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

Becerra Morata, Ana. *Diseño adictivo o engañoso de plataformas digitales i validez del consentimiento : un análisis del marco normativo vigente*. Treball de Final de Grau (Universitat Autònoma de Barcelona), 2026 (Dret). 36 pàg.

This version is available at <https://ddd.uab.cat/record/331941>

under the terms of the  license.



**Universitat Autònoma
de Barcelona**

**DISEÑO ADICTIVO O ENGAÑOSO DE PLATAFORMAS DIGITALES Y
VALIDEZ DEL CONSENTIMIENTO: UN ANÁLISIS DEL MARCO
NORMATIVO VIGENTE**

GRADO EN DERECHO

Trabajo de Fin de Grado en Derecho

Autora: Ana Becerra Morata

Tutora: Maria Barcons Campmajó

Curso académico 2025-2026

13 de mayo de 2026

RESUMEN

Cuando usamos redes sociales o plataformas digitales, creemos que estamos tomando decisiones libres. Pero su arquitectura está creada para lo contrario. Cada notificación, cada *scroll* infinito, cada recomendación algorítmica ha sido esencialmente diseñada para extraer nuestros datos personales. No pagamos con dinero, pagamos con nuestros datos, información y atención. Los términos y condiciones son intencionadamente complicados, el consentimiento se solicita de manera que nos fatiga, y los patrones de diseño están hechos a milímetro para que hagamos exactamente lo que las plataformas quieren. Vivimos un espejismo de una presunta libertad de elección, que está totalmente condicionada.

Los algoritmos conocen nuestras vulnerabilidades, nuestros datos se utilizan contra nosotros: para definirnos y clasificarnos. Esto genera una problemática jurídica fundamental. Según el Reglamento General de Protección de Datos, para que el consentimiento sea válido debe ser una manifestación de voluntad libre, específica, informada e inequívoca. Pero cuando el entorno está diseñado para influir en tus decisiones, cuando no puedes entender cómo funcionan realmente los algoritmos, cuando el cansancio de consentimiento te hace aceptar sin pensar ¿puede ese consentimiento realmente considerarse válido?

La respuesta formal es que la ley ya lo prohíbe. La Ley de Servicios Digitales, el RGPD, la Directiva sobre Prácticas Comerciales Desleales y la Agencia Española de Protección de Datos prohíben y declaran que el diseño manipulador y los patrones adictivos violan principios de la protección de datos. El marco regulatorio existe, la aplicación efectiva no. Todavía no hay jurisprudencia que condene a una plataforma por diseño adictivo y persuasivo o consentimiento inválido. Las plataformas continúan sus prácticas porque las consecuencias legales son mínimas.

Este trabajo examina si la ley actual puede realmente protegernos en una nueva era digital o si la brecha entre lo que la ley establece y lo que realmente se aplica ha derivado en la necesidad de una intervención más exhaustiva.

Palabras clave: adicción digital, validez del consentimiento, diseño persuasivo, patrones oscuros, manipulación algorítmica, RGPD, Ley de Servicios Digitales.

ABSTRACT

When we use social media or digital platforms, we believe we are making free choices. But their architecture is created for the opposite. Every notification, every infinite scroll, every algorithmic recommendation has been essentially designed to extract our personal data. We do not pay with money, we pay with our data, information, and attention. Terms and conditions are intentionally complicated, consent is requested in ways that exhaust us, and design patterns are crafted to the millimeter to make us do exactly what platforms want. We live in the illusion of a presumed freedom of choice that is entirely conditioned.

Algorithms know our vulnerabilities, our data is used against us: to define and classify us. This generates a fundamental legal problem. According to the General Data Protection Regulation, for consent to be valid it must be a manifestation of free, specific, informed, and unequivocal will. But when the environment is designed to influence your decisions, when you cannot understand how algorithms work, when consent fatigue makes you accept without thinking, can that consent really be considered valid?

The formal answer is that the law already prohibits it. The Digital Services Act, the GDPR, the Unfair Commercial Practices Directive, and the Spanish Data Protection Agency prohibit and declare that manipulative design and addictive patterns violate data protection principles. The regulatory framework exists, effective protection does not. There is still no case law condemning a platform for addictive and persuasive design or invalid consent. Platforms continue their practices because legal consequences remain minimal.

This work examines whether current law can truly protect us in a new digital era, or whether the gap between what the law establishes and what is enforced has created the need for more exhaustive intervention.

