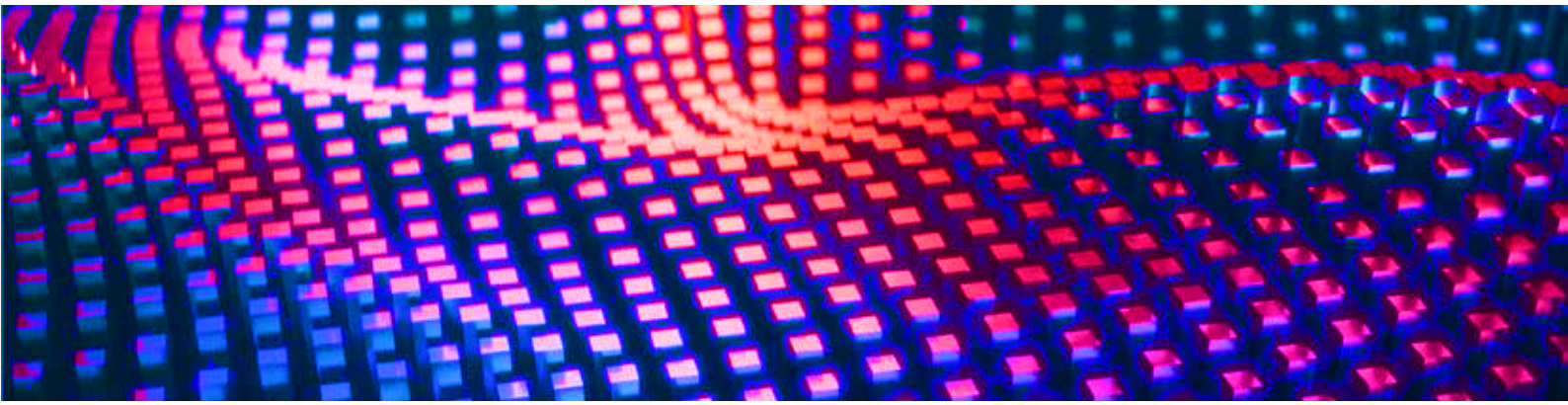
G A _ P

Gómez-Acebo & Pombo



Derecho Digital

2024 N.º 12

Contenido

Protección de datos personales en el ámbito digital

Los modelos de «consentimiento o pago»: Dictamen 08/2024 sobre el consentimiento válido en el contexto de los modelos de consentimiento o pago aplicados por las grandes plataformas en línea

El 17 de abril del 2024, el Comité Europeo de Protección de Datos (CEPD) emitió un dictamen sobre la validez del consentimiento para el tratamiento de datos personales con fines de publicidad comportamental en los modelos de «consentimiento o pago» utilizados por grandes plataformas en línea, a raíz de solicitudes de autoridades neerlandesas, noruegas y alemanas. El dictamen considera la Sentencia del Tribunal de Justicia de la Unión Europea de 4 de julio del 2023 en el asunto *Meta Platforms*.

A este respecto, el supervisor europeo de Protección de Datos (SEPD) enfatiza la necesidad de cumplir los requisitos de consentimiento válido según el Reglamento General de protección de datos (RGPD), enfocándose en los principios de necesidad, proporcionalidad, limitación de la finalidad y minimización de datos. El Comité Europeo de Protección de Datos señala que los modelos que ofrecen una elección binaria entre aceptar el tratamiento de datos o pagar una tarifa no cumplen con estos requisitos. Según Anu Talus, presidente de dicho comité, las plataformas deben proporcionar una alternativa genuina que no dependa del pago.

El comité propone que las plataformas ofrezcan una opción gratuita que implique menos tratamiento de datos personales o ninguno. Además, subraya que el consentimiento debe ser dado libremente y que imponer un pago como única alternativa no cumple este requisito, ya que priva a los usuarios de control sobre su información. Adicionalmente, se ha de apreciar si existe un desequilibrio de poder entre el usuario y la plataforma, considerando factores como la posición de la plataforma en el mercado y la dependencia del usuario del servicio.

