicio de WhatsApp, al respecto de la resolución de conflictos, se establece como Ley aplicable la del Estado de California "*independientemente de las disposiciones sobre conflictos de leyes*". Incluye, también, una disposición de arbitraje especial para los usuarios de los Estados Unidos y Canadá, arbitraje obligatorio individual – por el que se renuncia por tanto a resolver el conflicto ante un juzgado competente y renunciando expresamente a una demanda colectiva – y cuando se trata de un usuario fuera de Estados Unidos y Canadá, se acepta resolver el conflicto "*exclusivamente en el Tribunal de Distrito de los Estados Unidos para el Distrito Norte de California o un tribunal estatal ubicado en el condado de San Mateo en California*".

Ahora bien, tal y como resolvió recientemente la Sala Tercera del Tribunal de Justicia de la Unión Europea, *"…una cláusula que figura en las condiciones generales de venta de un profesional, que no ha sido negociada individualmente, en virtud de la cual la ley del Estado miembro del domicilio social de ese profesional rige el contrato celebrado por vía de comercio electrónico con un consumidor,* ***es abusiva en la medida en que induzca a error a dicho consumidor dándole la impresión de que únicamente se aplica al contrato la ley del citado Estado miembro, sin informarle de que le ampara también, en virtud del artículo 6,***

[137] WHATSAPP. Página Principal. *Información Legal*. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com

apartado 2, del Reglamento Roma n.º 593/2008, la protección que le garantizan las disposiciones imperativas del Derecho que sería aplicable, de no existir esa cláusula"[138] , la imposición de las leyes asignadas por WhatsApp sin que el usuario tenga opción alguna a su negociación no resta a que las normas de derechos privado internacional continúan protegiendo al usuario y se debería informar de ello al usuario. Caso contrario, se crea una situación de indefensión que, además, tiene como efecto el disuadir al usuario de iniciar actuaciones en unos tribunales extranjeros de los que desconoce la ley aplicable y con el coste que ello le supondría en asesoramiento jurídico local y, en su caso, desplazamiento hasta el estado de California.

El espíritu de esta cláusula se aleja, además, de la protección que normalmente se le reconoce al consumidor por el que en normas como la Ley de servicios de la sociedad de la información y de comercio electrónico (LSSI) se establece que "[l]*os contratos celebrados por vía electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual*"[139].

Se hace referencia, también, bajo el apartado "*Nuestras operaciones globales*" dentro de la política de privacidad sobre cómo el usuario reconoce "*que las leyes, disposiciones y normas del país en el que se almacena o precisa tu información pueden ser diferentes de aquellas que rigen en tu propio país*" si bien no indica cuál es la ubicación de sus servidores o en qué país(es) se procesa dicha información personal. En cualquier caso, la Directiva 95/46/CE establece en su artículo 4 lo siguiente:

> *"Derecho nacional aplicable*
>
> *1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:*
>
> *a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;*
>
> *b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;*
>
> *c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.*

[138] Tribunal de Justicia de la Unión Europea. TJUE (Sala Tercera). Asunto C-191/15. Sentencia de 28 Julio 2016.

[139] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Artículo 29.

> *2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".*

De forma que el hecho de que la información se almacene en otro país no conlleva necesariamente que no apliquen las normas nacionales y habría que entrar a analizar si alguno de los supuestos del artículo 4 de la Directiva 95/46/CE pudiesen aplicarse también como ya se ha hecho en el caso de Google (sentencia del Tribunal Supremo 1384/2016, Sala de lo Contencioso-Administrativo, Sección Sexta, de fecha 13 de junio de 2016) o de Facebook en la resolución de la Agencia Española de Protección de Datos (AEPD) en Procedimiento PS/00082/2017. Además, la propia Directiva 95/46/CE dispone en su considerando 20 que "*el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva*".

Según se deriva de los fundamentos anteriores, indicar que la normativa que aplica puede ser distinta a la ley del país del usuario por encontrarse almacenados los datos en un lugar diferente es una información errónea y hace confundir al usuario entre el rol de encargado, que tiene entre sus funciones la de atención de los derechos, con el de responsable del tratamiento. Por lo que la información facilitada al interesado no resulta ajustada a lo exigido en la normativa de la Unión Europea en materia de protección de datos de carácter personal.

Por otro lado, en todo contrato es importante establecer un canal de comunicaciones y notificaciones. Al respecto WhatsApp pone a disposición del usuario la dirección física donde contactar en caso de preguntas e, incluso, establecen un canal de comunicación electrónica que, tras varios enlaces, conduce a un listado de correos electrónicos a través de los cuales poder dirigirse el interesado con dudas. Sin embargo, no resulta proactivo y transparente la forma en que se comunica al usuario una actualización de la política de privacidad – tal y como se muestra en la **Imagen 17**[140] – WhatsApp indica que únicamente notificará

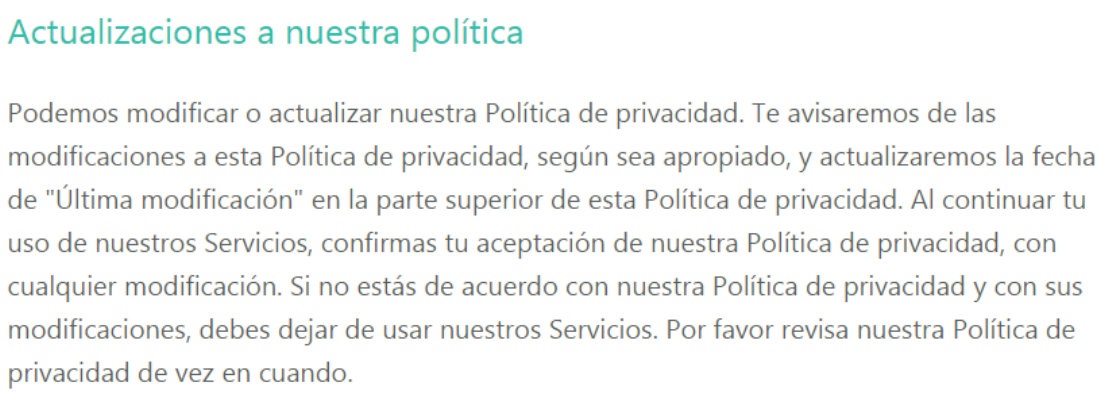


Imagen 17 – Actualizaciones a la Política de Privacidad de WhatsApp.

[140] WHATSAPP. Página Principal. *Información Legal*. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com

de las modificaciones "*según sea necesario*", esto es, dejando a su criterio unilateral determinar cuándo un cambio en la política es de suficiente relevancia como para prevenir al usuario.

Asimismo, como es común en los sitios web, se establece claramente el principio por el que el uso continuado de la red social constituye una aceptación tácita de la política de privacidad, inclusive "*cualquier modificación*" que se haya realizado, comunicado o no al usuario. Llama especialmente la atención la petición que hace WhatsApp al final de esta cláusula por la que el usuario debe – *por favor* - revisar "*de vez en cuando*" la política, trasladando así la obligación de notificar de WhatsApp al usuario. Lo cual, una vez más es información errónea y contraria a la normativa de protección de datos según la cual el responsable del fichero o tratamiento es quien tiene el deber de información, por el que está obligado a informar a los titulares de los datos personales en la recogida de éstos y obtener el consentimiento para el tratamiento de los mismos y no debe recaer sobre el usuario la carga de informarse y consultar "de vez en cuando" los términos de la política de privacidad.

IV.2.4. Uso de los datos

En lo que se refiere a la información que ofrece la política de privacidad de WhatsApp respecto del uso que se hace de los datos y exactamente qué datos se recopilan y cómo, la política dedica dos grandes apartados. El apartado "*Información Recopilada*" para definir la información que se recaba y cómo o cuándo se recaba la misma – a través de sub-apartados *Información que tú proporcionas / Información recopilada automáticamente / Información de terceros* – y el apartado "*Cómo usamos la información*". A través de estas secciones de la política se describe de forma estructurada y clara, con el uso de ejemplos, de forma que tras su lectura el usuario se hace una idea de qué tipo de datos se recaban en el uso normal de WhatsApp. A lo largo del mismo se indica que los mensajes enviados por medio de WhatsApp no se conservan y que se eliminan de los servidores tras su entrega. Además los mensajes son cifrados de extremo a extremo de forma que ni WhatsApp "*ni terceros los puedan leer*".