Keywords: digital addiction, consent validity, persuasive design, dark patterns, algorithmic manipulation, GDPR, Digital Services Act.

ÍNDICE

1	INTRODUCCIÓN	5
1.1	Planteamiento del problema: adicción digital y manipulación algorítmica.....	5
1.2	Objetivo del trabajo	6
1.3	Hipótesis y cuestiones planteadas	6
1.4	Metodología utilizada	7
2	MARCO TEÓRICO	8
2.1	El diseño persuasivo en las plataformas digitales: concepto y funcionamiento.....	8
2.2	La adicción digital como fenómeno con relevancia jurídica	9
3	MARCO NORMATIVO EUROPEO	12
3.1	Reglamento de Servicios Digitales (DSA 2022/2065).....	12
3.2	Reglamento General de Protección de datos (RGPD 2016/679)	15
3.3	Directiva 2005/29/CE sobre prácticas comerciales desleales.....	19
4	MARCO JURÍDICO ESPAÑOL	21
4.1	Ley General para la Defensa de los Consumidores y Usuarios	22
4.2	Agencia Española de Protección de Datos (AEPD).....	23
4.2.1	Guía sobre patrones adictivos y engañosos	23
4.2.2	Resolución relevante	25
4.3	Constitución Española.....	26
5	ANÁLISIS JURÍDICO Y CRÍTICO	27
5.1	El consentimiento en plataformas digitales.....	27
5.2	Límites e insuficiencias de la regulación vigente	28
6	CONCLUSIONES	30
7	REFERENCIAS.....	34

1 INTRODUCCIÓN

1.1 Planteamiento del problema: adicción digital y manipulación algorítmica

En la actualidad, las plataformas digitales se han convertido en un elemento central de la vida cotidiana. Sin embargo, estas no se limitan a ofrecer contenidos o servicios favorables, sino que están diseñadas para captar nuestra atención mediante algoritmos y patrones adictivos (AEPD, 2024). Este modelo se basa en técnicas como la personalización continua del contenido, el *scroll infinito*¹ o las notificaciones intermitentes, entre muchas otras. El Parlamento Europeo (2023) ha advertido expresamente de la naturaleza adictiva de estos servicios digitales, que explotan las vulnerabilidades de las personas usuarias para captar su atención, mantenerlas conectadas el mayor tiempo posible y monetizar sus datos.

La problemática jurídica surge cuando la capacidad de la persona para decidir cuándo cesar el uso de la plataforma se ve comprometida. Esto no es nuevo: Schüll (2012) demostró que las máquinas tragaperras de Las Vegas están deliberadamente diseñadas para mantener a la persona jugando el mayor tiempo posible, mediante entornos y sistemas de pequeñas recompensas que dificultan la decisión de parar (Schüll, 2012). Las plataformas digitales operan de una manera similar. En este sentido, el problema no radica únicamente en el uso intensivo de las plataformas, sino en la propia arquitectura del entorno digital, que está diseñada para aumentar la permanencia de la persona en él.

Desde esta perspectiva, el análisis se centra en la validez del consentimiento en el entorno digital. Si la persona actúa en un contexto diseñado para influir en su comportamiento, surge la duda de si dicho consentimiento cumple realmente con los requisitos de libertad exigidos por el ordenamiento jurídico. Ya que cabe preguntarse: ¿Es plenamente libre la decisión de permanecer en la plataforma? ¿Puede el Derecho seguir tratando el uso de plataformas digitales como un simple ejercicio de libertad individual, o debe hacer una intervención más exhaustiva para proteger de la adicción?

Este trabajo parte de la premisa de que el Derecho no puede ser neutral ante una tecnología que no solo facilita el acceso a la información, sino que influye activamente

¹ El desplazamiento infinito por la pantalla (denominado en inglés *scroll infinito*) es una técnica de diseño que permite a la persona desplazarse sin limitaciones por el contenido, que se carga de forma continua sin que exista un punto final, en lugar de organizarse en diferentes páginas (AEPD, 2024, p. 17).

en el comportamiento de los ciudadanos respecto al uso de las redes sociales o plataformas afines. Por tanto, se propone analizar si el marco normativo vigente ofrece una respuesta adecuada a este fenómeno, o si, por el contrario, existen lagunas en la regulación de los diseños algorítmicos persuasivos.