En definitiva, el dictamen destaca la necesidad de que las grandes plataformas en línea garan-

ticen una alternativa accesible que no implique de forma taxativa el pago de una tasa.

Iratze Arrigain García

Nueva regulación de los *influencers*

El 1 de mayo se publicó el Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado *usuario de especial relevancia* de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, General de Comunicación Audiovisual («Real Decreto de usuarios de especial relevancia»), el cual incorpora la Directiva (UE) 2018/1808 al marco jurídico español adaptando la normativa al mercado audiovisual en constante evolución.

El real decreto se aplica a usuarios de servicios de intercambio de vídeos o contenido publicitario que cumplan los requisitos del artículo 94.2 de la Ley 13/2022, excluyendo a prestadores de servicios de comunicación audiovisual registrados y otros sujetos tipificados en el artículo 94.3 de dicha ley. Esto incluye a los *vloggers*, *influencers* y *creadores de contenido*, los cuales tendrán obligaciones similares a las de los prestadores de servicios de comunicación audiovisual para asegurar el respeto de los principios básicos de comunicación y la protección del público.

Los requisitos para ser considerado *usuario de especial relevancia* son los siguientes:

a) Ingresos significativos: ingresos anuales brutos de al menos trescientos mil euros derivados exclusivamente de su actividad en plataformas de intercambio de vídeos.

b) Audiencia significativa: tener al menos un millón de seguidores en una plataforma o dos millones en varias.

c) Y número de publicaciones: haber publicado al menos veinticuatro vídeos en el año anterior.

Las principales obligaciones nacen con el objetivo claro de proteger a los menores adoptando medidas para salvaguardar su integridad moral y física y de cumplir las normativas de comunicaciones comerciales audiovisuales. Además, los usuarios de especial relevancia deben inscribirse en el Registro estatal, lo que implica una carga administrativa adicional.

Claudia Pérez Moneu

Nuevas designaciones de guardianes de acceso

Como es notorio, el Reglamento de mercados digitales [Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre, sobre mercados disputables y equitativos en el sector digital] se aplica a los servicios básicos de plataforma prestados u ofrecidos por guardianes de acceso a usuarios profesionales establecidos en la Unión o a usuarios finales establecidos o situados en la Unión, independientemente del lugar de establecimiento o residencia de los guardianes de acceso. Resulta, por tanto, crucial la determinación de los sujetos que tienen la consideración legal de guardianes de acceso. Y a tal efecto es la Comisión Europea la que designa a una determinada empresa como guardián de acceso, para lo cual es preciso que ésta tenga una gran influencia en el mercado interior, que preste un servicio básico de plataforma que sea una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales y que tenga una posición afianzada y duradera por lo que respecta a sus operaciones o que sea previsible que la alcance en un futuro próximo.

Pues bien, después de que la Comisión Europea hubiera designado en septiembre del 2023 seis guardianes de acceso (Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft, en relación con diferentes servicios básicos de plataforma), en mayo del 2024 nombró a Booking guardián de acceso para su servicio de intermediación en línea Booking.com, a la par que declaró estar examinando el servicio de la red social en línea X.

Ángel García Vidal

Uso de sistemas de reconocimiento facial en aeropuertos

El Comité Europeo de Protección de Datos (CEPD) ha emitido un dictamen sobre el uso de sistemas de análisis biométricos (especialmente el reconocimiento facial) en los aeropuertos para agilizar el flujo de pasajeros en áreas clave como en los controles de seguridad y zonas de entrega de equipaje y de embarque. Este dictamen dio respuesta a la petición por parte de la autoridad francesa de protección de datos para determinar la conformidad de estos sistemas con los artículos 5.1*e* y *f*, 25 y 32 del Reglamento General de protección de datos (RGPD).