Bajo el apartado "*Cómo usamos la información*" WhatsApp se refiere a que se usan únicamente para ayudar "*a operar, proveer, mejorar, entender, personalizar y comercializar [sus] servicios, así como ofrecer servicios de ayuda*". En este apartado no se hace referencia alguna a que se usen los datos con fines publicitarios, de hecho se refieren en todo caso a que WhatsApp es un entrono con "*cero anuncios banner de terceros*". A pesar de una afirmación tan rotunda como se puede apreciar en la **Imagen 18**[141], no es reconfortante leer a continuación que si alguna vez cambian de postura se limitarán a actualizar su política, y ya hemos

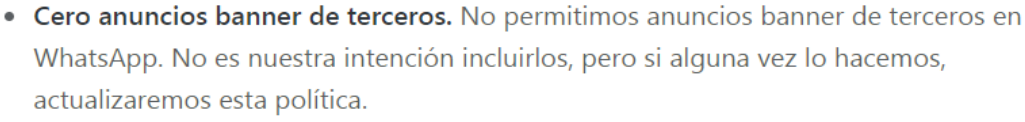

- **Cero anuncios banner de terceros.** No permitimos anuncios banner de terceros en WhatsApp. No es nuestra intención incluirlos, pero si alguna vez lo hacemos, actualizaremos esta política.

Imagen 18 – Parte del apartado "*Cómo usamos la información*" de la Política de Privacidad de WhatsApp

[141] WHATSAPP. Página Principal. *Información Legal*. [Consultado el: 6 de septiembre de 2017]. Disponible en: https://www.whatsapp.com

analizado cómo se notifican los cambios en la política – "*por favor, revisa nuestra política de vez en cuando*" – por lo que parece contradictorio y, una vez más, emplean un lenguaje que crea una apariencia de transparencia y seguridad que no es necesariamente efectiva.

Especialmente relevante respecto del uso de datos, aunque no recogido en el apartado "Cómo usamos la información" que hemos visto sino en la sección de "Empresas afiliadas", se establece que WhatsApp podrá compartir toda la información recopilada de sus usuarios con Facebook y todas las empresas que lo componen. En un primer momento se indica en este apartado de la política de privacidad que "*Facebook también puede usar nuestra [de WhatsApp] información para mejorar tus [del usuario] experiencias con sus servicios […] mostrarte anuncios y ofertas relevantes*" para luego afirmar que "*Facebook no usará tus mensajes de WhatsApp para ningún otro propósito distinto del de ayudarnos a operar y proveer nuestros Servicios*". De forma que se crea confusión respecto del fin que se le va a dar a dicha información compartida con las empresas que componen el grupo de Facebook, mencionan que es para mostrar anuncios pero no hablan expresamente de fines publicitarios y luego alegan que el único fin de compartir los mensajes es para mejorar la operación de los servicios.

Evidentemente este tipo de lenguaje, como adelantábamos, no contribuye a crear una política informadora ni transparente respecto del uso real que se hace de sus datos ni pone a disposición del usuario medidas para configurar la aplicación de forma que se impida usar sus datos para mostrar anuncios, de forma que se le otorgue control y capacidad de decisión al usuario. En consecuencia, no queda alternativa alguna y conlleva que el mero uso de los servicios significa que se va a compartir la información con la "familia" Facebook sin que nada pueda hacer el usuario para evitarlo más que dejar de usar los servicios de WhatsApp.

IV.2.5. Resumen

Tras el análisis realizado sobre la política de privacidad disponible de WhatsApp, podemos concluir que la misma no ha superado los requisitos mínimos que se esperan a un nivel técnico, lingüístico, legal y de uso de datos.

Desde la perspectiva de la accesibilidad técnica hemos visto que para garantizar su accesibilidad WhatsApp debería incluir, en primer lugar, la política de privacidad como un documento a consultar de forma independiente al resto de términos y condiciones de uso y en un formato que sea descargable y archivable a través de un enlace habilitado, que esté visible en todo momento desde la página web y que se abra en una nueva ventana. Desde la App, a su vez, debería ponerse a disposición del usuario directamente desde el apartado de "*Configuración*" de la App desde donde el usuario pueda leer la Política de Privacidad en cualquier momento y sin necesidad de acudir a demasiados sub-apartados ni al navegador.

En cuanto a la accesibilidad lingüística, aunque fácilmente accesible al usuario respecto de su presentación debe aún evitarse el uso las frases superfluas y vacías de información en su contenido que únicamente contribuyen a crear una falsa sensación de seguridad en el usuario y ponen en duda la validez del consentimiento otorgado ante la falta de precisión en la información.

Desde un punto de vista legal, resulta alarmante la ausencia de información de la política de privacidad sobre aspectos relevantes - fecha vinculante, ubicación del procesamiento de datos, la ley aplicable y jurisdicción – pero aún más grave es que en varias ocasiones se facilita información errónea que no resulta ajustada a lo exigido en la normativa de la Unión Europea en materia de protección de datos de carácter personal.

Y ello, de forma similar, sucede con la información que se ofrece respecto del uso que se hace de los datos que resulta no sólo ambigua sino también errónea y, en consecuencia, no podemos decir que se esté ante una manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

IV.3. YouTube (GOOGLE)

Al entrar a analizar la red social de YouTube apreciamos en seguida que la misma pertenece a Google y, por tanto, para registrarse en la misma se hace a través de la creación de una cuenta de Google. Con centros de datos presentes en todo el mundo, Google es capaz de procesar más de cien mil millones de peticiones de búsqueda mensuales[142] y su motor de búsqueda es el sitio web más visitado a nivel mundial tal como muestra el ranking web internacional Alexa[143].

De forma que para acceder a sus servicios de vídeo y música de YouTube, el usuario debe crearse una cuenta de Google (o asociar una ya existente) y es en ese momento que observamos que, una vez introducidos los datos mínimos para el registro y, justo antes de activar la cuenta, que se le solicita al usuario que acepte las Condiciones de Servicio y la Política de Privacidad de Google. Esto es, no cuenta YouTube con su propia política de privacidad.

En cualquier caso, no debe olvidarse que las condiciones de uso y política de privacidad de Google son un acuerdo legal vinculante y la relación que se crea con el usuario desde el momento del registro se va a regir por dichas condiciones y resulta ser este el momento en el que – justo antes de confirmarse el alta del usuario al clicar en "*Siguente Paso*" – tal y como se aprecia en la **Imagen 19,** se abre un diálogo que presenta un enlace tanto a las condiciones de servicio como a la política de privacidad y un breve resumen del contenido de las mismas. Un

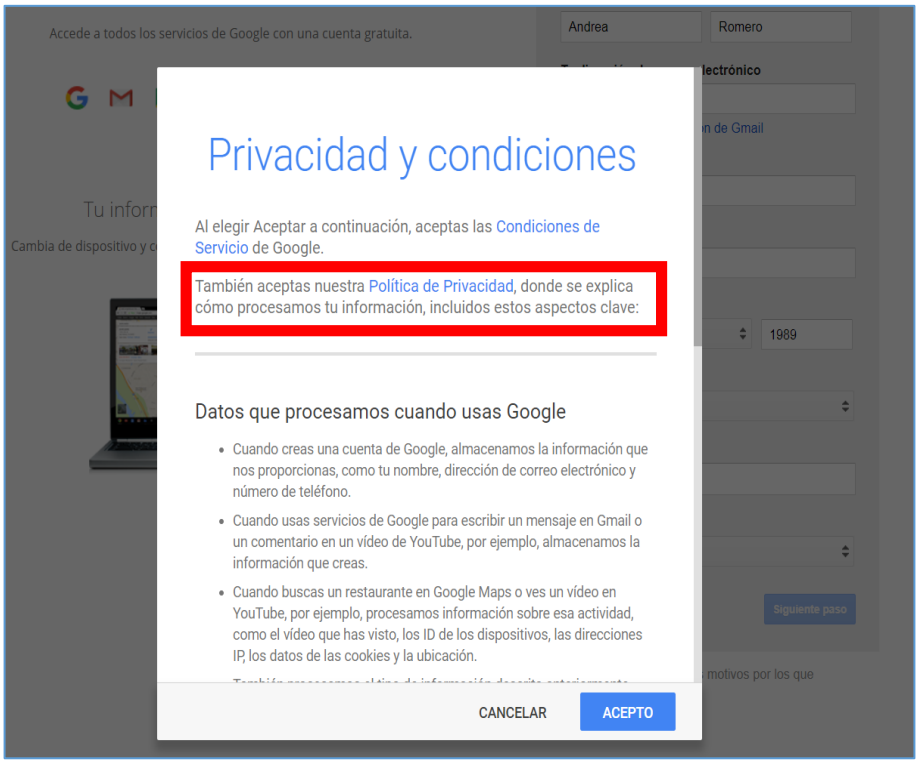


Imagen 19 – Aceptación de la Política de Privacidad de Google en el momento de registro.

