
This is the **published version** of the bachelor thesis:

Teruel Rosa, Ana. *La protección de datos personales, su captación y tratamiento por empresas privadas*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 54 pàg.

This version is available at <https://ddd.uab.cat/record/331968>

under the terms of the  license.



***LA PROTECCIÓN DE DATOS PERSONALES, SU
CAPTACIÓN Y TRATAMIENTO POR EMPRESAS
PRIVADAS***

Grado: ADE + Derecho

Trabajo de Fin de Grado

Curso 2025-2026

Autora: Ana Teruel Rosa

Tutor: José Carlos Remotti Carbonell

Fecha de entrega: 12.05.2026

Número de palabras: 11.854

Resumen:

Este trabajo analiza la captación y tratamiento de datos personales por empresas privadas en el entorno digital, prestando especial atención a los mecanismos de obtención de información, al papel del consentimiento y a los límites jurídicos que derivan del derecho fundamental a la protección de datos. A partir del estudio del marco constitucional, europeo y legislativo, así como de la jurisprudencia del Tribunal Constitucional, del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, se valora en qué medida prácticas como las cookies, el perfilado, la publicidad personalizada o la reutilización de datos pueden considerarse compatibles con las garantías que protegen la libertad y el control del individuo sobre su información personal.

Palabras clave: Protección de datos personales, empresas privadas, consentimiento digital, derechos fundamentales, Reglamento General de Protección de Datos, privacidad, libertad de empresa, publicidad personalizada.

Resum:

Aquest treball analitza la captació i el tractament de dades personals per part d'empreses privades en l'entorn digital, amb una atenció especial als mecanismes d'obtenció d'informació, al paper del consentiment i als límits jurídics que deriven del dret fonamental a la protecció de dades. A partir de l'estudi del marc constitucional, europeu i legislatiu, així com de la jurisprudència del Tribunal Constitucional, del Tribunal Europeu de Drets Humans i del Tribunal de Justícia de la Unió Europea, s'hi valora en quina mesura pràctiques com les cookies, el perfilat, la publicitat personalitzada o la reutilització de dades poden considerar-se compatibles amb les garanties que protegeixen la llibertat i el control de l'individu sobre la seva informació personal.

Paraules clau: Protecció de dades personals, empreses privades, consentiment digital, drets fonamentals, Reglament General de Protecció de Dades, privacitat, llibertat d'empresa, publicitat personalitzada.

Abstract:

This paper analyses the collection and processing of personal data by private companies in the digital environment, paying particular attention to data-gathering mechanisms, the role of consent, and the legal limits arising from the fundamental right to data protection. Based on the study of the constitutional, European and legislative framework, as well as the case law of the Constitutional Court, the European Court of Human Rights and the Court of Justice of the European Union, it assesses the extent to which practices such as cookies, profiling, personalized advertising or the reuse of data can be considered compatible with the safeguards that protect individual freedom and control over personal information.

Keywords: Personal data protection, private companies, digital consent, fundamental rights, General Data Protection Regulation, privacy, freedom of enterprise, personalized advertising.

En agradecimiento a mi abuela Leli, por siempre estar a mi lado, apoyándome en todas mis decisiones y cuidándome como una madre. Por ser mi faro y ejemplo a seguir.

ABREVIACIONES

AEPD – Agencia Española de Protección de Datos

BOE – Boletín Oficial del Estado

CDFUE – Carta de los Derechos Fundamentales de la Unión Europea

CE – Constitución Española

CEDH – Convenio Europeo de Derechos Humanos

CEPD – Comité Europeo de Protección de Datos

DOUE – Diario Oficial de la Unión Europea

FJ – Fundamento Jurídico

IA – Inteligencia Artificial

LOPD – Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal

LOPDGDD – Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales

LSSI-CE – Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico

RD – Real Decreto

RGPD – Reglamento General de Protección de Datos

STC – Sentencia del Tribunal Constitucional

STEDH – Sentencia del Tribunal Europeo de Derechos Humanos

STS – Sentencia del Tribunal Supremo

STJUE – Sentencia del Tribunal de Justicia de la Unión Europea

TC – Tribunal Constitucional

TEDH – Tribunal Europeo de Derechos Humanos

TJUE – Tribunal de Justicia de la Unión Europea

UE – Unión Europea

ÍNDICE

1. INTRODUCCIÓN	9
2. MARCO CONSTITUCIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS	11
2.1 El reconocimiento constitucional: art. 18.4 CE y autonomía del derecho ..	11
2.2 Interpretación conforme a estándares europeos: art. 10.2 CE, CEDH y CDFUE	12
2.3 Naturaleza jurídica: derecho subjetivo y dimensión pública.....	14
2.4 Función y finalidad: autodeterminación informativa y garantías de libertad personal.....	15
2.5 Titularidad del derecho: nacionales, extranjeros, menores y alcance subjetivo	16
2.6 Marco teórico: construcción jurisprudencial y normativa del contenido del derecho	18
2.7 Ejercicio, contenido esencial y límites: desarrollo legal, ponderación y estados excepcionales	24
3. MARCO LEGISLATIVO DE PROTECCIÓN DE DATOS	26
3.1 Reglamento (UE) 2016/679 (RGPD): marco general y obligaciones para empresas privadas	26
3.2 Ley Orgánica 3/2018 (LOPDGDD): desarrollo y concreciones en España.	28
3.3 Reglamento español y normativa complementaria: vigencia supletoria del RD 1720/2007 y criterios interpretativos	29
4. MECANISMOS DE CAPTACIÓN DE DATOS POR EMPRESAS PRIVADAS	

4.1 Internet, cookies y rastreadores	31
4.2 Aplicaciones móviles y permisos	33
4.3 Códigos QR y Wi-Fi gratuito	34
4.4 Comercio electrónico y perfilado del usuario	36
5. CONSENTIMIENTO DIGITAL Y LÍMITES A LA EXPLOTACIÓN EMPRESARIAL DE DATOS	38
5.1 El consentimiento como base jurídica del tratamiento en entornos digitales	38
5.2 Límites reales del consentimiento en la economía de los datos	40
5.3 Valoración jurídica de la captación y tratamiento de datos personales por empresas privadas	42
6. CONCLUSIONES.....	46
7. BIBLIOGRAFÍA.....	50
8. OTROS MATERIALES UTILIZADOS	52

1. INTRODUCCIÓN

El tratamiento masivo de datos personales se ha convertido en un elemento estructural de la actividad económica digital. Cada vez que utilizamos aplicaciones móviles, navegamos por internet, escaneamos un código QR, nos conectamos a una red Wi-Fi o aceptamos cookies, generamos información que las empresas recopilan, analizan y utilizan para finalidades muy diversas, desde la prestación del servicio hasta la publicidad personalizada o el diseño de estrategias empresariales. Esta realidad plantea cuestiones relevantes sobre la protección de los derechos fundamentales, especialmente sobre el derecho a la protección de datos personales en un contexto en el que la información personal posee un claro valor económico.

El interés central de este trabajo es examinar cómo captan y tratan datos las empresas privadas y en qué medida estas prácticas respetan o tensionan el marco jurídico de garantías aplicable. La relevancia del tema se explica por el impacto que estas dinámicas producen en la relación cotidiana de los ciudadanos con los servicios digitales, donde con frecuencia se aceptan condiciones de uso, políticas de privacidad o sistemas de rastreo sin un conocimiento real de sus implicaciones. En este contexto, resulta esencial analizar hasta qué punto el consentimiento prestado es verdaderamente libre, informado y específico o si por el contrario, se convierte en una aceptación rutinaria que dificulta el control efectivo sobre la propia información.

A partir de este planteamiento, el trabajo tiene como objetivo identificar las líneas jurídicas que delimitan la actuación de las empresas privadas en materia de protección de datos, prestando especial atención a los mecanismos actuales de captación y tratamiento y a los límites que derivan de los derechos fundamentales. Para ello, el estudio parte de que la protección de datos no puede entenderse únicamente desde el

art. 18.4 CE, sino desde un marco en el que desempeñan un papel decisivo el art. 10.2 CE, la jurisprudencia del Tribunal Constitucional, del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, así como el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, que reconoce expresamente la protección de datos personales como un derecho fundamental autónomo.

El análisis se proyecta sobre prácticas empresariales frecuentes en el entorno digital, como el uso de cookies y rastreadores, los permisos solicitados por aplicaciones móviles, los sistemas de acceso mediante códigos QR o redes Wi-Fi y las técnicas de perfilado en el comercio electrónico. La metodología combina el análisis constitucional, normativo, doctrinal y jurisprudencial. Primero se estudia la construcción del derecho a la protección de datos en el plano constitucional y europeo, después, su concreción legislativa en el RGPD, la LOPDGDD y la normativa complementaria, y por último, los principales mecanismos de captación utilizados por empresas privadas y los límites que plantea el consentimiento digital. En definitiva, este trabajo pretende mostrar que la cuestión no reside únicamente en que las empresas privadas traten datos personales, sino en determinar bajo qué condiciones dicho tratamiento puede considerarse jurídicamente admisible y cuándo, por el contrario, la información personal queda reducida a un mero recurso de explotación empresarial al margen de los derechos fundamentales de su titular.

2. MARCO CONSTITUCIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS

2.1 El reconocimiento constitucional: art. 18.4 CE y autonomía del derecho

El artículo 18.4 de la Constitución Española dispone que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar y el pleno ejercicio de sus derechos”*.¹ Se trata de un precepto de formulación abierta, que no define de manera exhaustiva el contenido del derecho ni concreta las técnicas de protección frente al tratamiento de datos. No obstante, la jurisprudencia constitucional (especialmente a partir de la relevante STC 94/1998, FJ 6) ha afirmado que de este precepto nace un derecho fundamental autónomo: el derecho a la protección de datos personales, diferenciado del derecho a la intimidad previsto en el artículo 18.1 CE.

La autonomía del 18.4 CE se explica porque el bien jurídico protegido no es solo la “intimidad” entendida como esa esfera reservada y oculta al público, sino el control del individuo sobre el flujo de su información personal. Como señala el TC en la citada sentencia, nos encontramos ante un derecho a la “libertad informática” que consiste en un poder de disposición y de control que faculta a la persona para decidir qué datos proporciona a terceros y qué uso se les da. Esta facultad se proyecta sobre cualquier información que identifique o pueda identificar al sujeto sin que sea necesario que el dato pertenezca al núcleo de su vida privada.