Los riesgos asociados con el uso del reconocimiento facial —incluidos falsos negativos, sesgos, discriminación y uso indebido de los datos biométricos— que podrían llevar a fraudes de identidad determinan que se implanten distintas salvaguardias como mecanismos para reducir sesgos en los algoritmos, asegurar la transparencia en el uso de los datos y evitar el almacenamiento de datos sin consentimiento.

Se distinguen dos funciones principales del reconocimiento facial: identificación (comparación de datos con una base de datos) y autenticación (verificación de una identidad registrada), ambas consideradas categorías especiales según el artículo 9 del Reglamento General de protección de datos. El dictamen evalúa varios escenarios para el almacenamiento y procesamiento de los datos biométricos:

— Almacenamiento en dispositivos individuales para autenticación, posiblemente compatible con el Reglamento General de protección de datos.

— Almacenamiento centralizado en el aeropuerto bajo control del operador, incompatible con dicho reglamento.

— Almacenamiento centralizado en la nube bajo control de la compañía aérea o del proveedor de servicios de la nube, incompatible con el citado reglamento.

En conclusión, el Comité Europeo de Protección de Datos enfatiza la necesidad de evaluar y regular rigurosamente la implantación de estos sistemas garantizando que el almacenamiento y el procesamiento de los datos minimicen riesgos y respeten los derechos fundamentales de los pasajeros.

Cristina Bonfanti Gris

Propiedad industrial e intelectual

Una autoridad nacional competente puede acceder a datos identificativos en virtud de una dirección IP en la lucha contra la infracción y vulneración de derechos de propiedad intelectual[1]

El Tribunal de Justicia de la Unión Europea resolvió, en su Sentencia de 30 de abril del 2024, asunto C-470/2, una cuestión prejudicial planteada en el contexto de un litigio ocurrido en Francia entre las asociaciones La Quadrature du Net, Fédération des Fournisseurs d´Accès à Internet Associatifs, Franciliens.net y French Data Network y el primer ministro y el Ministerio de Cultura de Francia en relación con la legalidad del Decreto núm. 2010\236, de 5 de marzo, relativo al tratamiento automatizado de datos personales autorizado por el artículo L331-29 del Código de Propiedad Intelectual francés.

El artículo en cuestión, que tiene como objetivo proteger las obras sujetas a derechos de autor o a derechos similares contra infracciones cometidas en línea, establece dos mecanismos para el tratamiento de los datos personales que permiten a la autoridad iniciar acciones sancionadoras contra las personas identificadas:

a) Organizaciones que representan a los autores recolectan las direcciones IP que parecen haberse usado en sitios de intercambio entre pares *(peer-to-peer)* para cometer estas infracciones y las envían a la Alta Autoridad Francesa para la Difusión de Obras y la Protección de Derechos en Internet (conocida como Hadopi).

b) Los proveedores de servicios de internet, a petición de la Hadopi, asocian la dirección IP con la identidad del titular de esa dirección.

[1] Sentencia del Tribunal de Justicia de la Unión Europea, asunto C-470/21, La Quadrature du Net y otros (Datos personales y lucha contra la vulneración de derechos de propiedad intelectual), de 30 de abril del 2024.

Ante la aprobación de esta norma, las asociaciones mencionadas decidieron presentar un recurso de anulación ante el Consejo de Estado francés. Para resolver el litigio, el órgano jurisdiccional competente planteó una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea sobre si los tratamientos de datos propuestos por el artículo eran conformes con el Derecho de la Unión Europea en materia de protección de datos.

En respuesta a esta cuestión prejudicial, el Tribunal de Justicia dictaminó que la legislación europea no prohíbe que una autoridad de un Estado miembro acceda a la dirección IP de una persona involucrada en una infracción de derechos de propiedad intelectual siempre y cuando se garantice que esta medida no permita obtener datos personales que se refieran a la vida privada del infractor. En la misma línea, el tribunal señala que no es necesario un control previo por parte de un órgano independiente para acceder a la dirección IP de estos sujetos, ya que no se produce una intromisión en los derechos fundamentales. Sin embargo, dicho control será necesario si la información obtenida permite obtener detalles específicos sobre la vida privada del individuo.

