InDret
3.2020

Identidad, cesión de datos personales y la decisión *Privacy Shield* tras la STJUE *Schrems II*[*]

Ignacio García-Perrote Martínez
Universitat Pompeu Fabra
ignacio.garciaperrote@upf.edu

Tomás Gabriel García-Micó
Universitat Pompeu Fabra
tomasgabriel.garcia@upf.edu
-

1. Introducción

Este trabajo tiene por objeto la regulación de la identidad de la persona[1] en los códigos de conducta de las redes sociales más utilizadas. El concepto de identidad es tratado de conformidad con el derecho vigente: el artículo 53 de la Ley de 8 de junio de 1957 sobre el Registro Civil[2], en el caso de las personas físicas; y el artículo 38.2 del Real Decreto 1784/1996, de 19 de julio, por el que se aprueba el Reglamento del Registro Mercantil[3], para las personas jurídicas.

En este sentido, es bien conocido que las redes sociales ceden los datos personales (entre ellos, la identidad) de sus usuarios a otras empresas con las que colaboran comercialmente.

[*] Los autores son miembros del Grupo de Investigación en Derecho Patrimonial (2017 SGR 1636), dirigido por el Prof. Josep Ferrer Riba (Universitat Pompeu Fabra) financiado por la Agencia de Gestión de Ayudas Universitarias y de Investigación (AGAUR), adscrita a la Secretaría de Universidades e Investigación del Departamento de Empresa y Conocimiento de la Generalitat de Catalunya.

Los autores, a su vez, son titulares de una beca para la contratación de personal investigador novel (FI-2020), concedida por el AGAUR en un proceso abierto y competitivo y cofinanciado por el Programa Operativo de Cataluña 2014-2020 CCI 2014ES05SFOP007 del Fondo Social Europeo.

El trabajo se enmarca en la ejecución del Proyecto de I+D+I correspondiente al Programa Estatal de Investigación, Desarrollo e Innovación orientada a los Retos de la sociedad "Responsabilidad civil y mercado. La compensación del daño económico", del cual es investigador principal el Prof. Carlos Ignacio Gómez Ligüerre, subvencionado por el Ministerio de Ciencia, Innovación y Universidades y el FEDER (DER2017-82673-R).

This publication was funded by the European Union's Justice Programme (2014-2020) under the grant agreement No 807056.

[1] La identidad es considerada un "dato personal" al amparo del artículo 4.1 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos): "A efectos del presente Reglamento se entenderá por: 1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre [...] un identificador en línea [...]".

[2] "Las personas son designadas por su nombre y apellidos [...]".

[3] "2. Tratándose de personas jurídicas se indicará: 1.º La razón social o denominación".

No obstante, cuando estos datos se ceden a empresas sitas en terceros estados surge un importante obstáculo: la garantía de una protección suficiente de los datos personales de los usuarios europeos frente a las actividades de tratamiento que puedan llevar a cabo las empresas y autoridades de estos terceros estados. El caso más reciente lo encontramos en la sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 (asunto C-311/18, *Schrems II*), en cuya virtud se declaró inválida la Decisión (UE) 2016/1250 de la Comisión Europea sobre la adecuación de la protección conferida por el Escudo de privacidad UE-EE.UU (*Privacy Shield*) y que, en consecuencia, dejó sin amparo legal tales transferencias de datos personales.

2. La sentencia del TJUE en el asunto C-311/18 (*Schrems II*) y la cesión de datos a países terceros. La invalidez de la Decisión *Privacy Shield*

El pasado 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea dictó la sentencia del asunto C-311/18 (*Schrems II*). En el caso se discutía la conformidad de la Decisión (UE) 2016/1250 de la Comisión Europea sobre la adecuación de la protección conferida por el Escudo de privacidad UE-EE.UU (*Privacy Shield*) con el Derecho de la Unión.