Bajo este contexto, el TC establece que el derecho fundamental a la protección de datos garantiza un conjunto de facultades que permiten al ciudadano conocer quién posee sus datos, para qué finalidades y bajo qué condiciones. De este modo, el artículo 18.4 CE se configura como una garantía que permite al individuo supervisar el tratamiento

¹ Constitución Española, (En adelante CE). art. 18.4.

automatizado de su información evitando que la tecnología degrade su dignidad o condicione su libertad mediante seguimientos detallados. Esta construcción permite entender que la protección constitucional no se limita a impedir intromisiones físicas o digitales en la vida privada, sino que establece un ámbito de control sobre la información esencial en entornos tecnológicos, donde la captación de datos es masiva y constante.

2.2 Interpretación conforme a estándares europeos: art. 10.2 CE, CEDH y CDFUE

El art. 10.2 CE impone que los derechos fundamentales reconocidos en la Constitución se interpreten de conformidad con los tratados internacionales sobre derechos humanos ratificados por España.² Este mandato tiene una especial relevancia en materia de protección de datos, ya que el art. 18.4 CE utiliza una fórmula abierta y remite a la ley sin detallar un catálogo cerrado de facultades. Por ello, su contenido no puede entenderse únicamente desde la literalidad constitucional, sino que se completa mediante el estándar europeo de protección de derechos.

En el marco del Consejo de Europa, el art. 8 del Convenio Europeo de Derechos Humanos (en adelante, CEDH) reconoce el derecho al respeto de la vida privada y familiar.³ La jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH), ha interpretado este precepto de manera amplia, incluyendo dentro de la “vida privada”, la recogida, almacenamiento y utilización de datos personales, incluso cuando no se trate de información estrictamente íntima. De este modo, el TEDH ha establecido que cualquier intromisión en este ámbito requiere una base legal suficiente, debe

² CE, art. 10.2.

³Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (En adelante CEDH), Roma, 4 de noviembre de 1950, art. 8.

perseguir una finalidad legítima y superar un juicio de necesidad y proporcionalidad.⁴

Estos criterios operan como parámetros interpretativos para el derecho interno, en virtud del art. 10.2 CE.

En la misma línea, en el ámbito de la Unión Europea, la Carta de Derechos Fundamentales (en adelante, CDFUE) reconoce de forma expresa el derecho a la protección de datos personales en su art. 8, diferenciándolo del derecho al respeto de la vida privada del art. 7.⁵ Esta dualidad refuerza la idea de que la protección de datos constituye un derecho autónomo, con exigencias propias, entre ellas la licitud del tratamiento, la determinación de finalidades, la transparencia y el control por parte del interesado. La interpretación conjunta de los arts. 7 y 8 CDFUE ha sido decisiva para consolidar un estándar europeo particularmente exigente frente a tratamientos intensivos de datos, lo que influye directamente en la lectura constitucional del art. 18.4 CE.

A mi entender, la relevancia del art. 10.2 CE en materia de protección de datos es especialmente determinante, porque el contenido del art. 18.4 CE no puede concretarse sin acudir al estándar europeo. Esta dependencia interpretativa muestra que la protección de datos es uno de los ámbitos donde con mayor claridad, se aprecia la naturaleza compartida de los derechos fundamentales, ya que el alcance de las garantías no se define solo en el plano constitucional interno, sino en diálogo constante con el TEDH y el Tribunal de Justicia de la Unión Europea (en adelante TJUE).

⁴ Sentencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH). En el caso *Amann c. Suiza*, de 16 de febrero de 2000.

⁵ Carta de los Derechos Fundamentales de la Unión Europea, (CDFUE en adelante). C 326, 26 de octubre de 2012, arts. 7 y 8.

2.3 Naturaleza jurídica: derecho subjetivo y dimensión pública

Desde la perspectiva constitucional, el derecho a la protección de datos presenta una estructura típicamente subjetiva, en la medida en que reconoce a cada persona facultades de control sobre el tratamiento de su información personal, integradas en el conjunto de derechos fundamentales del Título I CE. El TC ha vinculado este derecho con la idea de autodeterminación informativa, entendida como poder de disposición y control sobre los datos personales, lo que refuerza su condición de derecho fundamental de titularidad individual.⁶

No obstante, su naturaleza no se agota en esta dimensión subjetiva. Como ocurre con otros derechos fundamentales; presenta también una dimensión objetiva o institucional, ya que impone a los poderes públicos el deber de establecer un marco normativo de garantías que haga posible su ejercicio real y efectivo. Esta idea se conecta con la doctrina general del TC sobre la doble dimensión de los derechos fundamentales, como posiciones subjetivas y como principios estructurales del ordenamiento⁷.

Además, la eficacia del derecho a la protección de datos no se limita a las relaciones verticales frente al Estado, sino que adquiere especial relevancia en las relaciones entre particulares. En la economía digital, las empresas privadas son actores centrales en la captación y explotación de datos, lo que refuerza la proyección del derecho en el ámbito de las relaciones privadas.

A mi entender, esta doble dimensión es especialmente visible en la protección de datos, ya que sin la intervención normativa y de control público (autoridades de protección de datos, régimen sancionador, deberes de información...), el derecho quedaría reducido a una facultad formal difícilmente ejercitable frente a grandes operadores digitales.

⁶ Sentencia del Tribunal Constitucional (en adelante, STC) 292/2000, FJ 7.

⁷ Sentencia del Tribunal Supremo (en adelante, STS) 1/1985, de 11 de abril, FJ 4, BOE núm. 119, de 18 de mayo de 1985.

Precisamente por ello, la protección de datos no puede concebirse solo como un espacio de defensa individual, sino también como un ámbito en el que el ordenamiento debe crear condiciones reales para que la persona conserve el control real sobre su información.

2.4 Función y finalidad: autodeterminación informativa y garantías de libertad personal

La función del derecho a la protección de datos no se limita a evitar intromisiones en la intimidad, sino que se orienta a preservar condiciones materiales de libertad en sociedades caracterizadas por el tratamiento masivo de información personal. El TC ha subrayado (principalmente en la STC 292/2000 de 30 de noviembre, FJ 5) que el núcleo del derecho reside en la capacidad de la persona para controlar el uso de sus datos, lo que conecta directamente con el concepto de autodeterminación informativa.

Esta función se proyecta en una doble finalidad. En primer lugar, garantizar el control del individuo sobre el ciclo de vida de los datos (obtención, uso, comunicación, conservación y supresión) evitando que la información personal circule sin conocimiento ni control del afectado. En segundo lugar, impedir la consolidación de formas de poder informacional que a través de tratamientos masivos y creación de perfiles de usuario que puedan impactar en la libertad ideológica, la igualdad o la no discriminación.

En entornos digitales donde se combinan grandes volúmenes de datos y se generan deducciones automáticas sobre comportamientos, gustos o riesgos, la función del derecho adquiere una dimensión preventiva; no se protege solo frente al daño ya producido, sino frente al riesgo de configuraciones de perfiles persistentes que condicionen la posición de la persona en el tráfico social y económico. Desde una perspectiva constitucional, puede apreciarse que la protección de datos opera como una

herramienta de protección de otras libertades ya que, sin control sobre la información personal, resulta más fácil influir o clasificar a los individuos según comportamientos deducidos de forma automática.

La función preventiva del derecho se intensifica con el uso de procesamientos algorítmicos⁸ complejos, que al operar de forma autónoma, plantean nuevos retos para garantizar que la tecnología permanezca siempre al servicio de la persona y no a la inversa. Como advierte la Agencia Española de Protección de Datos (en adelante, AEPD),⁹ la adecuación de los tratamientos que incorporan Inteligencia Artificial¹⁰ (en adelante, IA) es hoy en día, un requisito imprescindible para asegurar que el poder de los algoritmos¹¹ no derive en una pérdida de libertad real o en discriminaciones automatizadas. Solo mediante el ejercicio efectivo de la autodeterminación frente a estas tecnologías, es posible garantizar que el individuo mantenga su autonomía y dignidad frente a sistemas automatizados cada vez más opacas y estructurales.

2.5 Titularidad del derecho: nacionales, extranjeros, menores y alcance subjetivo

La titularidad del derecho a la protección de datos corresponde con carácter general a las personas físicas en la medida en que el dato personal se entiende como una proyección de la propia persona y su dignidad. El objeto de protección no es el dato como unidad de información aislada, sino la posición jurídica del individuo frente a cualquier tratamiento que permita identificarlo. Como ha subrayado el TC¹² el derecho

⁸ Procesamientos algorítmicos: uso de sistemas automatizados para tratar grandes volúmenes de información y llevar a cabo clasificación o selección de manera continua (definición del autor).

⁹ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (en adelante, AEPD) *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial*, 2020, leído en <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf> (Consulta el 15/03/2026).

¹⁰ Inteligencia Artificial: tecnología capaz de imitar ciertos procesos de análisis y decisión que normalmente requerirían intervención humana (definición del autor).

¹¹ Algoritmo: Funciona como un conjunto de instrucciones diseñadas para procesar grandes volúmenes de datos y automatizar decisiones. Las empresas los utilizan para analizar cómo nos comportamos y así predecir nuestros gustos. (definición del autor)

¹² STC 292/2000, de 30 de noviembre, FJ 7.

se configura como un poder de control sobre el uso de la información personal, lo que lo vincula de forma inseparable a la libertad y a la autonomía individual.

En cuanto a los extranjeros, la titularidad no puede verse restringida por criterios de nacionalidad. Aunque la CE remite a la ley para regular el ejercicio de libertades por parte de extranjeros, el carácter de derecho inherente a la persona (vinculado a su dignidad) que define a la protección de datos, exige una interpretación extensiva. Esta visión está respaldada por el marco europeo que desplaza el criterio de aplicación desde la nacionalidad hacia la ubicación geográfica del interesado. De este modo, cualquier individuo que se encuentre en territorio de la Unión Europea goza de estas garantías frente a tratamientos vinculados a actividades económicas dirigidas al mercado común¹³.