1.2 Objetivo del trabajo

El objetivo del presente trabajo es analizar la licitud del uso de algoritmos de diseño persuasivo por parte de las plataformas digitales, evaluando si el marco normativo vigente en la Unión Europea y en España garantiza adecuadamente la validez del consentimiento de la persona usuaria.

Objetivos específicos

- i. Examinar el concepto de algoritmos de diseño adictivo o engañosos y su funcionamiento en las plataformas digitales.
- ii. Analizar el marco jurídico vigente aplicable a estas prácticas (normativa europea y española).
- iii. Evaluar si el consentimiento de la persona usuaria, en entornos digitales diseñados para influir en su comportamiento, cumple con los requisitos de validez exigidos por el ordenamiento jurídico.
- iv. Identificar los límites del marco normativo actual en relación con el uso de técnicas de diseño persuasivo por parte de las plataformas digitales.

1.3 Hipótesis y cuestiones planteadas

La utilización de algoritmos de diseño persuasivo por parte de las plataformas digitales plantea dudas sobre la validez del consentimiento de la persona usuaria, en la medida en que puede no reflejar una decisión plenamente libre. Lo que podría dar lugar a responsabilidad jurídica de las plataformas, de forma análoga a la regulación de otros productos con potencial adictivo.

- i. ¿Son jurídicamente lícitas las técnicas de diseño persuasivo utilizadas por las plataformas digitales a la luz del Derecho vigente?
- ii. ¿Es válido el consentimiento de la persona usuaria cuando las plataformas digitales utilizan diseños persuasivos para influir en su comportamiento?

- iii. ¿En qué medida el marco normativo actual permite abordar los efectos derivados del diseño algorítmico persuasivo?

1.4 Metodología utilizada

El presente trabajo se desarrolla mediante una metodología jurídico-dogmática complementada con un análisis crítico. La estructura metodológica se organiza en tres fases.

En primer lugar, se realiza una revisión de literatura académica sobre el diseño adictivo de las plataformas digitales y sus implicaciones jurídicas, tomando como referencia las aportaciones de Llana (2019) sobre la explotación de los datos personales en el entorno digital, de Barrio Andrés (2025) sobre el derecho digital, de Ponce Solé (2023) sobre manipulación, *nudging* digital y patrones oscuros, de Mato Pacín (2024) sobre los aspectos jurídicos del diseño de interfaces, y de Schüll (2012) sobre el diseño adictivo en la industria del juego. Esta fase teórica permite identificar los conceptos fundamentales y los problemas jurídicos derivados del diseño persuasivo.

En segundo lugar, se lleva a cabo un análisis jurídico-dogmático del marco normativo europeo y español aplicable. A nivel europeo se examina el Reglamento de Servicios Digitales (Reglamento (UE) 2022/2065), el Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) y la Directiva 2005/29/CE sobre prácticas comerciales desleales. A nivel nacional se analiza la Ley General para la Defensa de los Consumidores y Usuarios, con mención a la Ley 3/1991 de Competencia Desleal y por último la Constitución Española. Este análisis normativo se complementa con el estudio de documentos institucionales relevantes: la Guía de la Comisión Europea (2021) sobre la interpretación de la Directiva 2005/29/CE, las Directrices 03/2022 del Comité Europeo de Protección de Datos sobre patrones de diseño engañosos, el informe de la Agencia Española de Protección de Datos (2024) sobre patrones adictivos, la Resolución de la AEPD en el procedimiento PS/00080/2023 y la Resolución del Parlamento Europeo de 12 de diciembre de 2023 sobre el diseño adictivo de los servicios en línea.

Debe señalarse que, dada la novedad del fenómeno analizado, no existe hasta la fecha jurisprudencia española ni europea que aborde directamente la incidencia del diseño adictivo sobre la validez del consentimiento de la persona usuaria. El único precedente relevante en el ámbito español es la resolución de la Agencia Española de

Protección de Datos² (en adelante, AEPD) en el procedimiento PS/00080/2023, primera sanción en España por el uso de patrones oscuros, que se analiza en la sección 4.2.2. Esta ausencia de pronunciamientos judiciales no invalida el análisis propuesto, sino que confirma precisamente la necesidad de un estudio dogmático que examine si el marco normativo vigente ofrece herramientas suficientes para responder a esta problemática.