2.1. Resumen de los antecedentes del litigio principal y *Schrems I*

El 25 de junio de 2013, el Sr. Schrems – ciudadano de nacionalidad austríaca y usuario de Facebook – presentó ante el *Data Protection Commissioner* de Irlanda una reclamación en virtud de la cual solicitaba que se suspendiera la transferencia de sus datos personales efectuada por *Facebook Ireland* a su matriz (*Facebook Inc.*), establecida en los Estados Unidos, donde eran objeto de tratamiento. Según el Sr. Schrems, dicho tratamiento no garantizaba una protección suficiente frente a las actividades de vigilancia de las autoridades públicas de los Estados Unidos (la *National Security Administration* y el *Federal Bureau of Investigation*, principalmente) fundamentadas en la § 702 de la *Foreign Intelligence Surveillance Act* (50 U.S.C. § 1881a)[4] y la Orden Ejecutiva 12333, de 4 de diciembre de 1981, sobre las actividades de inteligencia de los Estados Unidos (*Executive Order 12333: United States Intelligence Activities*)[5].

Dicha reclamación fue desestimada por el *Data Protection Commissioner* de Irlanda alegando que los Estados Unidos ofrecían un nivel adecuado de protección, tal como había declarado anteriormente la Comisión Europea en su Decisión 2000/520, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (la "Decisión *Safe Harbour*").

[4] Véase: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title50-section1881a&num=0&edition=prelim

[5] Véase: https://www.archives.gov/federal-register/codification/executive-order/12333.html. La Orden Ejecutiva 12333 fue objeto de dos reformas posteriores, operadas por las Órdenes Ejecutivas 13355 (*Strengthened Management of the Intelligence Community*), de 27 de agosto de 2004; y 13470, de 30 de julio de 2008.

Frente a la decisión[6] del *Data Protection Commissioner* de Irlanda, el Sr. Schrems planteó recurso ante la *High Court* de Irlanda, la cual elevó una cuestión prejudicial al TJUE que fue resuelta mediante sentencia de 6 de octubre de 2015 (asunto C-362/14, *Schrems I*), declarando la invalidez de la Decisión *Safe Harbour*.

En el litigio principal, y en línea con la STJUE *Schrems I*, la *High Court* de Irlanda estimó el recurso del Sr. Schrems, revocó la decisión del *Data Protection Commissioner* de Irlanda y se la retornó. Durante la investigación llevada a cabo por el *Data Protection Commissioner* de Irlanda tras la devolución de la decisión, *Facebook Ireland* alegó que las transferencias de datos efectuadas se amparaban en cláusulas contractuales tipo reguladas en la Decisión (UE) 2010/87 de la Comisión, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países (la "Decisión CPT"). Tras terminar la investigación, el *Data Protection Commissioner* de Irlanda instó al Sr. Schrems a presentar una reclamación modificada.

El 1 de diciembre de 2015 el Sr. Schrems presentó la nueva reclamación alegando que el Derecho de los Estados Unidos obligaba a *Facebook Inc.* a poner a disposición de las autoridades de seguridad nacional los datos personales recibidos por esta última. A su vez, dichas autoridades utilizaban los datos personales en el marco de sus programas de vigilancia. El uso de datos personales para la finalidad expuesta anteriormente, en opinión del Sr. Schrems, era incompatible con los artículos 7[7], 8[8] – por ser el tratamiento de los datos personales de los usuarios de Facebook excesivo y contrario a la finalidad perseguida por dichos preceptos de la Carta – y 47[9] de la Carta de los Derechos Fundamentales de la Unión Europea, por no dotarse a los ciudadanos de la Unión Europea de una vía efectiva de recurso ante una autoridad imparcial. Asimismo, arguyó, la utilización de cláusulas contractuales tipo – amparadas por la decisión CPT – por sí sola, no subsanaba la infracción denunciada. Como consecuencia de lo anterior, el Sr. Schrems solicitaba al Comisario que suspendiera o prohibiese la transferencia de sus datos personales a *Facebook Inc.*