Respecto de los menores, el derecho exige una tutela reforzada debido a su especial vulnerabilidad ante la captación intensiva de datos en entornos digitales. Su titularidad conlleva una protección preventiva, ya que presentan una mayor dificultad para comprender las consecuencias a largo plazo del seguimiento automatizado o de la cesión de información con fines comerciales. El marco normativo europeo reconoce esta asimetría y exige estándares de transparencia y seguridad adaptados a su capacidad de comprensión asegurando que el ejercicio de su derecho sea real y no meramente formal ¹⁴.

En definitiva, la titularidad se proyecta sobre la persona física como centro de control. Este alcance universal garantiza que ni la edad ni la situación personal limiten la protección de datos convirtiéndola en una barrera ética frente al poder tecnológico de la sociedad digital.

¹³ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, art. 3.

¹⁴ Reglamento (UE) 2016/679 (RGPD), Considerando 38.

2.6 Marco teórico: construcción jurisprudencial y normativa del contenido del derecho

De acuerdo con la perspectiva jurídica, el marco teórico del derecho a la protección de datos no se construye desde definiciones abstractas, sino a partir de la interpretación que realizan los tribunales constitucionales y europeos, junto con su posterior concreción normativa. Es por tanto, un derecho jurisprudencial, cuya naturaleza se ha ido delimitando progresivamente ante los riesgos derivados del uso de la informática y del tratamiento masivo de información personal.

a) Jurisprudencia del TC: El punto de partida ineludible es la doctrina del TC, que configura el derecho a la protección de datos como un derecho fundamental autónomo cuyo bien jurídico protegido no es la intimidad en sentido clásico, sino el poder de control del individuo sobre su información personal. Advierte que el problema constitucional no surge solo cuando se difunden datos íntimos, sino cuando mediante el tratamiento automatizado, es posible construir un perfil completo de la persona que condicione su libertad.¹⁵

En esta línea, el TC identifica el contenido del derecho como un poder jurídico de disposición y control, que se traduce en la facultad de conocer quién trata los datos, con qué finalidad y durante cuánto tiempo, así como la posibilidad de oponerse a usos ilegítimos o desproporcionados. Estas facultades no son meramente formales, sino instrumentos destinados a impedir tratamientos excesivos o carentes de base legítima.

Además, insiste en que el concepto de “dato personal” es amplio y no se limita a la esfera íntima. Ya había señalado que el derecho se proyecta sobre cualquier información

¹⁵ STC 292/2000, FJ 6.

identificativa, aunque no pertenezca a la vida privada estricta.¹⁶ Esta idea es especialmente relevante frente a la actividad empresarial digital basada en datos de navegación, consumo o geolocalización ya que aislados pueden parecer neutros pero combinados permiten individualizar de forma precisa a la persona.

A mi entender, esta construcción jurisprudencial constituye hoy el marco necesario para abordar la economía digital. Al definir el derecho como un poder de disposición y control, el TC anticipó que el riesgo estructural en los entornos digitales no sería la simple difusión de secretos, sino la pérdida de soberanía personal frente a procesos de analítica avanzada capaces de predecir y dirigir el comportamiento humano sin su consentimiento efectivo.

b) Jurisprudencia del TEDH: El TEDH ha ampliado el concepto de “vida privada” del art. 8 Convención Europea de Derechos Humanos (en adelante, CEDH) hasta abarcar de forma estable la recogida, conservación y utilización de datos personales. Para el TEDH, el simple almacenamiento de información por autoridades o entidades ya constituye una intromisión en la vida privada, aunque los datos no sean íntimos.¹⁷

A partir de esta premisa, el TEDH ha establecido tres exigencias acumulativas para que el tratamiento sea legítimo: que exista base legal accesible y previsible, que persiga una finalidad legítima y que supere un juicio de necesidad y proporcionalidad.¹⁸

Esta doctrina refuerza la idea de que el control sobre los datos no depende de su carácter público o privado, sino del modo en que son tratados. La acumulación indefinida o la conservación generalizada de información sin justificación suficiente, resulta incompatible con el art. 8 CEDH.

¹⁶ STC 94/1998, FJ 6.

¹⁷ STEDH, Amann c. Suiza, de 16 de febrero de 2000, § 65.

¹⁸ STEDH, S. y Marper c. Reino Unido, de 4 de diciembre de 2008, §§ 67 y 103.

Desde mi punto de vista, la aportación del TEDH es clave porque sitúa el foco en el riesgo estructural del almacenamiento masivo, algo muy cercano a las prácticas actuales de recopilación empresarial de datos. Su jurisprudencia permite entender que la lesión del derecho no depende solo del uso final de la información, sino también de su recogida y conservación cuando estas se producen sin garantías suficientes. Precisamente por ello, el TEDH aporta un criterio especialmente útil para interpretar la protección de datos como una exigencia de control y proporcionalidad frente a cualquier acumulación injustificada de información personal.

c) Jurisprudencia del TJUE: El TJUE ha sido determinante en convertir la protección de datos en un derecho con eficacia real frente a tratamientos masivos, algo esencial en el ámbito empresarial digital. Su jurisprudencia parte de que los arts. 7 y 8 de la CDFUE no se limitan a proteger la esfera íntima, sino que tutelan el conjunto de la información personal cuando su tratamiento puede afectar a la libertad del individuo.

En *Digital Rights Ireland*, el TJUE analizó un sistema de conservación generalizada de datos de comunicaciones electrónicas y declaró que la intromisión era de gran magnitud porque permitía obtener conclusiones muy precisas sobre la vida privada de las personas (hábitos, desplazamientos, relaciones sociales). Lo relevante es que el TJUE no se centró en la sensibilidad de los datos por separado, sino en que su acumulación permitía extraer conclusiones muy precisas sobre la vida privada, concluyendo que un tratamiento indiscriminado vulnera el principio de proporcionalidad.¹⁹

¹⁹ Sentencia del Tribunal de Justicia de la Unión Europea (en adelante, STJUE), 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd*, ECLI:EU:C:2014:238, apdo. 37.

Esta lógica se proyecta directamente sobre la actividad empresarial basada en “big data”,²⁰ ya que aunque cada dato individual parezca inofensivo, el tratamiento masivo puede generar un conocimiento exhaustivo del individuo.

En *Google Spain*, el TJUE reconoció que los motores de búsqueda realizan un tratamiento autónomo de datos personales y que el interesado puede solicitar la supresión de enlaces cuando la difusión resulte desproporcionada.²¹ Esta sentencia es clave porque sitúa el control del titular por encima de la lógica puramente económica del tratamiento y demuestra que la protección de datos actúa como límite frente a modelos de negocio digitales.

Las sentencias *Schrems I* y *Schrems II* refuerzan esta línea al exigir que las transferencias internacionales garanticen un nivel de protección sustancialmente equivalente al europeo.²² El TJUE rechaza soluciones meramente formales y exige garantías efectivas, lo que evidencia que el derecho a la protección de datos no se satisface con cláusulas contractuales si en la práctica existen riesgos estructurales.

A mi entender, esta jurisprudencia muestra que el TJUE concibe la protección de datos como un derecho de defensa frente a estructuras tecnológicas y económicas complejas, algo que encaja plenamente con el análisis de las empresas privadas que realizan tratamientos masivos, perfilados y transferencias globales.

d) Normativa europea y española como contenido “vivo” del derecho: La jurisprudencia encuentra su concreción normativa en el RGPD, que transforma

²⁰ “Big data”: tratamiento automatizado de grandes volúmenes de datos procedentes de múltiples fuentes que permite identificar patrones o generar perfiles de comportamiento. (definición del autor).

²¹ STJUE, 13 de mayo de 2014, asunto C-131/12, *Google Spain SL y Google Inc. c. AEPD y Mario Costeja González*, ECLI:EU:C:2014:317, apdo. 81.

²² STJUE, 6 de octubre de 2015, asunto C-362/14, *Schrems*, ECLI:EU:C:2015:650, apdo. 95; STJUE, 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd y Maximilian Schrems*, ECLI:EU:C:2020:559, apdo. 187.

principios constitucionales y europeos en obligaciones jurídicas precisas para los responsables del tratamiento. El derecho fundamental deja de ser solo una garantía frente a abusos y se convierte en un modelo regulatorio preventivo, basado en la responsabilidad proactiva.²³

El RGPD incorpora principios que actúan como límites estructurales al tratamiento: Limitación de finalidad (impide reutilizar datos para objetivos incompatibles), minimización (obliga a tratar solo los datos necesarios) y limitación del plazo de conservación (evita acumulaciones indefinidas).

Estos principios son especialmente relevantes en entornos empresariales donde la lógica económica impulsa a conservar datos por tiempo indefinido y a reutilizarlos con fines comerciales adicionales.

Además, dicho reglamento introduce obligaciones organizativas (evaluaciones de impacto, privacidad desde el diseño, contratos con encargados) que reflejan que el riesgo no depende solo del uso final del dato, sino de la estructura del sistema de tratamiento.

La normativa española complementa este marco dotándolo de mecanismos de control, régimen sancionador y reglas específicas para contextos habituales como el uso de cookies, el tratamiento de datos en aplicaciones móviles o los sistemas de rastreo digital. Con ello, se evidencia que el derecho a la protección de datos no es una mera declaración de intenciones, sino un sistema normativo dinámico que adapta las garantías constitucionales a prácticas reales.

e) Doctrina científica: Junto a las normas y la jurisprudencia, el análisis del derecho a la protección de datos se apoya en la doctrina científica, entendida como los estudios

²³ Reglamento (UE) 2016/679 (RGPD), arts. 5 y 24.

elaborados por autores especializados en derecho, que permiten examinar críticamente el funcionamiento real de las garantías jurídicas en entornos digitales.

Desde esta perspectiva, se ha señalado que en la sociedad tecnológica el riesgo principal no radica únicamente en intromisiones puntuales en la esfera privada, sino en la construcción de patrones de personalidad automatizados a partir de la agregación de datos, que pueden condicionar oportunidades, decisiones y comportamientos futuros de los individuos. Esta lectura, presente en el pensamiento de Stefano Rodotà²⁴, pone el foco en la relación entre información, poder y libertad material, subrayando que la protección de datos se vincula directamente con la dignidad y con la posibilidad de que el individuo mantenga un margen real de autodeterminación frente a estructuras tecnológicas y económicas cada vez más influyentes.