2 MARCO TEÓRICO

2.1 El diseño persuasivo en las plataformas digitales: concepto y funcionamiento

Cuando navegamos por internet creemos estar tomando decisiones libres. Pero la realidad es que el entorno en el que tomamos esas decisiones no es neutro, sino que ha sido cuidadosamente diseñado para guiarnos en una dirección específica. Ponce Solé (2023) lo explica a través del concepto de arquitectura de la elección: la forma en que se presentan las opciones afecta directamente a lo que elegimos, incluso sin que nos demos cuenta. Mato Pacín (2024) añade que el éxito de la comunicación digital no depende solo de qué se nos dice, sino de cómo se nos dice. Las plataformas saben esto muy bien y utilizan ese conocimiento para influir en nuestro comportamiento de maneras que a menudo contradicen nuestras verdaderas preferencias.

Cuando ese diseño se vuelve deliberadamente manipulador, nos encontramos ante lo que se conoce como patrones oscuros: técnicas mediante las que los diseñadores explotan lo que saben sobre cómo pensamos y decidimos para llevarnos a hacer cosas que no querríamos hacer si tuviéramos libertad real (Mato Pacín, 2024). Lo peculiar de estos patrones es que afectan no solo a nuestras acciones, sino también a nuestro consentimiento: nos llevan a aceptar cosas sin ser plenamente conscientes de lo que estamos aceptando.

¿Cómo es posible? Porque somos más previsibles de lo que nos gustaría creer. Los psicólogos Tversky y Kahneman demostraron hace décadas que nuestro pensamiento no es tan racional como creemos. Recurrimos constantemente a atajos mentales para tomar decisiones rápidas sin gastarnos toda la energía cognitiva disponible (Ponce Solé, 2023). El problema es que esos atajos producen errores sistemáticos y predecibles. Los patrones oscuros están diseñados precisamente para

² La Agencia Española de Protección de Datos es “la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de la ciudadanía” (AEPD, 2025)

activar esos errores: nos empujan a pensar rápido e intuitivamente, sin dejarnos tiempo para reflexionar.

Llaneza (2019) describe esto a partir del trabajo del exdiseñador de Google Tristan Harris. Las plataformas controlan qué opciones ves y cuáles no. Deciden qué se ve destacado y qué queda oculto. Transforman lo que debería ser una experiencia puntual en un flujo infinito que te mantiene consumiendo. Como dice Llaneza con una frase que resume todo: “la libertad de elección es ilusoria si no se puede diseñar el menú” (Llaneza, 2019, p. 126). Y lo más irónico es que cuando las plataformas hablan de sí mismas dicen cosas como “solo facilitamos que el usuario vea el vídeo que quiere ver” o “solo recabamos los datos que el usuario libremente nos da”. Pero eso no es verdad. Tu libre albedrío está siendo limitado por técnicas aplicadas por una razón muy simple: el dinero (Llaneza, 2019).

El problema se vuelve exponencialmente peor con la llegada de la inteligencia artificial. Ahora las plataformas no solo tienen técnicas de manipulación: tienen datos sobre ti. Mato Pacín (2024) explica que tu interacción constante con dispositivos conectados genera una enorme cantidad de información sobre tu comportamiento. Esos datos alimentan algoritmos que pueden personalizar la experiencia de manera casi quirúrgica, dirigiéndose a tus vulnerabilidades específicas. Las plataformas pueden saber qué tipo de estímulos funcionan contigo, cuánto tiempo invertirías buscando una forma de cancelar tu suscripción antes de rendirte, o si te sentirías culpable ante cierto tipo de mensaje. Y lo más inquietante: pueden cambiar la interfaz constantemente para optimizar lo que te mantiene enganchado (Mato Pacín, 2024). Como observa Llaneza (2019), nadie discute que los servicios están diseñados para ser adictivos a propósito. Pero cuando hablamos de adicción digital, tendemos a culpar a la persona por no tener fuerza de voluntad, cuando en realidad deberíamos estar mirando a los diseñadores.

2.2 La adicción digital como fenómeno con relevancia jurídica

La historia de cómo las plataformas digitales crean adicción no es completamente nueva. Las máquinas tragaperras de Las Vegas ya lo sabían hace décadas. Llaneza (2019) señala que las plataformas usan exactamente las mismas técnicas que la industria del juego. Y lo más inquietante es que funcionan igual de bien. Llaneza cita estudios que demuestran que estos métodos son tan efectivos que pueden activar mecanismos similares a la cocaína en el cerebro, crear necesidades psicológicas e incluso provocar

«llamadas y notificaciones fantasma», en las que los usuarios perciben el zumbido de un teléfono inteligente, incluso cuando no está realmente allí (Busby, 2018).