142 MASHABLE. http://mashable.com/2015/10/12/google-mobile-searches/#EZtu.Dmkvuqw Consultado: 2 septiembre 2017.

143 ALEXA, Website Traffic, Statistics, and Analytics. Site Info on Google. https://www.alexa.com/siteinfo/google.com

resumen que no llega a 300 palabras – frente a las casi 10 páginas que representa solo la política de privacidad, véase el Apatado IV.2.2 (Accesibilidad lingüística) – y, sin embargo, es suficiente para dar por "leídas" y "entendidas" las condiciones por parte del usuario en una aceptación válida en el momento del registro. Es decir, no se exige que se continúe con la lectura de la política de privacidad completa para poder concluir el proceso de creación de la cuenta.

Asimismo, hay que remitirse a bien entrado el documento para encontrar el apartado que identifica que la política de privacidad aplica a todos las empresas de Google. Sin embargo, no se ofrece un listado de qué empresas son estas. De hecho, ofrece un lenguaje poco claro en cuanto a que no es de aplicación esta política de privacidad a aquéllas empresas de Google que dispongan de política de privacidad propia. Por lo que no se dispone de una forma clara e inequívoca cuándo aplica dicha política respecto de las empresas del grupo de Google. Ello supondría para el usuario verse obligado a realizar un esfuerzo adicional para poder comprobar, respecto de la empresa que forma parte de Google y que pretende estudiar, que no existe otra política de privacidad que prevalezca sobre esta de carácter general. Por lo que se podría decir que un usuario que busca informarse sobre el tratamiento de sus datos personales por las empresas de Google no podrá estar completamente seguro de estar analizando la política de privacidad efectivamente aplicable en su caso.

IV.3.1. Accesibilidad técnica

Una vez completado el registro, la política de privacidad aparece presente en el sitio web de YouTube – véase la **Imagen 20**[144] – aunque se ve agrupado entre otros enlaces y siempre un lado de la página donde inicialmente no aparece a la vista del usuario, al ser necesario que se desplace en la página para visualizar el enlace. Aunque sí aparece el enlace adecuado, el hecho de que durante el uso del servicio el acceso a la política de privacidad se presente de forma disimulada y sin mayor protagonismo denota un claro desinterés de esta red social por que dichas condiciones se conozcan por sus usuarios.

Al analizar la política de privacidad en general, se ha de tener en cuenta que la accesibilidad técnica por la cual un usuario pueda acceder a las mismas sin sentirse desalentado a ello por la remisión de una a otra página web o documento sin que sea sencillo seguir el hilo de información. En el caso de la política de privacidad de Google desde la página principal de YouTube, la misma no está visible a primera vista por parte del usuario pues, tal y como se muestra en la **Imagen 20** es necesario fijarse en los distintos apartados que aparecen en la columna a la izquierda y desplazarse dentro de la misma – que no dentro de la ventana en sí – hasta que aparece el enlace, en un tipo de letra de tamaño bastante menor que pasa desapercibido. Además, al clicar sobre el enlace "*Privacidad*" no se abre una nueva ventana sino que interrumpe la actividad del interesado que muestra la política de privacidad de Google que aplica, como ya hemos visto, como empresa principal tras la adquisición de YouTube. Sí se ofrece, en cambio, la

144 YOUTUBE. Página Principal. [Consultado: 16 Septiembre 2017.] Disponible en: "https://www.youtube.com".

opción de descargar una versión en PDF desde la ventana que contiene la política de privacidad y, por tanto, una versión archivable para el usuario.

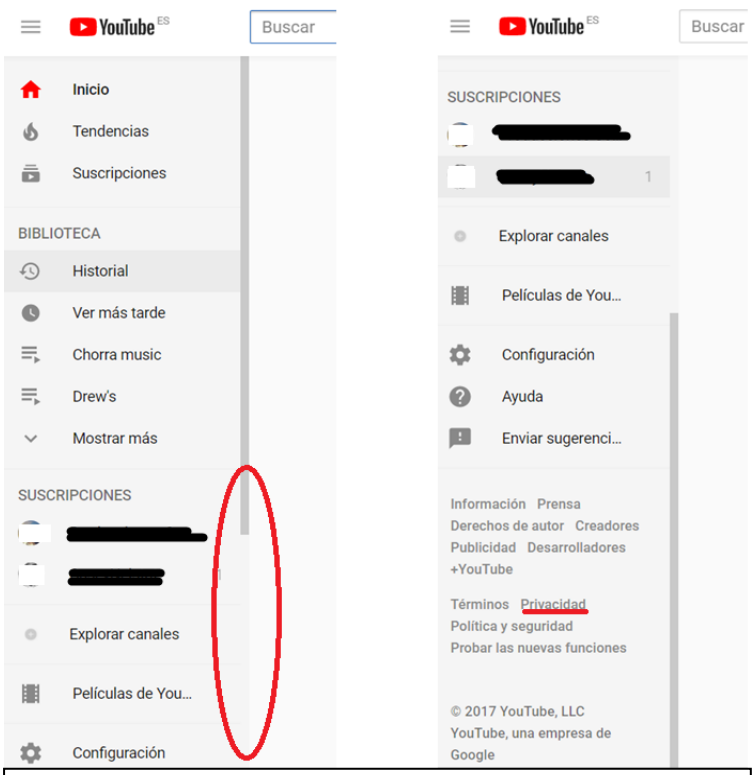


Imagen 20 – Acceso a la Política de Privacidad de YouTube desde la página web

En la **Figura 6**[145] podemos observar los distintos pasos para acceder a la política de privacidad de YouTube desde la App.

En primer lugar hay que acceder a la "Cuenta" del usuario donde aparecen desplegados cinco opciones – *Mi Canal / Cambiar de Cuenta / Configuración / Condiciones de Servicio y Política de… / Ayuda y Sugerencia* – de las cuales nos interesa la penúltima. Si bien en primera instancia podría resultar positivo que se presenten las condiciones de servicio desde la Cuenta resulta decepcionante que el título "*Condiciones de Servicio y Política de…"* no aparezca completo pues ello supone que no puede saber el usuario si al acceder a este apartado va a encontrar también la Política de Privacidad que estamos buscando.

En cualquier caso, al acceder a este apartado se redirige al usuario a los "*Términos y Condiciones del Servicio*" que están habilitados para su lectura desde la misma App, lo cual es positivo, pero que no contiene ninguna "política de" como se anticipaba en su título incompleto mostrado desde la Cuenta del usuario. De hecho, el usuario tiene que desplazarse en el texto de los términos y condiciones de uso de YouTube y leer el mismo para "toparse" con un enlace que redirige a la "Política de Privacidad de YouTube", un enlace que se presenta en un párrafo por el que se informa al usuario que la política de privacidad es parte de los términos de uso de YouTube. El Punto 1.2 que se muestra en el punto 4 de la **Figura 6**[146] dispone que el "*acuerdo legal con YouTube se compone de (A) los términos y condiciones establecidos en este documento, (B) la Política de Privacidad de YouTube [enlace] y (C) las Directrices de la Comunidad de YouTube [enlace] (conjuntamente, los "Términos y Condiciones")*".

[145] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de Abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"
[146] YOUTUBE. App, actualizada el 16 de septiembre de 2017.