En la misma línea, parte de la doctrina advierte que el consentimiento “pieza central del sistema” puede convertirse en una garantía meramente formal cuando el usuario acepta sin comprender el alcance del tratamiento o cuando el acceso a servicios digitales se condiciona a la cesión masiva de datos. En estos casos, el consentimiento deja de operar como instrumento de autodeterminación informativa y pasa a funcionar como mecanismo de legitimación de prácticas empresariales intensivas, lo que desplaza el eje de protección desde el control del individuo hacia la lógica del mercado de datos.

Además, se ha destacado que las técnicas de perfilado y predicción, basadas en el análisis automatizado de grandes volúmenes de información, pueden generar efectos estructurales sobre la igualdad, al producir clasificaciones, segmentaciones o decisiones diferenciadas que, aun siendo formalmente neutrales, repercuten de manera desigual en

²⁴ RODOTÀ, Stefano. *La vida y las reglas. Entre el Derecho y el no Derecho*. Trotta, Madrid, 2010, pp. 75-82

distintos colectivos. Desde esta visión, la protección de datos no se agota en la tutela de la intimidad, sino que se conecta con la garantía de condiciones materiales de libertad e igualdad en contextos digitales.

Además, tal y como advierte Piñar Mañas²⁵, la protección de datos se ha convertido en un instrumento jurídico destinado a equilibrar el creciente poder informacional de empresas y organizaciones frente a la posición del individuo en la sociedad digital. A partir de esta idea, puede entenderse que el derecho a la protección de datos no puede interpretarse únicamente como un conjunto de trámites formales (información al usuario, casillas de aceptación o políticas de privacidad) , sino como un mecanismo de equilibrio frente a formas de poder informacional que operan de manera estructural. La doctrina permite así identificar la distancia que puede existir entre la validez formal de un tratamiento y su compatibilidad material con la libertad real de la persona, cuestión especialmente relevante cuando el tratamiento de datos es llevado a cabo por grandes empresas digitales.

2.7 Ejercicio, contenido esencial y límites: desarrollo legal, ponderación y estados excepcionales

Tal y como hemos podido analizar, el art. 18.4 CE no define de manera cerrada el contenido del derecho a la protección de datos, sino que remite al legislador para establecer límites al uso de la informática con el fin de garantizar los derechos fundamentales. Esta técnica constitucional implica que el ejercicio efectivo del derecho se concreta a través de normas de desarrollo que transforman la autodeterminación informativa en facultades jurídicas de control por parte del titular de los datos.

²⁵ PIÑAR MAÑAS, José Luis. “El derecho fundamental a la protección de datos personales”, en PIÑAR MAÑAS, José Luis (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Reus, Madrid, 2016. pp. 21 y ss.

En este sentido, el derecho se ejerce mediante poderes concretos frente a entidades que gestionan la información que permiten al individuo conocer qué datos se tratan, con qué finalidad y oponerse cuando el tratamiento no sea legítimo. El RGPD traduce este control en un sistema estructurado de derechos (acceso, rectificación, supresión, oposición, limitación y portabilidad), configurando un auténtico estatuto jurídico del interesado frente al poder tecnológico y organizativo de quienes tratan datos de forma masiva.²⁶

El contenido esencial del derecho se vincula así con la posibilidad real de control sobre la información personal. El TC ha señalado que el núcleo del derecho radica en el poder de disposición sobre los datos, lo que impide tratamientos excesivos, carentes de finalidad o desproporcionados. Desde esta perspectiva, la protección de datos no solo tutela la esfera íntima, sino que evita que la persona quede definida externamente por perfiles o inferencias que no puede conocer ni corregir.

Ahora bien, el derecho no es absoluto. Puede ser objeto de limitaciones, pero únicamente cuando exista base legal, la medida persiga una finalidad legítima y supere un juicio de proporcionalidad. Este esquema, consolidado tanto en la jurisprudencia constitucional como europea, impide que intereses meramente económicos o de eficiencia empresarial justifiquen restricciones intensas del derecho.²⁷ La libertad de empresa no habilita tratamientos indiscriminados ni usos secundarios de datos que desborden la finalidad inicial.

Esta lógica de límites se hizo especialmente visible durante situaciones excepcionales como la pandemia de COVID-19. En ese contexto, se adoptaron medidas que implicaban tratamientos de datos de salud o de localización con fines de salud pública.

²⁶ Reglamento (UE) 2016/679 (RGPD), arts. 15-22.

²⁷ TEDH, *S. y Marper c. Reino Unido*, §§ 101–103.

Sin embargo, incluso en situaciones de emergencia, la afectación del derecho debe configurarse como restricción sujeta a garantías y no como autorización general para tratar datos sin control. Los estándares europeos insisten en que la excepcionalidad no suspende la exigencia de necesidad y proporcionalidad.²⁸

A mi entender, este punto muestra que la verdadera fortaleza del derecho a la protección de datos no está en su reconocimiento teórico, sino en la exigencia constante de justificación de cualquier tratamiento que limite el control de los individuos. Si permitimos que las excepciones se conviertan en algo habitual, el derecho a la protección de datos acaba perdiendo su sentido y deja de proteger la libertad real de los individuos.

3. MARCO LEGISLATIVO DE PROTECCIÓN DE DATOS

3.1 Reglamento (UE) 2016/679 (RGPD): marco general y obligaciones para empresas privadas

El Reglamento (UE) 2016/679 constituye la pieza central del sistema de protección de datos en Europa y debe entenderse como la concreción normativa del contenido del derecho fundamental reconocido en el art. 8 de la CDFUE y conectado con el art. 18.4 CE. Dicho reglamento no se limita a establecer reglas técnicas, sino que articula un modelo jurídico basado en la responsabilidad activa del responsable o quien gestiona el flujo de datos, lo que transforma la protección de datos en un elemento estructural de la actividad empresarial digital.

Los principios del art. 5 RGPD operan como verdaderos criterios de control de la licitud del tratamiento y deben interpretarse conjuntamente con las bases jurídicas del

²⁸ Comité Europeo de Protección de Datos (en adelante CEPD), *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la COVID-19*. 2020. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en Consulta: 15/03/2026.

tratamiento previstas en el art. 6 RGPD. El principio de limitación de la finalidad impide reutilizar datos para fines distintos e incompatibles con aquellos que justificaron su recogida inicial, cuestión especialmente sensible en modelos de negocio basados en la analítica y la publicidad segmentada individualmente. El criterio de reducción a los datos necesarios se opone a prácticas de captación masiva con fines indeterminados o difusos, obligando a las empresas a justificar la necesidad de cada dato. La transparencia y la lealtad exigen que el usuario comprenda qué se hace con su información, lo que conecta directamente con el problema del consentimiento digital analizado a lo largo del presente trabajo.

El RGPD también exige que todo tratamiento tenga una base jurídica. En el sector privado, esta exigencia impide que el interés económico actúe como justificación automática. El consentimiento debe ser libre y revocable, la ejecución contractual legítima solo lo necesario para el servicio principal y el interés legítimo exige un ajuste de equilibrio efectivo con los derechos del interesado. De este modo, la base jurídica funciona como límite material al poder informacional de la empresa.²⁹

Además, dicho reglamento refuerza la posición del titular mediante un sistema de derechos subjetivos (desde el acceso hasta la portabilidad de la información) que materializan la idea de control sobre los datos. Estos derechos buscan corregir la asimetría entre usuario y empresa, aunque su eficacia depende de la claridad de la información y de la facilidad real de ejercicio.

Finalmente, el RGPD introduce obligaciones organizativas, como el deber de diligencia constante, la adopción de medidas de seguridad, la regulación de relaciones con terceros que colaboran en el tratamiento y la evaluación de datos etc. Esto demuestra que la protección de datos se integra en las estrategias empresariales, no como una formalidad,

²⁹ Reglamento (UE) 2016/679 (RGPD), arts. 12–22.

sino como un requisito estructural. Con todo ello, el RGPD no solo regula el tratamiento de datos, sino que redefine los límites jurídicos del modelo de negocio digital basado en la información personal.

3.2 Ley Orgánica 3/2018 (LOPDGDD): desarrollo y concreciones en España

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (más adelante LOPDGDD), cumple una función complementaria respecto del RGPD, adaptando su aplicación al ordenamiento jurídico español y regulando supuestos frecuentes en la práctica empresarial. Dicha ley no altera los principios europeos, pero concreta escenarios donde la tensión entre actividad económica y derechos fundamentales es visible.³⁰

Un ejemplo es el tratamiento de datos de identificación en el entorno laboral y de empresarios individuales, habitual en relaciones comerciales. La Ley establece condiciones para su uso, evitando que se utilicen datos profesionales como puerta de entrada a tratamientos más amplios sin base jurídica clara. Además, regula los sistemas de información crediticia, ámbito donde el tratamiento masivo de datos puede afectar a la reputación económica de los usuarios, exigiendo garantías específicas.³¹

La LOPDGDD también delimita su finalidad (seguridad) y prohíbe usos incompatibles, recordando que la captación de imágenes no es neutra desde la perspectiva de los derechos fundamentales. Además, regula los sistemas internos de información (canales de denuncia), que implican tratamientos sensibles dentro de organizaciones privadas.

En relación con los menores, fija la edad para prestar consentimiento por sí mismos en servicios de la sociedad de la información, cuestión relevante para plataformas digitales

³⁰ Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), arts. 19 y 20.

³¹ LOPDGDD, arts. 22 y 24.

dirigidas a público joven; esta previsión refuerza la idea de protección reforzada frente a la captación intensiva de datos.

Desde mi perspectiva, la LOPDGDD evidencia que la protección de datos no se agota en principios generales, sino que exige regulación específica de prácticas empresariales concretas donde el riesgo para los derechos es mayor.