La investigadora Natasha Schüll pasó quince años estudiando las máquinas tragaperras de Las Vegas y llegó a una conclusión: la adicción no es un problema psicológico del individuo, sino un resultado de cómo la máquina está diseñada para interactuar con esa persona (Schüll, 2012). Las máquinas usan lo que Schüll llama “bucles lúdicos”: ciclos repetidos de incertidumbre, anticipación y recompensa que mantienen a la persona jugando. Lee (2014), reseñando el trabajo de Schüll, subraya que esto significa que la responsabilidad no está en la persona sino en quien diseña el sistema. Y lo aterrador es que esas mismas técnicas están en todas partes en internet. Llanea (2019) muestra cómo en *Snapchat*, en el desplazamiento infinito de redes sociales, en juegos como *CandyCrush*: todos ellos crean deliberadamente esos mismos ciclos de incertidumbre y recompensa. Todos están contruidos para ser adictivos exactamente de la misma manera que las máquinas tragaperras.

Pero aquí es donde entra la dimensión jurídica. Esto no es solo un problema de hábitos poco saludables. La atención está íntimamente ligada a la libertad y a la voluntad humana. Ponce Solé (2023) advierte que la manipulación a gran escala por diseño digital perjudica a ambas. Sin libertad de atención no puede haber libertad de pensamiento. John Stuart Mill, en su obra clásica “Sobre la libertad”, explicaba que la libertad de pensamiento comprende el dominio interior de la conciencia; la libertad absoluta de opinión y sentimiento sobre todos los temas y la libertad de gustos y actividades; de trazar el plan de nuestra vida de acuerdo con nuestro propio carácter (Mill, 1859). Un diseño digital que aprovecha los sesgos para manipular y captar la atención puede menoscabar directamente este derecho constitucional a la libertad de pensamiento, íntimamente ligado a la dignidad y al libre desarrollo de la personalidad (Ponce Solé, 2023).

Barrio Andrés (2025) advierte de que estamos viviendo lo que él llama el “eclipse de la autonomía de la persona en la época del capitalismo algorítmico” (p. 291). Constantemente se está recopilando información sobre nosotros, y esa información se está usando para construir algoritmos que deciden qué eres, quién eres, qué te gusta y quién serás. Tu identidad está siendo construida por máquinas, no por ti. Y el riesgo es que termines siendo juzgado no por lo que haces sino por lo que la máquina predice que

harás (Barrio Andrés, 2025). Barrio Andrés (2025) señala además que expertos de todo el mundo hablan de la urgencia de proteger los derechos digitales de las personas, de garantizar privacidad real, de crear un ciberespacio que sea realmente libre y abierto. Pero cuando miramos la Constitución Española, no encontramos esas protecciones. De hecho, hay quien piensa que la propia Constitución necesitaría ser reformada para responder a estos retos (Barrio Andrés, 2025).

Y aquí está lo más importante: Mato Pacín (2024) señala que la idea tradicional de “persona vulnerable” ya no tiene sentido en el mundo digital. Solía pensarse que algunos grupos eran más vulnerables que otros. Pero cuando la inteligencia artificial personaliza los patrones oscuros dirigiéndose específicamente a tus vulnerabilidades individuales, todos nos convertimos en vulnerables. El usuario medio es tan manipulable como cualquier otro cuando el diseño está optimizado para encontrar exactamente dónde presionar (Mato Pacín, 2024).

Sin embargo, existe otro problema que complica aún más la situación del consentimiento. Mato Pacín (2024) identifica que la opacidad y complejidad de muchas de las prácticas de recopilación automática de datos obstaculizan que el usuario medio pueda entender el lenguaje e implicaciones de las advertencias o los clausulados de privacidad que debe aceptar. Además, la existencia de continuos avisos y peticiones de consentimiento durante la navegación genera lo que se conoce como *privacy fatigue* o cansancio de privacidad. Este fenómeno produce una alta percepción de protección que, paradójicamente, da lugar a un mayor nivel de exposición en la práctica: las personas, cansadas de ser constantemente interrogadas, terminan aceptando consentimientos que no deberían aceptar (Mato Pacín, 2024).