Iratze Arrigain García

Servicios de intermediación en línea

Obligaciones de información de los prestadores de servicios de intermediación en línea: un Estado miembro no tiene la facultad de imponer obligaciones adicionales a un proveedor de servicios en línea que esté establecido en otro Estado miembro[2]

El pasado 30 de mayo, el Tribunal de Justicia de la Unión Europa dictó cuatro sentencias en relación con una serie de medidas italianas destinadas a garantizar el cumplimiento del Reglamento 219/1150, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea.

Italia impuso en el 2021 varias obligaciones a proveedores de servicios de intermediación y motores de búsqueda en línea como Airbnb, Expedia, Google, Amazon y Vacation Rentals. Estas medidas, destinadas a cumplir el Reglamento 2019/1150, incluían el registro en un censo gestionado por la Autorità per le Garanzie nelle Comunicazioni (AGCOM), la presentación de informes económicos periódicos y el pago de una contribución económica, con sanciones por incumplimiento. Las compañías afectadas, excepto Expedia —domiciliada en EE. UU.—, presentaron recursos ante el Tribunal Regional de lo Contencioso-Administrativo del Lacio (Italia). Argumentaron que estas obligaciones contravenían el Derecho de la Unión Europea, ya que el régimen de los servicios en línea debe regirse por las leyes del Estado miembro donde están establecidas (Irlanda y Luxemburgo, en este caso). Italia, según ellos, no tenía competencia para imponer requisitos adicionales.

[2] Sentencias del Tribunal de Justicia de la Unión Europea en los asuntos acumulados C-662/22, *Airbnb Ireland,* y 667/22, *Amazon Services;* en C-663/22, *Expedia*; en C-664/22, *Google Ireland*; en C-666/22, *EG Vacation Rentals Ireland*, y en C-665/22, *Amazon Services Europe*.

El Tribunal de Justicia de la Unión Europea examinó la Directiva 2000/31/CE sobre el comercio electrónico, que establece que el Estado miembro de origen regula el régimen de servicios en línea. Los Estados miembros de destino deben respetar el principio de reconocimiento mutuo y no pueden imponer restricciones adicionales, salvo en las excepciones del artículo 3.4 de la directiva. El tribunal concluyó que Italia no podía imponer las obligaciones adicionales mencionadas. También determinó que las medidas italianas no cumplían las condiciones del artículo 3.4, ya que no eran necesarias para proteger el orden público, la salud pública o la defensa de los consumidores. Por lo tanto, no podían considerarse excepciones válidas.

Finalmente, es pertinente destacar la argumentación utilizada por el Tribunal de Justicia de la Unión Europea en el asunto C-663/22, que involucra a Expedia (domiciliada en Seattle, EE. UU.) y a la Autorità per le Garanzie nelle Comunicazioni. Esta argumentación es especialmente relevante, ya que Expedia no se beneficia del artículo 3.4 de la directiva al tratarse de una empresa de un tercer país. Para resolver esta cuestión prejudicial, el tribunal examinó si el Reglamento 2019/1150 impone restricciones a las medidas nacionales que pueden adoptarse para su cumplimiento. En este contexto, determinó que la recopilación de información mencionada en los artículos 16 y 18 del reglamento sólo está permitida si existe un «vínculo suficientemente directo con ese objetivo». Por lo tanto, concluyó que no es posible aplicar medidas como las impugnadas.