3.3 Reglamento español y normativa complementaria: vigencia supletoria del RD 1720/2007 y criterios interpretativos

El marco reglamentario español actual está marcado por la convivencia de normas de distintas épocas. El Real Decreto 1720/2007 fue aprobado para desarrollar la antigua ley de 1999, por lo que responde a un modelo anterior, más formalista y centrado en medidas de seguridad predeterminadas. Tras la plena aplicación del marco europeo y la entrada en vigor de la nueva LOPDGDD, este reglamento no puede aplicarse de manera automática, sino solo de forma supletoria y en la medida en que sus previsiones técnicas no contradigan el estándar europeo que tiene primacía.³²

Esto es relevante porque el RGPD sustituye el cumplimiento de un catálogo cerrado de obligaciones, por un análisis de riesgos dinámico. Mientras que el RD 1720/2007 clasificaba los ficheros por niveles de seguridad fijos (básico, medio y alto), el RGPD exige que cada responsable valore el peligro real de su tratamiento y adopte medidas proporcionales. Esta transición muestra la evolución hacia un modelo donde lo decisivo no es cumplir un catálogo rígido, sino garantizar de forma real los derechos del afectado. Junto a la normativa adquieren un papel relevante los criterios de las autoridades de control. A nivel europeo el Comité Europeo de Protección de Datos (en adelante, CEPD) emite directrices que orientan la interpretación de conceptos complejos como la

³² Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, BOE núm. 17, de 19 de enero de 2008.

corresponsabilidad o el interés legítimo³³. Estas orientaciones, aunque no son leyes, influyen de forma decisiva en la práctica empresarial porque anticipan el criterio que seguirán los reguladores.

En el ámbito nacional, la AEPD publica guías que traducen estos estándares a situaciones cotidianas como el uso de cookies³⁴ o la videovigilancia³⁵. Estas guías cumplen una función de “puente” facilitando el cumplimiento y delimitando qué se espera de las empresas en el uso de la información personal.

A mi entender, esta estructura flexible refuerza la protección de los derechos fundamentales ya que impide que las empresas se limiten a un cumplimiento formal y las obliga ajustar su actividad a criterios actualizados sobre riesgo y garantías efectivas.

4. MECANISMOS DE CAPTACIÓN DE DATOS POR EMPRESAS PRIVADAS

El tratamiento de datos por empresas privadas no empieza necesariamente cuando el usuario “se registra”, sino mucho antes, a través de mecanismos cotidianos que funcionan de forma casi invisible: navegación web, aplicaciones móviles, sistemas de acceso (QR³⁶ o Wi-Fi) y compras online. En la práctica, estos mecanismos permiten recoger datos directos (los que el usuario aporta) y datos indirectos o inferidos (los que se deducen de su comportamiento), lo que incrementa el riesgo de pérdida de control sobre la información personal.

³³ CEPD. *Directrices 07/2020 sobre los conceptos de responsable y encargado del tratamiento*. 2021. Leído en: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf Consulta: 15/03/2026.

³⁴ Cookies: Dispositivos de almacenamiento y recuperación de datos que se instalan en el equipo del usuario al visitar una web. Su uso permite a las empresas identificar al navegador y rastrear la actividad del interesado con fines analíticos o publicitarios. (definición del autor)

³⁵ AEPD. *Guía para el cumplimiento del deber de informar*, 2022, leído en <https://www.aepd.es/es/documento/guia-modelo-clausula-informativa.pdf> (Consulta el 15/03/2026).

³⁶ QR: Es un código de barras que al ser escaneado redirige a un contenido digital. Su uso es relevante porque puede captar la ubicación y datos del dispositivo del usuario de forma automática funcionando como una herramienta de seguimiento silencioso. (definición del autor)

4.1 Internet, cookies y rastreadores

Uno de los mecanismos más extensos de captación de datos por parte de empresas privadas es el uso de cookies y tecnologías similares en páginas web. Aunque en ocasiones se presentan como instrumentos meramente técnicos, muchas de estas herramientas permiten identificar o hacer identificable al usuario mediante direcciones IP³⁷ o combinaciones de datos que, en conjunto pueden vincularse a una persona física³⁸. Esto implica que la actividad de rastreo online se sitúa plenamente dentro del ámbito de aplicación de la normativa de protección de datos, incluso cuando no se recaban datos tradicionalmente considerados “íntimos”.

Desde el punto de vista jurídico, la instalación y uso de cookies no se analiza exclusivamente desde el RGPD, sino también desde la normativa específica sobre el almacenamiento y acceso a información en los dispositivos de los usuarios.

En el ordenamiento español, el eje de esta regulación es el deber de información y la exigencia de consentimiento previo cuando las cookies no sean estrictamente necesarias para el funcionamiento del servicio solicitado por el usuario³⁹. De ahí que los denominados “banners de cookies”⁴⁰ se hayan convertido en una práctica habitual, no responden a una decisión de diseño, sino a una obligación jurídica vinculada a la licitud del tratamiento.

³⁷ Dirección IP (Protocolo de Internet): número que identifica la conexión de un dispositivo a una red y que puede servir para localizar o seguir su actividad en internet (definición del autor).

³⁸ Reglamento (UE) 2016/679 (RGPD), arts. 4.1 y Considerando 30.

³⁹ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, LSSI-CE), BOE núm. 166, de 12 de julio de 2002, art. 22.2.

⁴⁰ Banners de cookies: Piezas publicitarias gráficas que aparecen en las páginas web que suelen ir acompañados de sistemas de rastreo que monitorizan si el usuario interactúa con ellos permitiendo medir sus intereses y comportamiento de forma automática. (definición del autor)

No obstante, en la práctica el problema no se sitúa solo en la existencia formal del consentimiento, sino en su efectividad real. En muchos entornos digitales, el usuario acepta de forma automática para acceder al contenido sin comprender el alcance del seguimiento posterior ni la intervención de múltiples terceros. Tal y como señala Barrio Andrés,⁴¹ la complejidad de los entornos digitales actuales exige que el derecho no se limite a una protección formal, sino que garantice un control real sobre el rastro digital que genera el usuario para evitar que el consentimiento se convierta en una autorización meramente aparente.

Desde mi perspectiva crítica, el problema central reside en la asimetría de información entre empresa y usuario: mientras la primera conoce el valor que pueden adquirir los datos agregados, el segundo suele percibir el aviso como un trámite necesario para acceder al contenido, lo que reduce el consentimiento a un acto rutinario más que a una decisión consciente sobre el uso de su información.

Esta dinámica se enmarca en lo que Shoshana Zuboff describe como el "capitalismo de vigilancia".⁴² Según esta autora, el modelo de negocio de las grandes tecnológicas ha evolucionado, los datos ya no son solo un recurso para mejorar el servicio sino la "materia prima" esencial para anticipar y moldear la conducta del consumidor. A partir de lo que Zuboff denomina "excedente conductual", las empresas privadas pueden elaborar perfiles de enorme precisión, capaces de influir en las decisiones de los individuos y de comprometer su autonomía de la voluntad.

⁴¹ BARRIO ANDRÉS, Moisés. *Manual de Derecho Digital*. Tirant lo Blanch, Valencia, 2023, pp. 145-150.

⁴² ZUBOFF, Shoshana. *La era del capitalismo de vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder*. Paidós, Barcelona, 2020, pp. 25-40.

Desde una perspectiva constitucional, esto supone que el mandato del art. 18.4 CE debe ir más allá de la gestión formal de un "clic" en el banner de cookies ⁴³. El verdadero reto actual es evitar que la acumulación masiva de información derive en asimetrías de poder contundentes que terminen condicionando la libertad real y el ejercicio de los derechos de la ciudadanía en el entorno digital.

4.2 Aplicaciones móviles y permisos

En el ámbito de las aplicaciones móviles, la obtención de datos personales se produce de forma especialmente intensa, ya que muchas de estas aplicaciones requieren acceder a funciones del dispositivo como la ubicación, la cámara, el micrófono, los contactos o el almacenamiento. A ello se añade la intervención de terceros integrados en la propia aplicación, como servicios de analítica, publicidad o medición de uso, que amplían el volumen de información tratada. A diferencia de lo que sucede en la navegación web, gran parte de esta recogida de datos se desarrolla de manera poco visible para el usuario, lo que dificulta que este perciba con claridad el alcance real del tratamiento.

Desde una perspectiva jurídica, este contexto es especialmente sensible porque los permisos técnicos del dispositivo no equivalen por sí mismos a una habilitación jurídica válida. El hecho de que el sistema operativo permita a la aplicación acceder a la geolocalización o a los contactos, no sustituye la exigencia de que el responsable cuente con una base jurídica conforme al RGPD⁴⁴. En este sentido, el principio de licitud no se satisface por la mera posibilidad técnica, sino por la concurrencia de alguna de las bases del art. 6 RGPD, lo que obliga a diferenciar qué tratamientos son necesarios para

⁴³ AEPD. Guía sobre el uso de las cookies, 2023, leído en <https://www.aepd.es/es/documento/guia-cookies.pdf> (Consulta el 25/03/2026).

⁴⁴ Reglamento (UE) 2016/679 (RGPD), arts. 5, 6 y 7.

el servicio y cuáles responden a finalidades adicionales como la publicidad comportamental.⁴⁵

El riesgo principal en este entorno es la acumulación y combinación de múltiples categorías de información. Una sola aplicación puede recabar datos identificativos, datos técnicos e identificadores publicitarios que al combinarse permiten generar inferencias sobre rutinas, lugar de residencia o hábitos de consumo. Desde el punto de vista del RGPD, esta lógica de acumulación debe someterse a los principios de minimización y limitación de la finalidad que exigen que los datos sean adecuados pertinentes y no excesivos.

No basta con aceptar los permisos del sistema operativo, es necesario que el consentimiento sea libre específico informado e inequívoco. En entornos móviles donde el diseño de la interfaz⁴⁶ puede empujar a aceptar de forma rápida, surge la duda de si ese consentimiento refleja una decisión consciente o una aceptación rutinaria condicionada por la funcionalidad de la aplicación. Esta situación tensiona el modelo de legitimación actual y refuerza la necesidad de interpretar de forma estricta las exigencias del RGPD frente a aplicaciones que combinan flujos masivos de datos.

4.3 Códigos QR y Wi-Fi gratuito

Los códigos QR y las redes Wi-Fi gratuitas se han consolidado como mecanismos habituales de acceso rápido a servicios menús digitales o promociones. No obstante, desde la perspectiva de protección de datos, su relevancia no se limita al acto puntual de escanear o conectarse sino al circuito de tratamiento que se activa a partir de ese

⁴⁵ Publicidad comportamental: modalidad publicitaria basada en el seguimiento de la actividad del usuario para elaborar perfiles o inferir intereses y mostrar anuncios personalizados en función de su comportamiento en línea (definición del autor).