Así que cuando una persona decide quedarse en una plataforma, ¿está eligiendo libremente? ¿O está siendo mantenida allí por un entorno que ha sido diseñado específicamente para explotar cómo funciona su mente? Si el consentimiento para usar esa plataforma, o para que tus datos sean tratados de cierta forma, fue dado bajo la influencia de todos estos mecanismos de manipulación, bajo la opacidad de lo que realmente está aceptando, y bajo el cansancio de privacidad que la ha llevado a ceder sin reflexionar, ¿es realmente un consentimiento válido desde el punto de vista jurídico? Esa es la pregunta central que este trabajo intenta responder.

3 MARCO NORMATIVO EUROPEO

3.1 Reglamento de Servicios Digitales (DSA 2022/2065)

El Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales, conocido como *Digital Services Act* o DSA, constituye un pilar muy importante del nuevo marco regulador europeo en materia de plataformas digitales. Entró en vigor el 16 de noviembre de 2022 y resulta plenamente aplicable desde el 17 de febrero de 2024, siendo de aplicación directa en todos los Estados miembros al tratarse de un reglamento.

El DSA resulta especialmente relevante para el objeto de este trabajo porque aborda, por primera vez en el Derecho de la Unión Europea (en adelante, UE), la influencia que el diseño del entorno digital puede tener sobre la capacidad de tomar decisiones de las personas usuarias. En este sentido, introduce disposiciones que inciden en la protección de la voluntad libre del usuario frente a las técnicas de diseño persuasivo empleadas por las plataformas. A continuación, se analizan los preceptos más relevantes desde esta perspectiva.

a) Artículo 25: Diseño y organización de interfaces en línea

El artículo 25 del DSA constituye la disposición central en materia de diseño manipulativo de interfaces. Establece que los prestadores de plataformas en línea no podrán diseñar, organizar u operar sus interfaces de un modo que engañe o manipule a los destinatarios del servicio, ni de un modo que distorsione o menoscabe de forma sustancial la capacidad de dichos destinatarios para tomar decisiones libres e informadas. (Reglamento (UE) 2022/2065, art. 25.1).

Se trata de la primera norma de la UE que codifica y prohíbe expresamente los denominados *dark patterns*³ en las interfaces en línea. Si bien el artículo no emplea dicha expresión, el considerando 67 aclara que la prohibición abarca estas prácticas, definiéndolas como aquellas estructuras, diseños o funcionalidades de las interfaces que distorsionan o menoscaban la capacidad del usuario para adoptar decisiones autónomas e informadas. Entre los ejemplos que el considerando ofrece se incluyen la presentación

³ Los patrones oscuros (en inglés, *dark patterns*) son, según la Agencia Española de Protección de Datos, “interfaces e implementaciones de experiencia de usuario destinadas a influenciar en el comportamiento y las decisiones de las personas en su interacción con webs, apps y redes sociales, de forma que tomen decisiones potencialmente perjudiciales para la protección de sus datos personales” (AEPD, 2022).

no neutral de opciones, otorgando mayor prominencia visual o auditiva a determinadas alternativas, la solicitud reiterada de que el usuario reconsidere una decisión ya adoptada, la imposición de mayores dificultades para cancelar un servicio que para contratarlo, y la configuración de ajustes predeterminados difíciles de modificar.

Desde la perspectiva del consentimiento, este artículo resulta relevante porque, a mi juicio, el criterio determinante de la prohibición no es el contenido de la decisión adoptada por el usuario, sino la afectación de su libertad de elección. Dicho de otro modo, el legislador europeo reconoce que el diseño de la interfaz puede condicionar la voluntad de la persona hasta el punto de que sus decisiones no sean verdaderamente libres. Ahora bien, el alcance de esta protección debe matizarse. El artículo 25.2 excluye de su ámbito las prácticas ya cubiertas por la Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales (en adelante, DPCD) o por el Reglamento General de Protección de Datos (en adelante, RGPD), lo que plantea interrogantes sobre qué instrumento normativo resulta aplicable en cada caso concreto y puede reducir considerablemente el espacio real de aplicación del DSA, dado el amplio ámbito de la DPCD.

b) Artículo 27: Transparencia del sistema de recomendación

Los sistemas de recomendación constituyen uno de los mecanismos principales mediante los cuales las plataformas personalizan la experiencia del usuario, seleccionando y priorizando el contenido que se le muestra. En la medida en que estos sistemas determinan qué información recibe la persona y en qué orden, inciden directamente en el contexto en el que esta forma sus decisiones.