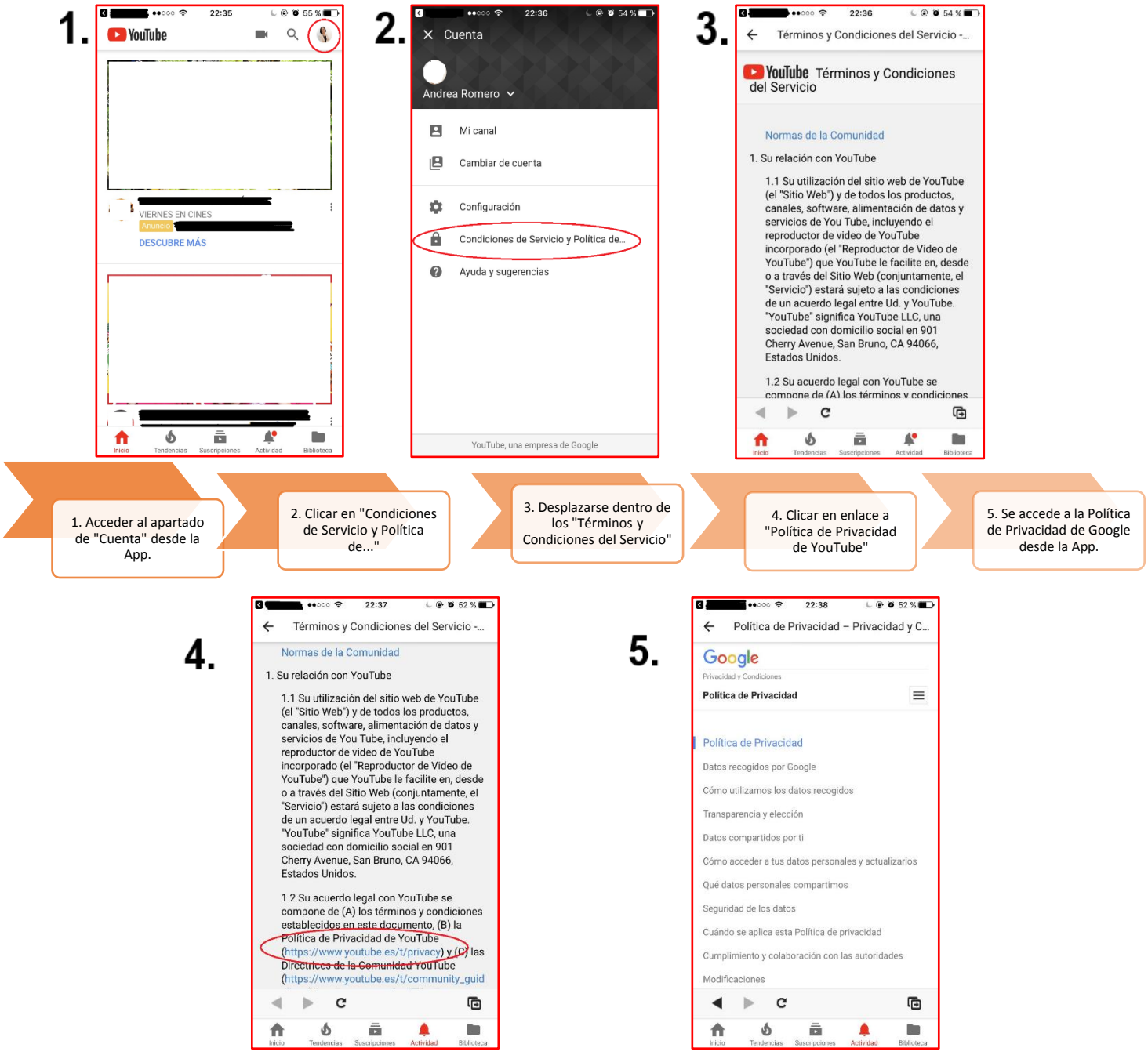


Figura 6 – Pasos para acceder a la Política de Privacidad de YouTube desde la App.

Por lo que, a pesar de que en el apartado 1.3 se informa al lector de que los Términos y Condiciones – que incluyen la Política de Privacidad – "*constituyen un contrato legalmente vinculante*" y recomienda que se lean "*detenidamente*" la misma no es de obligada consulta ni mucho menos se requiere aceptación expresa de la Política de Privacidad. YouTube se limita a insertar un mero enlace dentro del contenido de sus términos de uso. Enlace que una vez clicado, lleva al usuario a la Política de Privacidad de Google – la misma que hemos visto desde la página principal –, permitiendo su lectura desde la misma App y ofreciendo al usuario la posibilidad de abrir la política desde el navegador. Al igual que ocurría desde la página web, la Política de Privacidad de Google desde la App también incluye un enlace para descargar la versión en PDF, la cual, una vez clicada, ofrece un versión

PDF de la misma pero que, a diferencia de lo que ocurría desde el navegador, no ofrece la opción de descargar desde la App. El interesado tendría que remitirse a la versión al navegador para poder archivar una copia del documento PDF.

En definitiva, la accesibilidad técnica desde la App tiene múltiples aspectos positivos como son la puesta a disposición directamente desde un apartado dentro de la Cuenta del usuario, habilitando su lectura desde la misma App aunque ofreciendo de forma opcional su lectura desde el navegador. No obstante, para que la accesibilidad a la política de privacidad específicamente sea efectiva, debería habilitarse un apartado que lleve directamente a la misma – al igual que se hace desde la página principal – sin tener que acceder a la política a través de los Términos y Condiciones de YouTube e, incluso, habilitar la descarga en PDF versión archivable también desde la misma App.

IV.3.2. Accesibilidad lingüística

Otro aspecto a evaluar en las políticas de privacidad no es otra que la extensión del documento en sí y los términos que se emplean en los mismos, pues una política excesivamente extensa o el uso de palabras ambiguas que puedan disuadir al usuario de su completa lectura pues ello podría implicar que su aceptación no contaría con un consentimiento informado por el mero hecho de no haberse completado la lectura. Sin embargo, tampoco debería ser tan corta que no incluyese información relevante para el usuario y por tanto, por omisión, no se contase con un consentimiento debidamente informado a la hora de aceptarlas.

En el caso de la política de privacidad de Google, aplicable a YouTube, en su versión descargable en PDF cuenta con nueve páginas en lo que supone un total de 4.667 palabras. Además de ser significativamente extenso, lo especialmente complejo en este caso es que el lector se encuentra con que en las nueve páginas de que está compuesta se incluyen 91 hipervínculos que enlazan a otras ventanas que se abren o nuevos documentos a través de los cuales se ofrece información adicional y que sencillamente comprenden demasiada información como para poder ser abarcable por un usuario medio. En la práctica, incluso un individuo con todo su esmero, resulta imposible, de una sola lectura de la política de privacidad, abarcar toda la información que Google parece querer hacerle llegar a través de su política de privacidad. Es inevitable verse inmerso en una cascada de enlaces que desvían al lector del objetivo inicial que no es otro que comprender los términos que regulan el tratamiento de sus datos personales.

Por otro lado, se emplean en esta política numerosos términos que se podrían considerarse particular e intencionadamente ambiguos. Así, para referirse a los terceros con quienes comparten los datos, emplean expresiones como "*otras personas o empresas de confianza*", "*nuestros partners*" o "*nuestros afiliados*" o indican que no se compartirá con empresas "*que no tengan relación Google*". Si bien, por ejemplo, una referencia a sus afiliados puede verse como un término legal fácilmente identificable, lo cierto es que en el caso del grupo Google es especialmente relevante el hecho de que se estima que desde el año 2010 ha adquirido, de media, una empresa por semana y de cuya empresa Alphabet (desde 2015, la empresa matriz del grupo) se calcula que a fecha de diciembre de 2016

contaba con más de 200 empresas[147]. Dadas las circunstancias, puede que emplear un término tan sencillo como "afiliados" en el caso de Google no deba considerarse suficiente como para que el usuario se dé por informado y, cuanto menos, debería proporcionarse una lista detallada y actualizada sobre dichas filiales del grupo que, de por sí, tendrán acceso en todo caso a sus datos personales de acuerdo con la política de privacidad.

Por ello, nos encontramos con que, quizá en su afán de ser muy conciso, la política de privacidad de Google en cuanto a su contenido resulta ser contraproducente respecto de su fin mismo por no facilitar información de forma clara y no muy extensa y, además, el empleo de un lenguaje ambiguo a lo largo de la política de privacidad contrasta con la afirmación que hace Google en la misma bajo la sección "*Transparencia y Elección*": "*Nuestro objetivo es informarte claramente acerca de los datos que recogemos, de modo que puedas tomar decisiones adecuadas en lo que respecta a su utilización*." De forma que resulta evidente desde una perspectiva lingüística que la información presentada al usuario no resulta lo suficientemente clara como para que el consentimiento otorgado en su aceptación pueda ser considerado específico e informado.

IV.3.3. Aspectos Legales

Si entendemos la política de privacidad Google como un contrato jurídico que regula la relación que se establece con sus usuarios, sería de esperar que incluyese que quedase constancia de la fecha en que dicha relación se vuelve vinculante. En el caso de Google encontramos la fecha de última actualización de la misma que se indica fue el 17 de abril de 2017 – tal y como se aprecia en la **Imagen 21**[148] – que, aunque no se vincula expresamente, puede ponerse en relación con la fecha de registro para determinar cuál era la política aplicable en el momento de otorgar el consentimiento, más aún teniendo en cuenta que se dispone de las versiones anteriores.


Google

Política de Privacidad

Última modificación: 17 de abril de 2017 (ver versiones archivadas) (Los ejemplos con hiperenlaces están disponibles al final de este documento).