⁴⁶ Interfaz: Conexión, física o lógica, entre una computadora y el usuario, un dispositivo periférico o un enlace de comunicaciones. (Diccionario de Lengua Española)

momento. En estos casos, el código QR suele actuar como puerta de acceso a páginas web en las que pueden instalarse herramientas de seguimiento. Por su parte, la conexión a redes Wi-Fi gratuitas puede implicar el tratamiento de identificadores técnicos del dispositivo, lo que permite conocer no solo la conexión del usuario, sino también inferir su presencia física en un determinado espacio.

El elemento jurídicamente relevante es que estos tratamientos suelen ir más allá de la prestación del servicio inmediato. Los datos obtenidos pueden utilizarse para analizar patrones de presencia medir tiempos de permanencia o segmentar usuarios con fines comerciales. Como sostiene la AEPD ⁴⁷, no basta con que el tratamiento sea técnicamente posible, el responsable debe garantizar que el uso de estas tecnologías no suponga una vigilancia injustificada. En este punto cobra especial importancia el “principio de limitación de la finalidad” (art. 5.1.b RGPD), que prohíbe que los datos recogidos para un fin específico, como por ejemplo acceder a una red Wi-Fi o consultar un menú, sean tratados posteriormente de manera incompatible con dicha intención original.

Además, tal y como indica la AEPD en la “Guía para el cumplimiento del deber de informar – 2022”, cuando el acceso al servicio se condiciona a aceptar tratamientos que no son estrictamente necesarios, puede cuestionarse la libertad del consentimiento. Esto es especialmente problemático en el uso de tecnologías de proximidad, ya que el usuario puede no asociar un gesto físico cotidiano con la activación de un tratamiento de datos a gran escala. Esta falta de percepción real sobre el alcance de la tecnología facilita que el consentimiento se convierta en una autorización automática y poco consciente.

⁴⁷ AEPD. Informe Jurídico 0123/2019, sobre el seguimiento de terminales móviles a través de redes Wi-Fi, leído en <https://www.aepd.es/guias/orientaciones-wifi-tracking-seguimiento.pdf> (Consulta el 25/03/2026).

A mi entender, estos escenarios muestran cómo puntos de contacto físicos pueden convertirse en puertas de entrada a sistemas de análisis masivo. Por ello, la exigencia de información clara y la diferenciación entre finalidades obligatorias y accesorias no responde solo a una exigencia formal, sino a la necesidad de garantizar un consentimiento verdaderamente libre y específico. En esta línea, la jurisprudencia del TJUE ha subrayado que, en el entorno digital, el consentimiento no puede presumirse ni obtenerse mediante mecanismos ambiguos o configuraciones que diluyan la voluntad real del usuario. Solo así puede evitarse que el derecho a la protección de datos se convierta en una figura decorativa en el entorno digital ⁴⁸.

4.4 Comercio electrónico y perfilado del usuario

En el comercio electrónico, la captación de datos se produce por dos vías complementarias que encuentran su encaje en las condiciones de licitud del art. 6.1 del RGPD. Por un lado, a través de los datos que el usuario facilita directamente para la celebración del contrato: identificación, dirección de envío y medios de pago. Estos tratamientos se vinculan de forma clara con la finalidad prevista en la letra b) de dicho precepto, ya que son indispensables para la ejecución de la relación comercial.

Por otro lado, se desarrolla una segunda capa de tratamiento basada en el análisis del comportamiento, productos visualizados, tiempo de permanencia, historial de compras o carritos abandonados. Esta dimensión conductual permite a las empresas pasar de una mera transacción a una lógica de predicción de conductas de consumo. En este contexto, el perfilado se convierte en una herramienta estructural del modelo de negocio digital, no se limita a recomendar productos sino que puede utilizarse para segmentar usuarios, personalizar ofertas o incluso modular precios.

⁴⁸ STJUE (Gran Sala), de 1 de octubre de 2019, asunto C-673/17, Planet49, ECLI:EU:C:2019:801.

Jurídicamente el problema radica en que el perfilado no es una práctica neutra. Mientras que los datos básicos se amparan en la necesidad contractual, el análisis de conductas suele desplazarse hacia la letra f) del art. 6.1 RGPD, que permite el tratamiento por "intereses legítimos" del responsable. Sin embargo, esta base jurídica no es una habilitación general, sino que exige una evaluación donde los intereses comerciales de la empresa no pueden prevalecer sobre los derechos y libertades del usuario. Como ha señalado el CEPD,⁴⁹ el perfilado basado en el rastro digital del usuario exige una transparencia reforzada ya que permite a las empresas influir en las decisiones de compra mediante la explotación de sesgos o hábitos de consumo.

A mi juicio, el comercio electrónico muestra la tensión entre la eficiencia económica y el control del individuo, cuanto más afinado es el perfil, mayor es la capacidad de influencia sobre el usuario. Por ello, la exigencia de una transparencia material y el límite a la acumulación de datos constituyen los elementos centrales para que el derecho no quede diluido. En este punto, resulta especialmente relevante la STJUE de 4 de julio de 2023, asunto C-252/21, *Meta Platforms Inc. c. Bundeskartellamt*, en la que el Tribunal aclaró que el tratamiento masivo de datos para fines de publicidad personalizada no puede considerarse sin más, necesario para la ejecución de un contrato.

El TJUE estableció un criterio restrictivo fundamental; para que una empresa pueda ampararse en la necesidad contractual, el tratamiento debe ser objetivamente indispensable para el fin principal del servicio. En dicho caso, se determinó que el usuario no espera razonablemente que su actividad fuera de la plataforma sea monitorizada para ofrecerle anuncios. Al restringir el uso de las bases jurídicas del art.

⁴⁹ CEPD. *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679*. 2018. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en Consulta:25/03/2026.

6.1 del RGPD, el fallo refuerza el control del usuario sobre sus datos, al exigir que para estos tratamientos accesorios, la empresa recabe un consentimiento específico y libre. Esta sentencia marca un antes y un después ya que impide que las grandes plataformas conviertan sus condiciones de uso en una "licencia universal" para el perfilado sistemático.

5. CONSENTIMIENTO DIGITAL Y LÍMITES A LA EXPLOTACIÓN EMPRESARIAL DE DATOS

5.1 El consentimiento como base jurídica del tratamiento en entornos digitales

Una vez identificados los principales mecanismos de captación de datos utilizados por empresas privadas, la cuestión central ya no es únicamente cómo se obtiene la información, sino con qué base jurídica se legitima su tratamiento. En este contexto, el consentimiento ocupa una posición especialmente relevante, ya que en el entorno digital se utiliza con frecuencia para legitimar tratamientos que no resultan estrictamente necesarios para la prestación del servicio principal, como ocurre con la publicidad personalizada, el perfilado comercial o la cesión de datos a terceros con fines analíticos o publicitarios.

Desde la perspectiva del RGPD⁵⁰, el consentimiento constituye una manifestación de voluntad que debe ser libre, específica, informada e inequívoca. Su validez no depende de la mera existencia de una fórmula de aceptación, sino de que el interesado haya podido comprender de manera real el alcance del tratamiento y decidir sin presiones indebidas⁵¹. Por ello, el consentimiento no puede entenderse como una formalidad

⁵⁰ Reglamento (UE) 2016/679 (RGPD), arts. 6 y 7.

⁵¹ CEPD. *Directrices 05/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 2020, párrs. 60-63. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en Consulta: 15/03/2026.

documental, sino como una garantía destinada a preservar el control del individuo sobre su información personal.⁵² En este sentido, como advierte Piñar Mañas, el consentimiento opera como una de las expresiones más claras de la autodeterminación informativa, al permitir que la persona acepte o rechace usos de sus datos que exceden de lo estrictamente necesario para la ejecución del servicio.

En el ámbito de las empresas privadas, esta cuestión adquiere una importancia singular. Los modelos de negocio digitales no se limitan a prestar un servicio, sino que a menudo incorporan finalidades adicionales basadas en la explotación económica de la información personal. De este modo, la base jurídica del consentimiento se convierte en la vía a través de la cual muchas empresas pretenden legitimar tratamientos especialmente intrusivos de datos que no encuentran cobertura ni en la necesidad contractual ni en otras bases del art. 6 RGPD. Precisamente por ello, el análisis jurídico del consentimiento no puede quedarse en su configuración normativa, sino que debe examinar si la voluntad del usuario se forma en condiciones que permitan hablar realmente de una decisión libre y consciente.

A mi entender, el consentimiento sigue siendo una pieza importante del sistema de protección de datos, pero no puede operar como una cláusula general de legitimación al servicio del mercado digital. Su función no es facilitar cualquier tratamiento que resulte útil a la empresa, sino permitir que el interesado conserve un control efectivo sobre aquellas operaciones que afectan de manera relevante a su esfera de libertad.

⁵² PÉREZ ASENSIO, José Manuel. *El consentimiento en la protección de datos*. Aranzadi, 2021, pp. 112-115.

5.2 Límites reales del consentimiento en la economía de los datos

El principal problema del consentimiento en entornos digitales no reside tanto en su configuración normativa, sino en las condiciones reales en las que se presta. En la práctica, la aceptación suele producirse en contextos de fuerte asimetría informativa, mediante interfaces diseñadas para favorecer respuestas rápidas, poco reflexivas y funcionales al interés económico del responsable del tratamiento. De este modo, el consentimiento corre el riesgo de convertirse en un acto rutinario, carente de la deliberación mínima que exige una verdadera manifestación libre de voluntad. En este sentido, como advierte Pérez Asensio en “El consentimiento en la protección de datos - 2021”, el consentimiento solo cumple realmente su función de garantía cuando refleja una decisión formada con conocimiento suficiente sobre el alcance del tratamiento.

Esta dificultad se aprecia con especial claridad en los supuestos analizados en el capítulo anterior: banners de cookies, permisos en aplicaciones móviles, accesos mediante códigos QR o redes Wi-Fi y entornos de comercio electrónico. En todos estos casos, el usuario suele encontrarse ante decisiones fragmentadas, repetitivas y técnicamente complejas que reducen su capacidad de comprender qué datos se recogen, con qué finalidad se tratarán y qué terceros intervendrán en el proceso. Como ha señalado Barrio Andrés, la complejidad de los entornos digitales actuales dificulta que el usuario alcance un conocimiento real y efectivo del alcance del tratamiento.⁵³ El resultado es que el consentimiento puede existir formalmente sin que ello implique una comprensión material del tratamiento.