El 24 de mayo de 2016, el *Data Protection Commissioner* de Irlanda emitió un proyecto de decisión en el cual resumía las conclusiones provisionales de su investigación y, en lo sustancial, acogía la argumentación del Sr. Schrems. Ante ello, el *Data Protection Commissioner* de Irlanda inició un procedimiento ante la *High Court* de Irlanda, con el fin de que este Tribunal valorase la conveniencia de plantear una cuestión prejudicial al TJUE que tuviese por objeto la

---

[6] Para más información sobre los antecedentes del procedimiento en Irlanda, véase: https://www.dataprotection.ie/en/legal/explanatory-memoranda-litigation-concerning-standard-contractual-clauses-sccs#background.

[7] Artículo 7. Respeto de la vida privada y familiar: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

[8] Artículo 8. Protección de datos de carácter personal: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[9] Artículo 47. Derecho a la tutela judicial efectiva y a un juez imparcial: "Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia".

validez de la Decisión CPT. La *High Court* de Irlanda, en fecha de 4 de mayo de 2018, elevó una petición de cuestión prejudicial[10], la cual daría lugar a la sentencia de 16 de julio de 2020.

2.2. La sentencia del TJUE de 16 de julio de 2020

La resolución declara la validez de la Decisión CPT. Sin embargo, considera que la Decisión *Privacy Shield* es inválida por los siguientes motivos:

- En primer lugar, la normativa estadounidense sobre acceso y utilización de datos personales con fines relacionados con la seguridad nacional a través de programas de vigilancia[11] infringe el principio de proporcionalidad, pues no se limitan a lo estrictamente necesario. En particular, el Tribunal de Justicia considera que los ciudadanos de la UE no tienen, al amparo de la Decisión *Privacy Shield* y frente a las autoridades estadounidenses, un nivel de protección sustancialmente equivalente al que tienen en el marco del Reglamento General de Protección de Datos (RGPD)[12] (apartado 181).

  > A tal efecto, el TJUE se remite a la respuesta escrita ofrecida por las autoridades estadounidenses, según la cual "la PPD-28 no confiere a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales" (apartado 181) y, por ende, concluye que "esta [la Decisión *Privacy Shield*] no puede garantizar un nivel de protección sustancialmente equivalente al resultante de la Carta, contrariamente a lo que exige el artículo 45, apartado 2, letra a), del RGPD, según el cual la constatación de dicho nivel de protección depende, en particular, de la existencia de derechos efectivos y exigibles que sean reconocidos a los interesados cuyos datos personales hayan sido transferidos al país tercero de que se trate" (apartado 181).

- En segundo lugar, la Decisión *Privacy Shield* infringe el derecho a la tutela judicial efectiva reconocido en el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea, ya que la figura del Defensor del Pueblo que se nombraba en la Decisión *Privacy Shield* y con la que "los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al garantizado en el artículo 47 de la Carta" (apartado 193).

  > Considera el TJUE que el Defensor del Pueblo americano es una autoridad nombrada por el Secretario de Estado e incardinada en el Departamento de Estado, por lo que la exigencia, que emana de la Carta, de que los ciudadanos tengan la posibilidad de ejercer "acciones en Derecho ante un tribunal independiente e imparcial" (apartado 194) no estaría asegurada. Citando las propias palabras del TJUE: "no existe, en la referida Decisión, [...] ninguna indicación de que la destitución del defensor del pueblo o la anulación de su nombramiento vengan acompañadas de garantías específicas, lo que pone en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo" (apartado 195).

---

[10] Una lectura de las preguntas 1 a 11 de la cuestión prejudicial formulada por la *High Court* al TJUE (apartado 68) permite observar que el análisis de la validez de la Decisión CPT incluye, además, la Decisión *Privacy Shield*.

[11] Véanse las notas al pie 15 y 16.

[12] 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, OJ L 119, 4.5.2016, p. 1–88.