Imagen 21 – Fecha de actualización de la Política de Privacidad de Google

De la misma manera, sería de esperar que en un contrato se estableciesen unas normas de notificaciones entre las Partes. Sin embargo, en esta política no se

[147] WIKIPEDIA. *List of Mergers and Acquisitions by Alphabet.* [Consultado el: 18 septiembre 2017]. Disponible en: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet#cite_note-1

[148] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"

incluyen los datos de contacto de Google, ni el domicilio social de la misma, ni un correo electrónico de contacto. Además, en caso de que tenga lugar un cambio en las condiciones que rigen la política de privacidad, Google no se obliga a comunicar dichos cambios salvo que limiten los derechos del usuario o si son significativas, en cuyo caso se comprometen a notificar por medios "*más destacados*" sin especificar cuáles. En cualquier caso, se emplea un término ambiguo – "*significativo*" – que lejos de definir en qué casos sería pertinente una notificación, queda a la sola discreción de Google determinar cuándo tal notificación "más destacada" sería necesaria sin siquiera conceder un mínimo plazo de preaviso para que un usuario informado pueda tomar medidas y revocar el consentimiento si así lo estima oportuno. Véase la **Imagen 22**[149], resaltado propio.

Modificaciones

Nuestra Política de privacidad se podrá modificar en cualquier momento. No limitaremos los derechos que te corresponden con arreglo a la presente Política de privacidad sin tu expreso consentimiento. Publicaremos todas las modificaciones de la presente Política de privacidad en esta página y, si son significativas, efectuaremos una notificación más destacada (por ejemplo, te enviaremos una notificación por correo electrónico si la modificación afecta a determinados servicios). Además, archivaremos las versiones anteriores de la presente Política de privacidad para que puedas consultarlas.

Imagen 22 – Cláusula de Modificaciones en la Política de Privacidad de Google.

En este marco legal que debería imponerse en las políticas de privacidad general normalmente se esperaría que se incluyese también una cláusula de Ley Aplicable y Jurisdicción, con mayor sentido teniendo en consideración el contexto global que caracteriza al mundo digital que es Internet y donde se desenvuelven las redes sociales en general. Asimismo, cobra especial relevancia si se tiene en cuenta la discrepancia que existe en la mayoría de los casos entre la ubicación geográfica del domicilio social del operador y el lugar donde efectivamente se lleva a cabo el procesamiento de los datos.

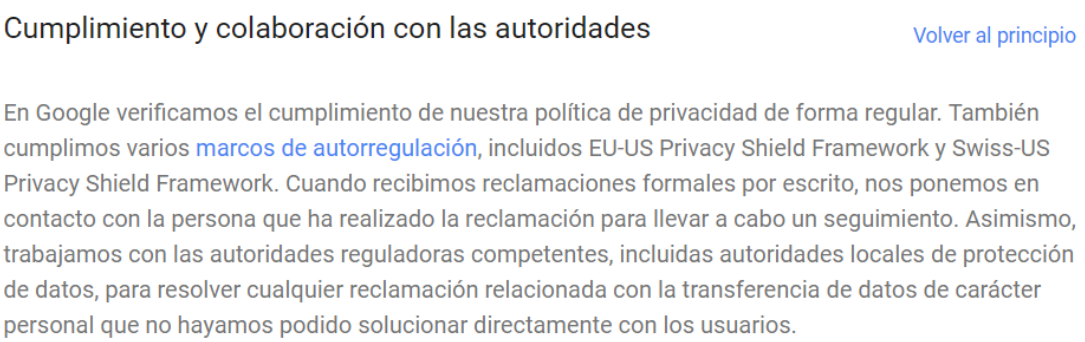
En este sentido, ya hemos visto que la política de privacidad de Google no establece claramente el domicilio social de la empresa y, respecto de la ubicación donde tiene lugar el procesamiento de datos se limita a indicar que "*están ubicados en distintos países del mundo*" – véase **Imagen 23**[150] –, lo cual resulta bastante alarmante por sí solo pero se ve agravado por el hecho, como vemos, de que no se incluye una cláusula que defina específicamente la ley y jurisdicción aplicable. Ello podría contribuir a crear una situación de indefensión respecto del usuario que, incluso una vez tomada la decisión de tomar medidas legales en caso de violación

Google lleva a cabo el tratamiento de los datos personales en sus servidores, que están ubicados en distintos países del mundo. Podremos llevar a cabo el tratamiento de tus datos personales en un servidor que no esté ubicado en tu país de residencia.

Imagen 23 – Tratamiento de los datos personales por Google según su política de privacidad.

[149] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"
[150] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"

de sus datos personales, tendría que salvar primero el obstáculo de determinar ante qué jurisdicción y qué ley aplicaría en ese caso.
No obstante, la política de privacidad de Google sí hace referencia a ciertos marcos de autorregulación entre los que se incluyen el *EU-US and Swiss-US Privacy Shield Frameworks* ("Privacy Shield"), tal y como se muestra en la **Imagen 24**[151]. Tal y como vimos en el Apartado IV.I.3., después de que el Tribunal Europeo de Justicia derogase el 6 de octubre de 2015 el conocido como el acuerdo Safe Harbor [152], se redactó rápidamente el Privacy Shield que busca garantizar la transferencia de datos conforme a las exigencias del RGPD y a partir del mismo, pone a disposición de las empresas de la Unión Europea una serie de recursos como un sistema de arbitraje paritario, gratuito para las empresas miembros del nuevo acuerdo en el que las reclamaciones podrán efectuare en la lengua propia del que las realiza y los afectados dispondrán de acciones eficaces y prácticas cuando consideren que sus derechos han sido vulnerados entre otros aspectos[153].


Cumplimiento y colaboración con las autoridades

Volver al principio

En Google verificamos el cumplimiento de nuestra política de privacidad de forma regular. También cumplimos varios marcos de autorregulación, incluidos EU-US Privacy Shield Framework y Swiss-US Privacy Shield Framework. Cuando recibimos reclamaciones formales por escrito, nos ponemos en contacto con la persona que ha realizado la reclamación para llevar a cabo un seguimiento. Asimismo, trabajamos con las autoridades reguladoras competentes, incluidas autoridades locales de protección de datos, para resolver cualquier reclamación relacionada con la transferencia de datos de carácter personal que no hayamos podido solucionar directamente con los usuarios.

Imagen 24 – Referencia al EU-US Privacy Shield en la política de privacidad de Google.

Dado que el Privacy Shield ha sido ratificado por la Comisión Europea [154] el cumplimiento del mismo por parte de Google debería garantizar la protección de los derechos individuales. Sin embargo, no se pone en conocimiento del usuario cuáles son los mecanismos accesibles y asequibles de resolución de litigios de que dispone y cuál es la forma de poner una reclamación por parte del usuario. Por esto, la referencia al Privacy Shield que se incluye en la política de privacidad ofrece ciertas garantías pero, en lo que al consentimiento informado se refiere, el que se incluya un enlace para profundizar en el Privacy Shield es insuficiente por no presentarse la información de forma clara, y directa, al usuario. En primer lugar porque el usuario no tiene por qué conocer los términos del Privacy Shield y, en segundo lugar, porque es un dato relevante a la hora de otorgar consentimiento a la política de privacidad que le es aplicable.

[151] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"
[152] Tribunal de Justicia de la Unión Europea. Petición de decisión prejudicial planteada por la High Court (Irlanda). Caso Maximillian Schrems y Data Protection Commissioner (C-362/14). Sentencia de 6 Octubre 2015
[153] Cámara de Comercio de EE.UU. en España. 2016. "*Privacy Shield y el impacto de la privacidad y la ciberseguridad en las relaciones transatlánticas*".
[154] Comisión Europea. Comunicado de Prensa. *La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos*. Bruselas, 12 de Julio de 2016.

IV.3.4. Uso de los datos

Como hemos anticipado, uno de los aspectos más importantes a evaluar cuando se analiza una política de privacidad es la información que se transmite al usuario respecto del uso que se va a hacer de sus datos personales. Por ejemplo, una buena política de privacidad explicará claramente por cuánto tiempo retiene los datos, si se transmiten a terceros y, en tal caso, a quién, cómo y con qué objeto. Sin embargo, en el estudio llevado a cabo de la política de privacidad de Google se ha podido apreciar que no se hace referencia a la duración por la que se retendrán los datos.

Por otro lado, Google incluye en su política de privacidad un apartado que denomina "*Datos recogidos por Google*" que a su vez se desglosa en diferentes apartados que describen en qué supuestos se recaban datos pero, aunque cita algunos ejemplos no ofrece al usuario una lista clara de la información recopilada. De forma similar, se incluye una sección dentro de la política de privacidad para hacer referencia a qué datos son compartidos con terceros – "*Qué datos personales compartimos*", véase la **Imagen 25**[155] –, pero tampoco aquí se precisa un listado completo de qué información se comparte en cada caso. Llama especialmente la atención el hecho de que Google emplea una frase rotunda afirmando que, como regla general, no se comparten los datos personales con personas o entidades ajenas a Google –"*No compartimos información personal con empresas, organización ni particulares* ***que no tengan relación con Google***", resaltado propio–, lo que es un claro ejemplo del uso de un lenguaje que busca crear apariencia de seriedad a pesar de que ya hemos visto que lo realmente importante en las políticas de privacidad no son los estándares de la empresa respecto de lo que ellos entienden por privacidad sino el contenido e información que logran transmitir al usuario a través de ella respecto del uso que se hace de sus datos. En este sentido, de una afirmación como esta, el usuario es incapaz de comprender qué empresas tienen efectivo acceso a su información personal pues no sólo las empresas del grupo – que veíamos anteriormente que como tal tampoco están claramente delimitadas – sino que cualquier socio, empresa subcontratada o cliente de Google, entre a saber cuántos otros, tendrían "*una relación*" con ellos y, por tanto, Google podrá compartir información con estos.