A ello se añade el fenómeno de la aceptación automática, característico de la economía digital. Como ha advertido el CEPD, determinados diseños de interfaz pueden favorecer

⁵³ BARRIO ANDRÉS, Moisés. *Manual de Derecho Digital*. Ob. Cit., pp. 165-175.

respuestas poco reflexivas y empujar al usuario hacia la aceptación, de modo que el consentimiento termine operando más como una cobertura formal del tratamiento que como una manifestación real de autodeterminación informativa.⁵⁴

En esta línea, el consentimiento condicionado constituye otro de los grandes límites materiales del sistema. Cuando el acceso al servicio se vincula a la aceptación de tratamientos adicionales que no son estrictamente necesarios para la prestación principal, la libertad de elección del usuario queda seriamente comprometida. En estos casos, el problema no es solo la escasez de información, sino la ausencia de una alternativa real. Si el usuario debe ceder datos para acceder a un servicio que desea o necesita, el consentimiento deja de ser una manifestación real de autonomía y se convierte en una adhesión forzada a las condiciones impuestas por la empresa. Esta exigencia resulta coherente con la jurisprudencia del TJUE, que ha rechazado formas de consentimiento obtenidas mediante mecanismos ambiguos o poco transparentes.⁵⁵

Desde esta perspectiva, puede afirmarse que la crisis del consentimiento digital no responde a una insuficiencia teórica, sino a la distancia entre sus exigencias formales y la realidad económica y tecnológica en la que se aplica. Por ello, el análisis jurídico no debe agotarse en verificar si existe una casilla marcada o un texto informativo visible, sino que debe preguntarse si el contexto permite hablar realmente de una voluntad libre, específica e informada. Solo desde esta lectura material puede evitarse que el consentimiento se convierta en una figura vaciada de contenido.

⁵⁴ CEPD. *Directrices 03/2022 sobre patrones engañosos en interfaces de plataformas de redes sociales*, versión final, 14 de marzo de 2023. Leído en: https://www.edpb.europa.eu/system/files/2025-05/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_es.pdf
Consulta: 25/03/2026.

⁵⁵ STJUE (Gran Sala), de 1 de octubre de 2019, asunto C-673/17, *Planet49*, ECLI:EU:C:2019:801.

5.3 Valoración jurídica de la captación y tratamiento de datos personales por empresas privadas

La explotación empresarial de datos personales no puede valorarse únicamente desde la utilidad económica del tratamiento o desde la existencia formal de una base jurídica, sino a la luz del marco de garantías que define hoy la protección de datos como derecho fundamental. En este contexto, la libertad de empresa reconocida en el art. 38 CE ampara sin duda la iniciativa económica y la creación de modelos de negocio innovadores en el entorno digital, pero no puede entenderse como una habilitación autónoma para la explotación ilimitada de la información personal.

Desde esta perspectiva, la valoración jurídica, constitucional y europea de las prácticas empresariales basadas en datos, depende de su adecuación a un conjunto de exigencias ya consolidadas en nuestro ordenamiento: el respeto al art. 18.4 CE, la interpretación conforme derivada del art. 10.2 CE, los estándares del TEDH en materia de vida privada, la centralidad de la CDFUE, cuyo art. 8 reconoce expresamente la protección de datos personales como un derecho fundamental autónomo y las exigencias de finalidad, necesidad, proporcionalidad, transparencia y control efectivo del interesado que concreta el RGPD. Como advierte Llorens Espada, la actividad empresarial no puede apoyarse en la libertad de empresa o en el interés legítimo como si se tratara de una habilitación general, sino que debe someter cada tratamiento a un verdadero juicio de proporcionalidad y equilibrio con los derechos del interesado.⁵⁶

Aplicado a las prácticas analizadas en el presente trabajo, ello permite advertir que no toda captación o reutilización de datos plantea el mismo juicio jurídico. La utilización de cookies, el acceso a permisos en aplicaciones móviles, la recogida de datos mediante

⁵⁶ LLORENS ESPADA, Julen. “El ‘interés legítimo’ de la empresa como base de licitud”, Documentación Laboral, núm. 126, 2022, pp. 27-50.

códigos QR o redes Wi-Fi y el perfilado en el comercio electrónico pueden resultar compatibles con este marco cuando responden a finalidades delimitadas, se apoyan en una base jurídica suficiente y respetan la posición del usuario como titular del derecho. En consecuencia, la licitud del tratamiento no depende solo de su apariencia formal, sino de que garantice de manera efectiva el control del interesado sobre sus datos personales.

Esta exigencia resulta especialmente relevante en el caso de grandes empresas tecnológicas que operan a través de estructuras societarias complejas y con sedes situadas fuera de España o incluso fuera de la UE. La localización formal de la empresa no excluye por sí misma la aplicación del marco europeo de protección de datos cuando el tratamiento se dirige a usuarios situados en territorio europeo o se inserta en actividades orientadas a ese mercado, como puso de manifiesto el TJUE en el asunto *Weltimmo*⁵⁷. Del mismo modo, en *Wirtschaftsakademie Schleswig-Holstein* el Tribunal dejó claro que la complejidad de la estructura tecnológica no puede diluir la responsabilidad por el tratamiento cuando intervienen varios actores en su configuración⁵⁸. En esta misma línea, la sentencia *Fashion ID* confirmó que la participación de terceros en la recogida y transmisión de datos tampoco excluye la exigencia de responsabilidad jurídica respecto del tratamiento realizado⁵⁹. De este modo, la jurisprudencia europea refuerza la idea de que la captación y explotación empresarial de datos solo resulta jurídicamente admisible cuando permanece sometida a límites materiales efectivos, incluso en entornos digitales complejos y transnacionales.

⁵⁷ STJUE, de 1 de octubre de 2015, asunto C-230/14, *Weltimmo*.

⁵⁸ STJUE, de 5 de junio de 2018, asunto C-210/16, *Wirtschaftsakademie Schleswig-Holstein*.

⁵⁹ STJUE, de 29 de julio de 2019, asunto C-40/17, *Fashion ID*.

En cambio, estas prácticas dejan de ser compatibles con ese marco cuando la recogida se amplía de forma continua, se reutiliza para objetivos distintos o se integra en sistemas de seguimiento y segmentación que exceden de lo necesario para la prestación principal del servicio.

Esta misma lógica se aprecia cuando las empresas no se limitan a tratar los datos obtenidos directamente del usuario, sino que recurren además a la adquisición, cesión o cruce de bases de datos procedentes de terceros con fines de segmentación comercial, perfilado o diseño de estrategias empresariales. En estos supuestos, el problema no reside solo en la amplitud de la información tratada, sino en que los datos pasan a circular fuera del contexto en el que fueron inicialmente recabados, lo que puede debilitar la finalidad originaria del tratamiento y reducir de forma significativa el control del afectado sobre su propia información. La jurisprudencia del TJUE ha puesto de manifiesto, además, que la comunicación de datos a terceros con fines comerciales no queda automáticamente legitimada por su utilidad económica, como muestra el asunto *Koninklijke Nederlandse Lawn Tennisbond (KNLTB)*⁶⁰, relativo a la cesión onerosa de datos de miembros a patrocinadores con fines promocionales y que la transmisión de datos entre entidades exige en todo caso garantizar debidamente la información al interesado, tal como subrayó el Tribunal en el asunto *Bara y otros*⁶¹, referido al traslado de datos personales entre administraciones sin información previa suficiente a los afectados. Todo ello evidencia que la comercialización de bases de datos solo puede considerarse jurídicamente admisible cuando respeta de forma estricta las exigencias de base jurídica, finalidad, transparencia y control efectivo que derivan del art. 8 CDFUE y del RGPD. Esta tensión se aprecia con especial claridad en aquellos

⁶⁰ STJUE, de 4 de octubre de 2024, asunto C-621/22, *Koninklijke Nederlandse Lawn Tennisbond (KNLTB)*.

⁶¹ STJUE, de 1 de octubre de 2015, asunto C-201/14, *Bara y otros*.

modelos de negocio que convierten la información personal en un recurso de explotación constante.

En esta línea, Zuboff ha señalado que la economía digital contemporánea tiende a transformar la experiencia del individuo en recurso básico para procesos de análisis, predicción y modulación de la conducta.⁶² Desde el punto de vista, todo ello exige un control especialmente estricto sobre aquellas prácticas que, aunque se presenten como normales dentro del funcionamiento del mercado digital, terminan tratando la información personal como un recurso económico disponible sin tener suficientemente en cuenta los derechos de su titular.

A mi juicio, este es el verdadero núcleo del problema. El análisis realizado a lo largo del trabajo permite sostener que la legitimidad de las prácticas empresariales basadas en datos no depende solo de su viabilidad técnica o de su rentabilidad económica, sino de su compatibilidad material con el sistema de garantías constitucionales y europeas que protege a la persona frente al poder derivado del control de la información personal. En este sentido, como advierte Pérez Luño, el desarrollo tecnológico solo resulta compatible con el marco jurídico cuando permanece al servicio de la persona y de sus derechos fundamentales.⁶³ Por ello, la explotación empresarial de datos personales solo puede considerarse jurídicamente admisible cuando se mantiene dentro de un marco que preserve la dignidad, la libertad y la capacidad de control del individuo sobre su propia información, impidiendo que los datos personales queden reducidos a un mero recurso económico disponible para el mercado.

⁶² ZUBOFF, Shoshana. *La era del capitalismo de vigilancia*. Ob. Cit., pp. 25-40.

⁶³ PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Tecnos, Madrid, 2012.