> Además, el TJUE afirma que "dicha Decisión no contiene ninguna indicación de que dicho defensor del pueblo esté facultado para adoptar decisiones vinculantes con respecto a esos servicios ni tampoco menciona ninguna garantía legal que acompañe a ese compromiso y pueda ser invocada por los interesados" (apartado 196).

2.3. Las implicaciones de la STJUE *Schrems II*

El pasado 24 de julio de 2020, el Comité Europeo de Protección de Datos (*European Data Protection Board* o "EDPB") publicó un documento titulado *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*[13].

La pregunta 4 del documento trata sobre las concretas implicaciones de la sentencia en la transferencia de datos al amparo de la decisión *Privacy Shield* desde un proveedor europeo a un proveedor de los Estados Unidos. En concreto, según el EDPB, dichas transferencias son ilegales con carácter general.

Tras ver cómo la STJUE *Schrems II* ha causado un cambio tan imporante en el paradigma de la regulación de las relaciones de cesión de datos entre empresas situadas en alguno de los Estados Miembro de la UE a otras sitas en terceros estados (en este caso, los Estados Unidos), conviene analizar con mayor detenimiento cómo los códigos privados de conducta de las redes sociales regulan la identidad de sus usuarios y, a su vez, cuál es su política de cesión de datos[14].

3. Twitter

3.1. Protección de la identidad

Las reglas de Twitter[15] que rigen las relaciones entre los usuarios y la red social se basan en cinco pilares: seguridad, privacidad, autenticidad, control de cumplimiento y apelaciones, y publicidad de terceros en contenidos de vídeo.

En lo que respecta a la identidad, las reglas de "Autenticidad" prohíben suplantar la identidad del usuario:

- En primer lugar, los usuarios se comprometen a no crear cuentas "en las que se finja ser otra persona, marca u organización". Es decir, los usuarios de Twitter deben emplear cuentas verídicas. No obstante, ello no implica que un usuario deba identificarse necesariamente con su nombre y apellidos según su propio derecho aplicable, pues puede emplear un seudónimo[16]. Pero esta regla conoce dos salvedades: Twitter permite cuentas de parodia o de grupos de admiradores, siempre que se ajusten escrupulosamente a los términos previstos por la red social[17].

---

[13] Se puede acceder al documento a través del siguiente enlace: https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[14] Los códigos de conducta de las redes sociales han sido consultados a fecha de la publicación de la presente nota y todavía no han incorporado cambio alguno tras la STJUE *Schrems II*.

[15] Véase: https://help.twitter.com/es/rules-and-policies/twitter-rules.

[16] Véase: https://twitter.com/es/privacy. Véase el apartado 1.1. "Información básica de la cuenta".

[17] Véase: https://help.twitter.com/es/rules-and-policies/parody-account-policy.

- En segundo lugar, hay suplantación si y solo si el usuario actúa con una intención que puede calificarse como maliciosa – dolosa – pues, dichos perfiles deben tener por objeto "confundir o engañar".

- En tercer lugar, Twitter puede proceder a la suspensión permanente de la cuenta, si media una denuncia de la persona afectada pues, según Twitter, "[r]evisamos los reclamos de suplantación de identidad cuando recibimos una denuncia válida" pero, bajo ningún concepto "monitoreamos activamente el contenido de los usuarios"[18].

3.2. Cesión de datos a terceros[19]

Twitter distingue dos supuestos:

- Aquellos en los cuales el usuario mismo recibe servicios de terceros y les ofrece los datos de su cuenta de Twitter, autorizándole a emplearlos; y

- Aquellos en los que Twitter, en el marco de sus relaciones comerciales, cede los datos de sus usuarios a terceros.

El supuesto problemático es el segundo.

El usuario no puede excluir la cesión de datos, sino que únicamente puede limitar su alcance, mediante la opción "Permitir el intercambio de información adicional con socios comerciales". La limitación no incluye, por ejemplo, a los proveedores de servicios domiciliados en los Estados Unidos, Irlanda y otros países (que la compañía no especifica), siempre con arreglo a la política de privacidad.