[155] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"

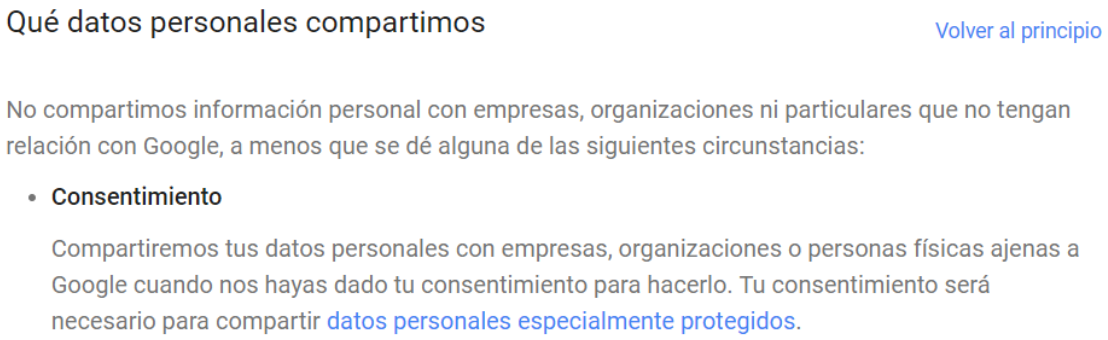


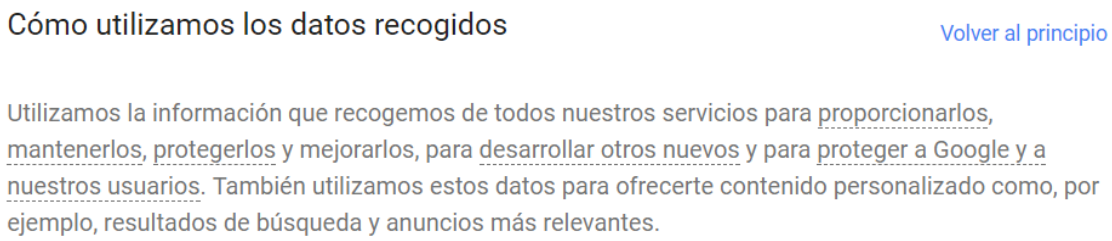
Imagen 25– Consentimiento para compartir datos con terceros.

A continuación establecen una serie de excepciones a dicha regla general – ya de por sí muy amplia – para tratar de definir en qué ocasiones podrán, además, compartir los datos recabados del usuario con terceros. El primer supuesto se refiere al "*Consentimiento*", tal y como también aparece en la **Imagen 25**, se refieran a que el *"consentimiento será necesario*". Lo cual es algo que se encuentra varias veces a lo largo de la política de privacidad de Google: "*Te pediremos tu consentimiento antes de utilizar tus datos para cualquier fin distinto de los establecidos en la presente Política de privacidad.*" Pero en ningún caso se establece la forma en que se obtendrá dicho consentimiento o de qué forma puede oponerse el afectado.

Teniendo en cuenta que el objeto principal de una política de privacidad debería ser el establecer un marco legal por el que se regule la obtención de un consentimiento informado por parte del usuario para autorizar qué datos y con qué fin son usados los mismos en este caso no encontramos que se defina en este apartado de manera adecuada de qué forma se obtiene y conserva dicho consentimiento al uso de los datos que se comparten de forma general y, mucho menos, respecto de los datos personales especialmente protegidos a los que se refiere la **Imagen 25** y para los que, excepcionalmente, podrán también ser compartidos con terceros siempre y cuando cuenten con el consentimiento del usuario. No se garantiza un sistema de preferencias para el tratamiento de los datos especialmente protegidos.

Todo ello lleva a poner en duda que sea suficiente la información descrita en la política de privacidad de Google como para dar eficacia a las garantías contempladas en la normativa de protección de datos respecto del consentimiento informado, el cual debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, de acuerdo con la definición que hace la LOPD en su artículo 3.h). Si bien se viene admitiendo que dicho consentimiento será válido con marcar una casilla de un sitio web de Internet, no parece que se incluya tal casilla en la política de privacidad de Google y sería cuestionable que una casilla por la que se acepten de forma general las condiciones generales de Google – aunque incluyan un enlace a su política de privacidad – sea suficiente como para considerar que dicho consentimiento sea "informado".

Por otro lado, es interesante contemplar el uso que le dan a esos datos y, en este sentido, Google ha incluido un apartado expreso para tratar de definir el objeto y fin por el que se recaban los datos personales de sus usuarios – "*Cómo utilizamos los datos recogidos*"- pero se limita a emplear expresiones ambiguas como que utilizan la información que recogen "*para proporcionarlos, mantenerlos, protegerlos*


Cómo utilizamos los datos recogidos

Volver al principio

Utilizamos la información que recogemos de todos nuestros servicios para proporcionarlos, mantenerlos, protegerlos y mejorarlos, para desarrollar otros nuevos y para proteger a Google y a nuestros usuarios. También utilizamos estos datos para ofrecerte contenido personalizado como, por ejemplo, resultados de búsqueda y anuncios más relevantes.

Imagen 26 – Extracto de la Sección "*Cómo utilizamos los datos recogidos*" en la política de privacidad de Google.

y mejorarlos [los servicios], para desarrollar otros nuevos servicios y para proteger a Google y a sus usuarios", tal y como se aprecia en la **Imagen 26**[156]. Una vez más, a través de la elección del lenguaje empleado, Google crea una falsa apariencia de seguridad e información cuando realmente describe el uso que se hace de los datos de forma que resulta lo suficientemente ambigua como para que no queden claramente delimitados por el interesado.

IV.3.5. Resumen

En el caso de la política de privacidad de Google, aplicable a YouTube, queda probado que no cumple de forma satisfactoria la accesibilidad técnica o lingüística, el contenido legal mínimo ni la claridad suficiente respecto del uso que se hace de los datos recabados.

La política no se encuentra perfectamente habilitada para un acceso fácil y directo por parte de los usuarios ni desde la página principal ni desde la aplicación para móviles y, una vez se logra acceder a ella, resulta imposible abarcar toda la información de una sola lectura de la política de privacidad, pues el lector se ve inmerso en una cascada de enlaces que le desvían del objetivo inicial, que no es otro que comprender los términos que regulan el tratamiento de sus datos personales

En cuanto a la accesibilidad lingüística se emplea un lenguaje ambiguo a lo largo de la política de privacidad de forma que la información presentada al usuario no resulta lo suficientemente clara como para que el consentimiento otorgado en su aceptación pueda ser considerado específico e informado.

Igualmente, desde el punto de vista legal, no incluye la política de Google nada de lo que se esperaría de un documento jurídico vinculante entre las partes y de aquéllos aspectos legales que sí menciona, la información relativa que se aporta es ambigua e insuficiente. Lo que se ve reflejado en la información que se da al usuario sobre el uso que se hace de sus datos o qué información se emplea para

[156] GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de abril de 2017. [Consultado el: 18 septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"

qué finalidad. Finalmente, la política es demasiado ambigua y no cumple adecuadamente su objetivo de informar a la hora de recabar el consentimiento.

V. Conclusión

Toda persona física tiene derecho a la protección de los datos de carácter personal que le conciernen y este derecho le atribuye la facultad de controlar sus datos. La Constitución española, la Ley Orgánica 15/1999 de protección de datos y la carta de derechos fundamentales de la Unión Europea reconocen dicho derecho. Sin embargo, la creciente popularidad de las redes sociales presenta grandes retos en el ámbito de la privacidad y protección de datos.

A diferencia del mundo real donde la información es efímera, en el mundo online la información está prácticamente disponible de forma permanente. Los resultados de este trabajo respaldan nuestra conclusión de que los nuevos desafíos de la era digital se deben abordar desde un enfoque multidisciplinar: social, legal y, especialmente, tecnológico, que deberá jugar un papel importante al promover la investigación en detalle de las violaciones de privacidad online que se presenten[157] y desarrollar políticas de trazabilidad más eficientes.