6. CONCLUSIONES

- I. Una vez analizado el derecho a la protección de datos personales desde su dimensión constitucional, europea y legislativa, puede afirmarse que no nos encontramos ante una garantía meramente accesorio, sino ante un verdadero derecho fundamental autónomo, estrechamente vinculado a la dignidad, la libertad y la autodeterminación informativa de la persona. En este sentido, el trabajo ha permitido comprobar que el art. 18.4 CE no define por completo el contenido del derecho, sino que este se construye en interacción continua con el art. 10.2 CE, con la jurisprudencia constitucional y europea y de forma especialmente relevante, con el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
- II. El trabajo muestra que la protección de datos personales no se limita a evitar intromisiones en la intimidad en sentido clásico, sino que tiene como finalidad garantizar que el individuo conserve un control real sobre la obtención, uso, circulación y conservación de su información. Esta idea resulta especialmente importante en el entorno digital, donde la recopilación de datos no se produce únicamente a partir de aquello que el usuario comunica de forma expresa, sino también mediante técnicas de observación o rastreo capaces de reconstruir hábitos, preferencias y pautas de comportamiento.
- III. En relación con las empresas privadas, el trabajo confirma que la captación de datos personales se ha convertido en un elemento estructural de la economía digital. Cookies, rastreadores, permisos en aplicaciones móviles, códigos QR, redes Wi-Fi y mecanismos propios del comercio electrónico muestran que gran parte del tratamiento de datos se desarrolla en contextos cotidianos, automatizados y poco visibles para el usuario. Ello explica que el verdadero

problema jurídico no resida solo en la existencia del tratamiento, sino en el modo en que este se articula, en las finalidades que persigue y en el grado de transparencia y control que se reconoce al afectado.

- IV. A lo largo del trabajo se ha podido comprobar que el consentimiento ocupa una posición central dentro del sistema de protección de datos, pero también que su funcionamiento en la práctica se aleja en muchos casos de la idea de consentimiento libre, específico, informado e inequívoco que exige el RGPD. En muchos entornos digitales, la aceptación se produce en condiciones de asimetría informativa, mediante diseños de interfaz que favorecen respuestas rápidas y poco meditadas, lo que debilita de forma considerable la capacidad del usuario para comprender el verdadero alcance del tratamiento. Por ello, el consentimiento no puede seguir interpretándose como una simple formalidad documental, sino como una garantía que solo cumple su función cuando preserva una decisión auténticamente libre y consciente.
- V. Del análisis de los distintos mecanismos de captación puede afirmarse que no toda práctica empresarial plantea el mismo juicio jurídico. Existen tratamientos que pueden considerarse compatibles con el marco de protección de datos cuando responden a finalidades delimitadas, resultan necesarios para la prestación del servicio y respetan una base jurídica suficiente. Sin embargo, dejan de serlo cuando la recogida se amplía de forma continua, se reutiliza para objetivos distintos o se integra en sistemas de rastreo y segmentación que exceden de lo necesario para la relación inicial con el usuario. En estos casos, la licitud del tratamiento no puede apreciarse solo desde un plano formal, sino desde su compatibilidad real con el sistema de garantías.

- VI. El comercio electrónico y los modelos de negocio basados en la publicidad personalizada permiten apreciar con especial claridad esta tensión. La investigación realizada muestra que el tratamiento de datos deja de ser un mero soporte del servicio para convertirse en muchos casos, en el auténtico núcleo económico de la actividad empresarial. El perfilado, la personalización de ofertas y la reutilización de información convierten al usuario en una fuente constante de datos y a su comportamiento en un objeto de análisis y predicción. Desde esta perspectiva, la información personal deja de cumplir solo una función vinculada al servicio y pasa a integrarse en una lógica de explotación económica continuada.
- VII. Una de las cuestiones más relevantes que muestra este trabajo es la creciente importancia de la cesión, adquisición y cruce de bases de datos procedentes de terceros. Estas prácticas intensifican el riesgo jurídico porque los datos pasan a circular fuera del contexto en el que fueron inicialmente recabados, debilitando la finalidad originaria del tratamiento y reduciendo la capacidad real de control del afectado. En este sentido, la utilidad comercial de la información no basta por sí sola para justificar su circulación empresarial, ya que la comercialización de datos personales solo resulta admisible cuando respeta de manera estricta las exigencias de base jurídica, transparencia, finalidad y control efectivo propias del derecho fundamental a la protección de datos.
- VIII. Además, el trabajo permite afirmar que la dimensión transnacional de muchas empresas tecnológicas no excluye la aplicación del estándar europeo de protección de datos. El hecho de que determinadas compañías operen desde estructuras societarias complejas o con sedes situadas fuera de España o de la Unión Europea no las sitúa al margen del marco jurídico europeo cuando sus

actividades se dirigen a usuarios situados en territorio europeo. Esta idea refuerza la necesidad de entender la protección de datos no como un límite puramente interno del ordenamiento español, sino como una garantía cuyo contenido se proyecta en un espacio jurídico europeo más amplio y especialmente exigente.

- IX. A mi juicio, uno de los resultados más importantes del trabajo es haber constatado que la libertad de empresa reconocida en el art. 38 CE no puede operar como un título general de legitimación para la explotación ilimitada de la información personal. La actividad económica digital puede utilizar datos personales en determinados supuestos, pero no puede tratarlos como si fueran un activo disponible al margen de los derechos fundamentales de su titular. En consecuencia, la protección de datos no impide la actividad económica, pero sí exige que esta se desarrolle dentro de límites que eviten convertir la información personal en un mero instrumento de rentabilidad empresarial.
- X. En definitiva, el trabajo permite concluir que la cuestión central ya no es si las empresas privadas pueden captar y tratar datos personales, sino bajo qué condiciones dicho tratamiento puede considerarse jurídicamente admisible. La respuesta no depende únicamente de la existencia de una base jurídica aparente o de una cláusula de aceptación, sino de que el tratamiento respete de manera efectiva la finalidad para la que fue recabado, la transparencia debida, la proporcionalidad de la medida y el control real del individuo sobre su propia información. Solo desde esta apreciación material puede evitarse que el derecho a la protección de datos quede vacío de contenido en la economía digital actual.

7. BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial*. 2020. Leído en: <https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf> Consulta: 15/03/2026.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para el cumplimiento del deber de informar*. 2022. Leído en: <https://www.aepd.es/documento/guia-modelo-clausula-informativa.pdf> Consulta: 15/03/2026.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía sobre el uso de las cookies*. 2023. Leído en: <https://www.aepd.es/documento/guia-cookies.pdf> Consulta: 25/03/2026.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe Jurídico 0123/2019, sobre el seguimiento de terminales móviles a través de redes Wi-Fi*. Leído en: <https://www.aepd.es/guias/orientaciones-wifi-tracking-seguimiento.pdf> Consulta: 25/03/2026.
- BARRIO ANDRÉS, Moisés. *Manual de Derecho Digital*. Tirant lo Blanch, Valencia, 2023.
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Directrices 03/2022 sobre patrones engañosos en interfaces de plataformas de redes sociales*. Versión final, 2023. Leído en: https://www.edpb.europa.eu/system/files/2025-05/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_es.pdf Consulta: 25/03/2026.
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el*

- contexto de la COVID-19*. 2020. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en Consulta: 15/03/2026.
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Directrices 05/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*. 2020. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en Consulta: 15/03/2026.
 - COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Directrices 07/2020 sobre los conceptos de responsable y encargado del tratamiento*. Versión final, 2021. Leído en: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_es.pdf Consulta: 15/03/2026.
 - COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679*. 2018. Leído en: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en Consulta: 25/03/2026.
 - LLORENS ESPADA, Julen. “El ‘interés legítimo’ de la empresa como base de licitud”, *Documentación Laboral*, núm. 126, 2022.
 - PÉREZ ASENSIO, José Manuel. *El consentimiento en la protección de datos*. Aranzadi, 2021.
 - PÉREZ LUÑO, Antonio Enrique. *Los derechos humanos en la sociedad tecnológica*. Tecnos, Madrid, 2012.
 - PIÑAR MAÑAS, José Luis. “El derecho fundamental a la protección de datos personales”, en PIÑAR MAÑAS, José Luis (dir.), *Reglamento General de*

Protección de Datos. Hacia un nuevo modelo europeo de privacidad. Reus, Madrid, 2016.

- RODOTÀ, Stefano. *La vida y las reglas. Entre el Derecho y el no Derecho.* Trotta, Madrid, 2010.
- ZUBOFF, Shoshana. *La era del capitalismo de vigilancia: la lucha por un futuro humano frente a las nuevas fronteras del poder.* Paidós, Barcelona, 2020.

8. OTROS MATERIALES UTILIZADOS

A. Sentencias

Jurisprudencia española

- STS 1/1985, de 11 de abril.
- STC 94/1998, de 4 de mayo.
- STC 69/1999, de 26 de abril.
- STC 290/2000, de 30 de noviembre.
- STC 292/2000, de 30 de noviembre.
- STC 170/2013, de 7 de octubre.

Jurisprudencia del Tribunal Europeo de Derechos Humanos

- STEDH, Amann c. Suiza, de 16 de febrero de 2000.
- STEDH, Rotaru c. Rumanía, de 4 de mayo de 2000.
- STEDH, S. y Marper c. Reino Unido, de 4 de diciembre de 2008.

Jurisprudencia del Tribunal de Justicia de la Unión Europea

- STJUE, de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd.
- STJUE, de 13 de mayo de 2014, asunto C-131/12, Google Spain SL y Google Inc. c. AEPD y Mario Costeja González.

- STJUE, de 1 de octubre de 2015, asunto C-201/14, Bara y otros.
- STJUE, de 1 de octubre de 2015, asunto C-230/14, Weltimmo.
- STJUE, de 6 de octubre de 2015, asunto C-362/14, Schrems.
- STJUE, de 5 de junio de 2018, asunto C-210/16, Wirtschaftsakademie Schleswig-Holstein.
- STJUE, de 29 de julio de 2019, asunto C-40/17, Fashion ID.
- STJUE (Gran Sala), de 1 de octubre de 2019, asunto C-673/17, Planet49.
- STJUE, de 16 de julio de 2020, asunto C-311/18, Schrems II.
- STJUE, de 4 de octubre de 2024, asunto C-621/22, Koninklijke Nederlandse Lawn Tennisbond (KNLTB).

B. Normativa utilizada

Normativa española

- Constitución Española, BOE núm. 311, de 29 de diciembre de 1978.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm. 166, de 12 de julio de 2002.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, BOE núm. 17, de 19 de enero de 2008.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, BOE núm. 294, de 6 de diciembre de 2018.

Normativa europea e internacional

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4 de noviembre de 1950.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

- Carta de los Derechos Fundamentales de la Unión Europea, DOUE C 326, de 26 de octubre de 2012.
- 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, DOUE L 119, de 4 de mayo de 2016.