4. YouTube

YouTube, desde 2006 integrada dentro de Google[20], prohíbe que una persona pueda hacerse pasar por otra distinta, si ello genera confusión[21]. A diferencia de lo que sucedía con Twitter, no se requiere dolo, basta con la simple causación de confusión sobre la identidad de la persona creadora del contenido.

YouTube distingue entre suplantación de canal y suplantación de personalidad en sentido estricto:

- Hay suplantación de canal si un canal reproduce el perfil, las características visuales o cualquier otra información o forma de presentación de otro de modo que el primero (el perfil que suplanta) aparece como una copia exacta del segundo (el perfil suplantado).

---

[18] Véase: https://help.twitter.com/es/rules-and-policies/twitter-impersonation-policy. Véase el apartado "¿En qué circunstancias Twitter revisa las cuentas para asegurar el cumplimiento de esta política?".

[19] Véase: https://twitter.com/es/privacy. Véase el apartado 3. "Información que compartimos y revelamos".

[20] Véase Paul R. LA MONICA, *Google to buy YouTube for $1.65 billion*, CNN Money, October 9 2006: https://money.cnn.com/2006/10/09/technology/googleyoutube_deal/.

[21] Véase: https://support.google.com/youtube/answer/2801947.

- Hay suplantación en sentido estricto si se genera la apariencia de que los contenidos publicados han lo han sido por otra persona.

Mas, como en el caso de Twitter, YouTube no exige a sus usuarios emplear un perfil que revele su identidad personal, pues permite emplear seudónimos siempre y cuando no incurran en uno de los supuestos prohibidos por su política de suplantación de personalidad.

La cesión de datos de YouTube se basa en la política de privacidad de Google[22]: como regla general, los datos se podrán ceder con el consentimiento del usuario. No obstante, hay algunos supuestos en los que se ceden datos con los administradores de dominio, para procesamiento externo y, por último, por motivos legales:

- Cumplir con cualquier requisito previsto en la legislación aplicable, o atender cualquier requerimiento de un órgano administrativo o judicial[23].

- Hacer cumplir las condiciones de servicio aplicables, incluida la investigación de posibles infracciones.

- Detectar, prevenir o solucionar cualquier fraude o incidencia técnica o de seguridad.

- Proteger los derechos, los bienes o la seguridad de Google, de sus usuarios o del público en general de la manera que lo exige o lo permite la legislación aplicable.

5. Facebook

El punto de partida de la política relativa a la identidad de los usuarios de Facebook es la autenticidad: la compañía exige que los usuarios se registren e identifiquen con su nombre real (según el derecho aplicable a su identidad personal).

La política de suplantación de Facebook incluye tres categorías de conductas prohibidas[24]:

- Primero, la falsificación de la identidad mediante el uso de un nombre diferente al utilizado por el usuario en su vida diaria[25] y, también, la inexactitud de la fecha de nacimiento.

- Segundo, el uso indebido de su red social, sea ya por registrarse antes de haber cumplido la edad de 14 años, por utilizar varias cuentas, por compartir una cuenta con otras personas o por crear perfiles no auténticos u otras cuentas reales si al usuario se le ha prohibido el uso de la red social por algún motivo.

- Tercero, la suplantación en sentido estricto:

---

[22] Véase: https://policies.google.com/privacy?hl=en#infosharing.

[23] En el Informe de Transparencia (https://transparencyreport.google.com/user-data/overview?hl=ca), Google comparte la información sobre el nombre y tipo de solicitudes y requerimientos recibidos.

[24] Véase: https://www.facebook.com/communitystandards/misrepresentation.

[25] Sobre la política de nombres de Facebook, véase https://www.facebook.com/help/112146705538576?ref=ccs.