Si bien las redes sociales han evolucionado para hacer las políticas de privacidad más comprensibles, con resúmenes o el uso de formatos no-textuales, como es el caso de Facebook, de los resultados de este trabajo se deduce que las redes sociales han desarrollado una forma de comunicar e informar a los usuarios en distintos estratos, donde se presentan diferentes niveles de información en función de las inquietudes o intereses de cada usuario[158]. Sin embargo, aún en el nivel más profundo de información que aportan las redes sociales a través de sus políticas de privacidad, hemos observado que el empleo de un lenguaje ambiguo y poco conciso es un factor común en todas ellas.

Al igual que hemos visto que las políticas de privacidad son la herramienta para obtener el consentimiento de los usuarios para el uso de sus datos, también sabemos que para que el consentimiento corresponda con una manifestación de voluntad libre, inequívoca, específica e informada, ha de obtenerse libre de vicios – es decir, sin que se induzca a error –, no admitiéndose como válidos los consentimientos genéricos o inespecíficos. El afectado tiene derecho al acceso a sus datos y, a través del ejercicio de este derecho, debe poder conocer qué datos de carácter personal suyos están siendo tratados por parte del operador, la finalidad de este tratamiento, el origen de los citados datos y si se han comunicado o se van comunicar a un tercero.

Sin embargo, los resultados de este análisis muestran que la capacidad de decisión de los usuarios de las redes sociales se ve sistemáticamente distorsionada por los operadores de las redes sociales, pues está sujeta a una información limitada que impide una completa racionalización por parte del afectado. Se ha demostrado a través del presente estudio de las principales redes sociales en España que la escasez de información accesible para los usuarios es fomentada por las propias redes sociales, a través de alicientes como la "personalización" de los servicios que, finalmente, limitan la importancia de la privacidad online.

[157] Op. Cit. "Interdisciplinary Impact Analysis of Privacy in Social Networks". "*Security and Privacy in Social Networks*". 2013. Página 30.
[158] Op. Cit. (2009) "*The privacy jungle: on the market for data protection in social networks*". Páginas 34-35.

La **Tabla 3** muestra de una forma visual la falta de efectividad de la información que se presenta al usuario de las redes sociales, en base a los datos recabados en el Apartado IV de este estudio pues, a día de hoy, todavía escasea en las políticas de privacidad la mayor parte de lo que se considera información esencial respecto de la privacidad y el uso que se hace de los datos, fundamentales para un consentimiento informado del afectado.

		Facebook	Whatsapp	Youtube (Google)
Accesibilidad Técnica	PP Disponible en Página web	✓	✓	✓
	PP se abre en nueva ventana	✗	✗	✗
	PP versión imprimible/ archivable	✗	✗	✓
	PP Disponible en App	✗	✗	✓
	PP Accesible desde App	✗	✗	✗
Accesibilidad Lingüística	PP menos de 3.000 palabras	✓	✓	✗
	PP evita enlaces con información adicional	✗	✗	✗
	PP evita términos complejos (técnico/legales)	✓	✓	✓
	PP evita expresiones superfluas	✗	✗	✗
	PP incluye formato y estructura clara	✓	✗	✓
Aspectos Legales	PP incluye fecha actualización	✓	✓	✓
	PP contiene correo electrónico de contacto con Red Social	✗	✗	✗
	PP contiene dirección Red Social	✓	✓	✗
	PP indica ley aplicable	✗	✗	✗
	PP indica resolución disputas	✗	✗	✗
Uso de datos	PP indica ubicación datos	✗	✗	✗
	PP indica duración retención datos	✗	✗	✗
	PP notificación de cambios a usuario	✓	✗	✗
	PP identifica terceros con que comparte datos	✗	✗	✗
	PP indica si comparte o no datos con anunciantes	✓	✓	✓
	Efectividad	**40%**	**30%**	**35%**

Tabla 3– Comparación entre las Políticas de Privacidad objeto de estudio y la información aportada en ellas.

PP = Política de Privacidad

Innegablemente, sigue estando latente la ineficacia de la información legal en las redes sociales respecto del uso de los datos al no destacar suficientemente, en las páginas de inicio y en las fases de registro, las políticas de privacidad que regulan el servicio y al no destacar tampoco cuáles son las consecuencias más relevantes sobre el uso y tratamiento de datos personales.

Asimismo, el nuevo Reglamento Europeo de Protección de Datos, que entra en vigor en mayo del 2018, será aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión Europea y, sin embargo, se regían por

normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea. Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. El Reglamento prevé una batería completa de medidas como la protección de datos desde el diseño y por defecto, la realización de evaluaciones de impacto sobre la protección de datos o la promoción de códigos de conducta y esquemas de certificación. Actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

En cualquier caso, las redes sociales deberán adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que la normativa de protección de datos exige. Teniendo en cuenta, que con el nuevo Reglamento Europeo de Protección de Datos desaparece el "consentimiento tácito" y los requisitos a cumplir en relación a la obtención del consentimiento para finalidades adicionales serán más estrictos, ya que se exigirá claridad y concisión (así como no perturbar innecesariamente el uso del servicio) a la hora de detallar las finalidades adicionales y recabar dicho consentimiento, se hace evidente que las redes sociales deberán revisar sus políticas de privacidad y adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento, y demás normativa de protección de datos, establecen.

Todo ello sin olvidar que es fundamental que se continúe investigando y desarrollando nuevas medidas para crear una mayor concienciación en los usuarios y una protección más eficaz de su privacidad por parte de los operadores de las redes sociales. El papel del nuevo Reglamento es incuestionable, pero para que sea efectivo debe integrarse de una forma más sencilla e intuitiva en la experiencia del propio usuario al navegar por las redes sociales.

VI. Bibliografía

Acquisti, A. 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification*. Proceedings of the 5th ACM conference on electronic commerce.* Nueva York, USA.

Acquisti, A.; Gross, R. 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook*. Proceedings of the 6th workshop on privacy enhancing technologies*, pp. 36-58. Cambridge, Reino Unido.

Acquisti, R.; Gross, A. 2005. Information Revelation and Privacy in Online Social Networks (The Facebook Case)*. ACM Workshop on Privacy in the Electronic Society (WPES).* Nueva York.

Agencia Española de Protección de Datos (AEPD). 2017. Procedimiento Núm. PS/00082/2017*.* Resolución R/01870/2017.

Agencia Española de Protección de Datos (AEPD). Resolución de archivo de actuaciones*.* Expediente Núm. E/04948/2016. Disponible en: "https://www.samuelparra.com/wp-content/uploads/2017/09/E-04948-2016_Resolucion-de-fecha-26-07-2017_Art-ii-culo-15-RD-1720-b-2007.pdf"

ALEXA. Website Traffic, Statistics, and Analytics, Site info on facebook.com actualizado el 30 de Agosto de 2017. Consultado el: 01 de Septiembre de 2017. Disponible en: "https://www.alexa.com/siteinfo/facebook.com"

ALEXA. Website Traffic, Statistics, and Analytics. Site info on google.com [Consultado: 2 Septiembre 2017.] Disponible en: "https://www.alexa.com/siteinfo/google.com"

Altshuler, Y.; Elovici, Y; Cremers, A.B.; Aharony, N.; Pentland, P. [ed.]. 2013. *Security and Privacy in Social Networks.* Nueva York : Springer.

Andrews, L.B. 2012. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy.* Nueva York : Free Press

Arce, A. *"*El Derecho a la Intimidad" de Samuel D. Warren y Louis D. Brandeis*.*1995. *Revista Española de Derecho Constitucional*. ISSN 0211-5743, Año nº 16, Nº 47, 1996, pp. 367-373

Argento, Z. 2013. Whose Social Network Account? A trade Secret Approach to Allocating Rights*. Michigan Telecommunications and Technology Law Review*, Vol. 19. Disponible en: "http://repository.law.umich.edu/mttlr/vol19/iss2/1"

Baden, R.; Bender, A.; Spring, N.; Bhattacharjee, B.; Starin, D. 2009. Persona: an online social network with user-defined privacy*.* P*roceedings of the ACM SIGCOMM conference on data communication*, pp. 135-146. Barcelona, España.

BLOG Samuel Parra. "*La casilla premarcada de Whatsapp para ceder datos a Facebook es legal*". [Consultado el: 27 de septiembre de 2017]. Disponible en:

https://www.samuelparra.com/2017/09/04/la-casilla-premarcada-de-whatsapp-para-ceder-datos-a-facebook-es-legal/

Bonneau, J.; Preibusch, S. 2009. The Privacy Jungle: On the Market for Data Protection in Social Networks. *The Eighth Workshop on the Economics of Information Security.* University of Cambridge.

Boyd, D. 2004. Friendster and Publicly Articulated Social Networking. *Conference on Human Factors and Computing Systems (CHI 2004)*. Viena.