Claudia Pérez Moneu

Inteligencia artificial

Informe del Comité Europeo de Protección de Datos sobre ChatGPT

El informe presentado por el Comité Europeo de Protección de Datos (EDPB) analiza los aspectos más relevantes relacionados con el Reglamento General de protección de datos y el uso de modelos de lenguaje a gran escala (LLM) como ChatGPT de OpenAI. La peculiaridad de estos modelos reside en su método de aprendizaje, ya que los usuarios pueden entrenar dicha inteligencia artificial mediante la aportación de información, además de los datos accesibles para la herramienta en fuentes públicas. Así, al poder aportar datos de carácter personal, resulta indispensable asegurar que el tratamiento de los datos cumpla el Reglamento General de protección de datos. Si bien las autoridades competentes ya han empezado investigaciones que aún están en curso, el objetivo de este informe es ofrecer algunas opiniones preliminares relativas a dichas investigaciones.

En particular, respecto a la licitud del tratamiento, dicho tratamiento debe ampararse en alguna de las bases legitimadoras del artículo 6.1 del Reglamento General de protección de datos conjugándolo con las excepciones del artículo 9 del mismo cuerpo normativo. Asimismo, se señala la especial relevancia de diferenciar los distintos tipos de tratamiento involucrados en este caso: la recogida de datos para entrenar el chat, el pretratamiento de datos, el entrenamiento, los *prompts* (instrucciones introducidas en la herramienta para que dén lugar a un resultado) y el resultado.. Por otro lado, sobre el principio de transparencia, se pone de manifiesto que, al nutrirse la herramienta de datos provenientes de fuentes de acceso público, resulta difícil poder informar a todos los interesados, por lo que, en caso de que se cumplieran todos los requisitos, sería posible invocar la excepción prevista en el artículo 14.5*b* del reglamento. Por el contrario, si los datos se recaban a través de la interacción directa del usuario, el deber de información del artículo 13 del reglamento deberá cumplirse.

En cuanto al principio de exactitud, deben distinguirse dos escenarios: por un lado, los datos recabados de fuentes de acceso públicas o introducidos por el usuario (los cuales no tienen por qué ser exactos) y, por otro, los datos relativos al resultado emitido por la herramienta (sobre

el cual sí existe cierta expectativa de que sean exactos). No obstante, en cualquiera de los casos, debe cumplirse el principio de exactitud. Finalmente, el Comité Europeo de Protección de Datos recuerda los derechos de los interesados recogidos en el Reglamento General de protección de datos y la obligatoriedad de permitir su ejercicio.

Cristina Bonfanti Gris

Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho

Durante la 133.ª sesión del Comité de Ministros del Consejo de Europea, celebrada el 17 de mayo del 2024, se ha aprobado el Convenio Marco sobre Inteligencia Artificial (IA) y Derechos Humanos, Democracia y Estado de Derecho, que constituye el primer tratado internacional sobre la materia y al que pueden adherirse los Estados miembros del Consejo de Europa, los Estados miembros de la Unión Europea y cualquier otro Estado que haya participado en el proceso de elaboración (entre los que se encuentran los Estados Unidos, Japón o Canadá). Para que el convenio entre en vigor será necesaria la ratificación de al menos cinco Estados, de los cuales, tres al menos han de ser miembros del Consejo de Europa. Una vez que entre en vigor, podrá adherirse cualquier otro Estado distinto de los anteriores.

En el convenio se establecen como obligaciones principales de las partes la adopción o mantenimiento de medidas destinadas 1) a garantizar que las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial sean consistentes con las obligaciones de proteger los derechos humanos, según lo consagrado en el Derecho internacional aplicable y en su Derecho interno, y 2) a garantizar que los sistemas de inteligencia artificial no se utilicen para socavar la integridad, independencia y eficacia de las instituciones y procesos democráticos, incluidos el principio de separación de poderes, el respeto a la independencia judicial y el acceso a justicia, y 3) a proteger sus procesos democráticos en el contexto de las actividades dentro del ciclo de vida de los sistemas de inteligencia artificial, incluido el acceso equitativo de las personas al debate público y a su participación en él, así como su capacidad para formar opiniones libremente.