- (i) Uso malicioso de la imagen de una persona con finalidades de engañar a terceros usuarios

- (ii) Creación de perfiles o páginas mediante las cuales el usuario se apropie la identidad de un tercero, y;

- (iii) Publicación de imágenes que lleven a engaño en cuanto al origen del contenido si media oposición de la entidad afectada o si puede causar daños al público.

Según la política de cesión de datos de Facebook, la red social colabora con operadores económicos con el fin de mejorar sus propios productos. En ningún caso, afirma, vende los datos personales de sus usuarios y, además, impone restricciones estrictas sobre cómo pueden los operadores económicos con los que colabora utilizar y divulgar los datos de los usuarios[26]:

- A los socios que emplean los servicios de análisis, les proporcionan el número de personas o cuentas que han visto, reaccionado o comentado publicaciones, así como información demográfica agregada.

- A los anunciantes, les proporcionan informes sobre el tipo de personas que ven sus anuncios y qué rendimiento tiene su publicidad, sin compartir información identificativa (nombre y dirección de correo electrónico, en particular) de los usuarios.

- Con los socios de que ofrecen bienes y servicios en los productos de la red social comparten la información pública y otra información compartida por el usuario, así como los datos de envío y de contacto.

- Con los investigadores y académicos comparten información con el fin de colaborar en la formación e innovación que apoye la misión de Facebook, así como a la mejora del descubrimiento y la innovación en cuestiones ligadas al bienestar social general, el avance tecnológico, la salud y el bienestar públicos.

Con el fin de dar cumplimiento a los requerimientos legales, Facebook puede compartir con las autoridades – en el marco de un requerimiento u obligación judicial, una investigación gubernamental, o investigación de posibles infracciones de los términos y condiciones de Facebook – los datos de sus usuarios, incluidos los relativos a las transacciones financieras relacionadas con compras realizadas con Facebook.

6. Instagram

La política de suplantación de personalidad de Instagram, integrada dentro de Facebook prohíbe a los usuarios:

- Hacerse pasar por otras personas.

[26] Véase: https://es-es.facebook.com/privacy/explanation.

- Crear cuentas con la finalidad de infringir las normas comunitarias o engañar a los otros usuarios.

La red permite que sus usuarios utilicen seudónimos o se den a conocer mediante nombres diferentes al suyo propio siempre que no incumplan las prohibiciones anteriores. Ahora bien, Instagram requiere a los usuarios que proporcionen información correcta y actualizada[27].

Como Instagram está integrada en Facebook, ambas plataformas tienen la misma política de cesión de datos[28], a la cual nos remitimos. pues ya ha sido expuesta anteriormente.

7. TikTok

TikTok prohíbe a los usuarios suplantar dolosamente a terceras personas u organizaciones, es decir, con finalidades de engañar al público.

Ahora bien, si el usuario no persigue engañar al público sobre su identidad o sobre la finalidad de su perfil en la red social, la red permite la existencia de cuentas que parodien a personas o sean cuentas de seguidores (*fan accounts*)[29].

Según la política de privacidad de TikTok, la plataforma comparte los datos de sus usuarios con otros proveedores de servicios, tanto internos como externos, para mejorar sus productos. A diferencia de Facebook – e Instagram, por extensión –, TikTok aclara que puede vender los datos de sus usuarios, es decir, operar con fines lucrativos[30].

[27] Segundo párrafo del apartado "Fomenta las interacciones relevantes y genuinas":
https://help.instagram.com/477434105621119/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad.

[28] Véase:
https://help.instagram.com/519522125107875/?helpref=hc_fnav&bc[0]=Ayuda%20de%20Instagram&bc[1]=Centro%20de%20privacidad%20y%20seguridad.

[29] Apartado "Integridad y autenticidad" de las Normas de la comunidad, que pueden encontrarse aquí: https://www.tiktok.com/community-guidelines?lang=es.

[30] Véase: https://www.tiktok.com/legal/privacy-policy?lang=es.