Boyd, D. 2008. Taken out of context: American teen sociality in networked publics. *Ph.D. thesis.* University of California, Berkeley.

Cámara de Comercio de EE.UU. en España. 2016. Privacy Shield y el impacto de la privacidad y la ciberseguridad en las relaciones transatlánticas. Madrid.

Centro de Investigaciónes Sociológicas (CIS). *Barómetro de Febrero 2017.* Estudio núm. 3168. Disponible en: "http://www.cis.es/cis/export/sites/default/-Archivos/Marginales/3160_3179/3168/es3168mar.pdf%20"

Comisión Europea. Comunicado de Prensa. *La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos.* Bruselas, 12 de Julio de 2016. Disponible en: "http://europa.eu/rapid/press-release_IP-16-2461_es.htm"

Cranor, L.; Dobbs, B.; Egelman, S., 2006. The platform for privacy preferences 1.1 (P3P1.1) specification. Disponible en: "https://www.w3.org/TR/P3P11/"

Debatin, B.; Lovejoy, J.P.; Horn, A.K.; Hughes, B.N. 2009. Facebook and online privacy: attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, Vol. 15(1), pp. 83–108.

DiMicco, J.M.; Millen, D.R. 2007. Identity management: multiple presentations of self in Facebook. *Proceedings of the international ACM conference on supporting group work*, pp. 383-386. Florida, EEUU.

Dix, A. 2010. Daten- und Personlichkeitsschutz im Web 2.0. *Netzwelt - Wege, Werte, Wandel.* Berlín : Springer, pp. 195-210.

Donath, J.; Boyd, D. 2004. Public Displays of Connection. *BT Technology Journal*, Vol. 22 (4), pp. 71–82.

EL MUNDO. [Consultado el: 1 de Septiembre de 2017]. Disponible en: "http://www.elmundo.es/economia/2017/02/01/589266c622601d790e8b45b7.html"

España. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). *Boletín Oficial del Estado,* 12 de Julio de 2002, núm. 166, pp. 25388 a 25403.

FACEBOOK APP. [Consultado en Septiembre de 2017]

FACEBOOK. Página principal. [Consultado en Agosto de 2017]. Disponible en: "http://www.facebook.com"

FACEBOOK. Política de Privacidad. [Consultado el: 3 de Agosto de 2017]. Disponible en: "https://www.facebook.com/privacy/explanation"

García, C. 2003. El derecho a la intimidad y dignidad del Tribunal Constitucional. Universidad de Murcia. (ed.): *Colección Estudios de Derecho*. ISBN-9788483713969.

Goffman, E. 1959. *Presentation of Self in Everyday Life*. New York : Anchor Books.

GOOGLE. Política de Privacidad de YouTube. Actualizado 17 de Abril de 2017. [Consultado el: 18 Septiembre 2017]. Disponible en: "https://www.google.com/policies/privacy/?hl=es-419"

Guha, S.; Tang, K.; Francis, P. 2008. NOYB: Privacy in Online Social Networks. *Proceedings of the 1st workshop on online social networks*, pp. 49-54. Seattle (WA), Estados Unidos.

Hans, G.S. 2012. Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era. *Michigan Telecommunications and Technology Law Review*, University of Michigan Law School, Vol. 19.

IAB Spain y Elogia. *Estudio Anual de Redes Sociales.* 2017. Disponible en: "http://iabspain.es/wp-content/uploads/iab_estudioredessociales_2017_vreducida.pdf"

Instituto Nacional de Tecnología de la Comunicación (INTECO). 2008. *Redes sociales, menores de edad y privacidad en la red.* Área Jurídica de la Seguridad y las TIC, Observatorio de la seguridad de la información.

Instituto Nacional de Tecnologías de la Comunicas (INTECO) y Agencia Española de Protección de Datos (AEPD). 2009. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online.*

Islam, M.B.; Iannella, R., 2010. Privacy by Design: Does It Matter For Social Networks? *IFIP Advances in Information and Communication Technology,* vol. 375.

Kim, N. 2014 *T*hree's A Crowd: Towards Contextual Integrity In Third-Party Data Sharing. *Harvard Journal of Law & Technology*, Vol. 28, No. 1.

Kolter, J.; Netter, M.; Pernul, G. 2010. Visualizing past personal data disclosures. *Proceedings of the fifth international conference on availability, reliability and security*. Cracovia, Polonia.

Lampinen, A.; Tamminen, S.; Oulasvirta, A. 2009. All my people right here, right now: management of group co-presence on a social networking site.

Proceedings of the ACM 2009 international conference on Supporting group work, pp. 281-290. Florida, Estados Unidos.

Leenes, R. E., 2010. Context is Everything - Sociality and Privacy in Online Social Network Sites. *Privacy and identity*, pp. 48-65, Disponible en: "https://ssrn.com/abstract=1706295" https://ssrn.com/abstract=1706295 .

MASHABLE. Actualizado 2015. [Consultado: 2 Septiembre 2017.] Disponible en:"http://mashable.com/2015/10/12/google-mobile-searches/%23EZtu.Dmkvuqw"

Milt, K. Junio 2017. Fichas Técnicas sobre la Unión Europea (La protección de datos personales). Unión Europea. Disponible en: "http://www.europarl.europa.eu/ftu/pdf/es/FTU_5.12.8.pdf"

Organización para la Cooperación y el Desarrollo Económicos (OCDE). 1981. *Guidelines on the protection of privacy and transborder flows of personal data, vol 11.* París.

Patil, S.; Kobsa, A. 2004. *The Challenges in Preserving Privacy in Awareness Systems.* School of Information and Computer Science. University of California, Irvine.

Patil, S.; Kobsa, A. 2009. Privacy considerations in awareness systems: designing with privacy in mind. *Awareness Systems. Human-Computer Interaction Series*. Londres : Springer.

Privacy Shield Framework. [Consultado el: 3 de Septiembre de 2017]. Disponible en: "https://www.privacyshield.gov/participant_search"

Rosenberg, M. 2016. The Price of Privacy: How access to digital privacy is slowly becoming divided by class*. UCLA Journal of Law & Technology*, Vol. 20.

Strahilevitz, L. 2005. A Social Networks Theory of Privacy. *University of Chicago Law & Economics, Olin Working Paper No. 230 and Public Law Working Paper No. 79*. Disponible en: "https://ssrn.com/abstract=629283".

THE GUARDIAN. Actualizado: 3 de Julio de 2017. [Consultado el: 3 de Septiembre de 2017]. Disponible en: "https://www.theguardian.com/technology/2017/jul/03/facebook-track-browsing-history-california-lawsuit"

THOMSON REUTERS. [Consultado: 6 de Septiembre de 2017]. Disponible en: "http://www.reuters.com/article/us-eu-facebook-antitrust/eu-fines-facebook-110-million-euros-over-whatsapp-deal-idUSKCN18E0LA"

Unión Europea. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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. *Diario Oficial de la Unión Europea L 281,* 23 de noviembre de 1995, pp. 31-50.

Unión Europea. Reglamento (UE) no 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016, 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*, 4 de Mayo de 2016, pp. 1-88.

Unión Europea. Tribunal de Justicia de la Unión Europea. Caso *Verein für Konsumenteninformation contra Amazon EU Sàrl (*C-191/15). Sala Tercera, Sentencia de 28 Julio 2016.

Unión Europea. Tribunal de Justicia de la Unión Europea. Petición de decisión prejudicial planteada por la High Court (Irlanda). Caso Maximillian Schrems y Data Protection Commissioner (C-362/14). Sentencia de 6 Octubre 2015.

Warren, S.; Brandeis, L.D. 1890 The Right to Privacy*. Harvard Law Review*, vol. 4, núm 5.

wearesocial and hootsuite. *Three billion people now use social media.* 2017. Disponible en: "https://wearesocial.com/blog/2017/08/three-billion-people-now-use-social-media".

WHATSAPP. Página Principal. [Consultado el: 6 de Septiembre de 2017]. Disponible en: "https://www.whatsapp.com"

WHATSAPP APP. [Consultado el: 5 de Septiembre de 2017].

WIKIPEDIA. *List of Mergers and Acquisitions by Alphabet.* Disponible en: "https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet%23cite_note-1."

YOUTUBE. Página Principal. [Consultado: 16 Septiembre 2017.] Disponible en: "https://www.youtube.com".

YOUTUBE APP. Actualizada el 16 de Septiembre de 2017*.* [Consultado: 17 Septiembre 2017.]

Ziegele, M., Quiring, O. 2011. Privacy in social network sites. *Privacy online. Perspectives on privacy and self-disclosure in the social web.* Heidelberg/New York : Springer, pp. 175-189.