Ángel García Vidal

Directrices orientativas del supervisor europeo de Protección de Datos sobre el uso de sistemas de inteligencia artificial generativos y protección de datos

El supervisor europeo de Protección de Datos (EDPS) ha publicado sus primeras directrices orientativas para asegurar la protección de datos con el uso de sistemas de inteligencia artificial generativos, que cobran especial relevancia al ser él la autoridad supervisora designada por el Reglamento de inteligencia artificial.

Estas directrices están dirigidas a las instituciones, organismos y agencias de la Unión Europea (EUI) y hacen hincapié en la necesidad de cumplir las obligaciones de protección de datos establecidas en el Reglamento General de protección de datos. Los sistemas de inteligencia artificial generativa utilizan modelos de aprendizaje automático para proporcionar una respuesta utilizando un gran volumen de datos. Por lo tanto, deben asegurar que el tratamiento de los datos personales en estos sistemas se ampare en las bases legales adecuadas, como la obligación legal o el consentimiento explícito. Aunque el citado reglamento no menciona explícitamente la

inteligencia artificial, se subraya la importancia de aplicar correctamente los principios de protección de datos para evitar perjuicios relacionados con los derechos fundamentales de las personas.

Dichas directrices suponen una primera aproximación a diversas cuestiones relativas a la intersección entre la mencionada herramienta y los datos personales. Por ejemplo, se recalca la necesidad de que los datos utilizados por la inteligencia artificial generativa sean precisos, teniendo en cuenta el impacto que pueden tener en los derechos fundamentales de los interesados, por lo que se deberá atender a esta cuestión al considerar su uso. Además, las instituciones, organismos y agencias de la Unión Europea de la Unión Europea deben proporcionar a los interesados la información requerida por el Reglamento General de protección de datos cuando utilicen sistemas de inteligencia artificial generativa que traten datos personales y habrán de actualizar tal información según sea necesario. Asimismo, cuando los sistemas de inteligencia artificial generativa estén involucrados en procedimientos de toma de decisiones, dichas instituciones, organismos y agencias deben evaluar de forma cuidadosa su legalidad y asegurarse de que no conduzcan a decisiones injustas, éticamente cuestionables o discriminatorias.

Si bien se espera que las directrices se actualicen periódicamente, suponen un paso relevante hacia la regulación de la inteligencia artificial generativa y de su impacto en materia de protección de datos.

Claudia Pérez Moneu

Estrategia Nacional de Inteligencia Artificial en España

Recientemente se ha aprobado la Estrategia Nacional de Inteligencia Artificial (ENIA), que determina la ruta para consolidar la posición de España en el desarrollo y aplicación de la inteligencia artificial.

Así, se estudian los sectores en los que se espera un mayor impacto a corto plazo (por ejemplo, telecomunicaciones, servicios financieros, distribución o sanidad) y se propone la colaboración de las distintas Administraciones para impulsar la estrategia en línea con la regulación de la Unión Europea en materia de inteligencia artificial.

En el texto de esta propuesta se establecen siete objetivos: 1) excelencia científica e innovación en inteligencia artificial; 2) proyección de la lengua española mediante el desarrollo de tecnologías de inteligencia artificial; 3) creación de empleo cualificado y promoción de la educación y la formación; 4) transformación del tejido productivo integrando la inteligencia artificial para mejorar la productividad española; 5) entorno de confianza en relación con la inteligencia artificial; 6) valores humanistas en la inteligencia artificial: promover el debate global sobre el progreso tecnológico enfocado en salvaguardar el bienestar social durante los avances, y 7) inteligencia artificial inclusiva y sostenible, empleando sistemas para mitigar la brecha salarial y digital, así como para respaldar la transición ecológica.

Para dar cumplimiento a estos objetivos, la Estrategia Nacional de Inteligencia Artificial divide su plan de acción en seis ejes estratégicos, entre los que se encuentran el impulso a la investigación científica, la promoción del desarrollo de capacidades digitales, el desarrollo de plataformas de datos e infraestructuras que den soporte a la inteligencia artificial, la integración de ésta en las cadenas de valor, el impulso del uso de la inteligencia artificial en la Administración Pública y el establecimiento de un marco ético normativo que garantice los derechos de los individuos.

Finalmente, se indica que la Secretaría de Estado de Digitalización de Inteligencia Artificial, mediante los distintos instrumentos del Estado, coordinará las acciones necesarias para ejecutar esta estrategia. De igual modo, se pone de relieve que, para impulsarla, será fundamental la colaboración entre el sector público y el privado.

Cristina Bonfanti Gris

Redes sociales

Reputación de una empresa en una red social

El Tribunal Supremo (Sala de lo Civil) —en su Sentencia núm. 408/2024, de 20 de marzo (ECLI:ES:TS:2024:1579)— ha conocido de un interesante caso en el que una sociedad mercantil demandó al responsable de una red social (Facebook) por haberle cancelado la cuenta, lo que —entendía— era una vulneración de su derecho al honor. Argumentaba que la inhabilitación de la cuenta implicaba la desaparición de la empresa en la red social predominante y ello causaba su invisibilidad, con grave quebranto de su reputación y prestigio. Su imagen pública o «reputación *on-line*» resultaba dañada, especialmente porque el mensaje que aparece al buscar la cuenta en Facebook es «Cerrado permanentemente», junto con la denominación y la ubicación de la empresa.

Pues bien, aunque el Tribunal Supremo reconoce —como ya ha venido haciendo en pronunciamientos anteriores en las sentencias núm. 429/2020, de 15 de julio, y núm. 458/2023, de 17 de abril— que las personas jurídicas, en general, y las sociedades mercantiles, en particular, son titulares del derecho al honor, destaca «que la protección del derecho al honor es de menor intensidad cuando su titular es una persona jurídica y que para que un ataque al prestigio profesional o empresarial integre además una transgresión del derecho fundamental al honor es necesario que revista una cierta intensidad y que no basta la mera crítica de la actividad profesional, sino que es precisa la descalificación injuriosa o innecesaria del comportamiento profesional de una persona, especialmente mediante infamias que pongan en duda o menosprecien su probidad o ética en el desempeño de aquella actividad, lo que dependerá y deberá apreciarse en función de las circunstancias del caso, de quién, cómo, cuándo y de qué forma se ha cuestionado la valía profesional del ofendido».

Partiendo de esas premisas, en el caso concreto, el alto tribunal considera que la vulneración del derecho al honor de las personas jurídicas no se puede identificar simplemente con la reputación empresarial, comercial o, en general, con el mero prestigio con que se desarrolla la actividad, y que la frase «Cerrado permanentemente», que aparece en el perfil de la recurrente, no constituye una intromisión ilegítima en su derecho al honor, incluso aunque se interprete como cierre permanente

de su negocio, pues «carece de contenido infamante y no imputa hechos ni manifiesta juicios de valor que impliquen su descalificación injuriosa o que supongan el menosprecio de su probidad o su ética en lo relativo a su actividad negocial, puesto que dejar de ejercerla, cerrando el negocio, no constituye sin más una conducta deshonrosa o una muestra de indignidad ni es algo que conlleve por sí mismo demérito o desmerecimiento en la consideración ajena».

Asimismo, el Tribunal Supremo también considera que «en las plataformas de redes sociales no se garantiza un derecho absoluto a tener presencia si no se cumplen las condiciones establecidas por los proveedores de servicios. Y la recurrente no proporcionó su nombre real ni información veraz al crear su perfil y, además, lo utilizó con fines comerciales». En consecuencia, al haber infringido las condiciones de uso establecidas por el responsable de la red social, tanto al registrarse como al utilizar el servicio, se considera justificado el cierre de la cuenta.

Ángel García Vidal

Para más información, contacte con los siguientes letrados del Grupo de Propiedad Intelectual:

Jesús Muñoz-Delgado Mérida

Socio
jmunoz@ga-p.com

Sofía Martínez-Almeida y Alejos-Pita

Socia
smartinez@ga-p.com