El artículo 27 obliga a los prestadores de plataformas en línea que utilicen sistemas de recomendación a establecer en sus condiciones generales, de forma clara y comprensible, los parámetros principales empleados en dichos sistemas, así como las opciones disponibles para que los destinatarios del servicio puedan modificar o influir en tales parámetros (Reglamento (UE) 2022/2065, art. 27.1). Estos parámetros deberán explicar las razones por las que se sugiere determinada información al usuario. Asimismo, cuando existan varias opciones de configuración, la plataforma deberá ofrecer una funcionalidad que permita al destinatario seleccionar y modificar en

cualquier momento su opción preferida, de forma accesible y directa. (Reglamento (UE) 2022/2065, art. 27.3).

El enfoque adoptado por el artículo 27 es de transparencia ya que, no prohíbe los sistemas de recomendación ni su capacidad de personalización, sino que exige que el usuario conozca su funcionamiento y pueda intervenir sobre él. Esta aproximación parte de la premisa de que un usuario informado está en mejores condiciones de adoptar decisiones libres. El enfoque de transparencia del artículo 27 parte de la premisa de que una persona informada está en mejores condiciones de adoptar decisiones libres. Sin embargo, cabe preguntarse si la mera información sobre los parámetros algorítmicos es suficiente cuando el propio sistema está diseñado para maximizar la retención y el tiempo de uso, como advierte el Parlamento Europeo (2023) al señalar que muchos servicios en línea están diseñados para retener la atención de las personas usuarias y ser lo más adictivos posible (Parlamento Europeo, 2023).

d) Artículos 34 y 35: Evaluación y mitigación de riesgos

Los artículos 34 y 35 imponen obligaciones reforzadas a las plataformas en línea de muy gran tamaño y a los motores de búsqueda de muy gran tamaño⁴.

El artículo 34 obliga a estos prestadores a detectar, analizar y evaluar con diligencia cualquier riesgo sistémico en la UE que se derive del diseño o del funcionamiento de su servicio y los sistemas relacionados, incluidos los sistemas algorítmicos, o del uso que se haga de sus servicios (Reglamento (UE) 2022/2065, art. 34.1). La evaluación debe realizarse al menos una vez al año y, en todo caso, antes de desplegar nuevas funcionalidades con impacto potencial sobre los riesgos identificados. Entre los riesgos sistémicos que deben evaluarse, el artículo 34.1 incluye expresamente cualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDFUE), en particular los relativos a la dignidad humana (artículo 1 CDFUE), al respeto de la vida privada y familiar (artículo 7 CDFUE), a la protección de los datos de carácter personal (artículo 8 CDFUE), a la libertad de expresión e información (artículo 11 CDFUE), a la no discriminación (artículo 21 CDFUE), a los

⁴ Aquellos con un promedio mensual igual o superior a 45 millones de usuarios activos en la UE.

derechos del niño (artículo 24 CDFUE) y a un nivel elevado de protección de los consumidores (artículo 38 CDFUE). También deben evaluarse los riesgos sobre la protección de los menores, la seguridad y salud pública, así como las consecuencias negativas graves para el bienestar físico y mental de la persona. Además, al realizar la evaluación, los prestadores deben tener en cuenta el diseño de sus sistemas de recomendación y de cualquier otro sistema algorítmico pertinente.

Por su parte, el artículo 35 establece que estos prestadores deberán aplicar medidas de reducción de riesgos razonables, proporcionadas y efectivas, adaptadas a los riesgos sistémicos específicos detectados, teniendo especialmente en cuenta las consecuencias de dichas medidas sobre los derechos fundamentales (Reglamento (UE) 2022/2065, art. 35.1). Entre las medidas contempladas se incluyen la adaptación del diseño, las características o el funcionamiento de los servicios, y el refuerzo de los procesos internos de supervisión.

Desde la perspectiva del consentimiento, estos artículos son relevantes en la medida en que obligan a las grandes plataformas a identificar y mitigar activamente los riesgos que su diseño algorítmico puede generar sobre el bienestar de los usuarios. La inclusión expresa de los efectos negativos sobre el bienestar mental de la persona como riesgo sistémico evaluable permite encuadrar en esta categoría los efectos derivados del diseño adictivo. No obstante, se trata de obligaciones de diligencia y gestión de riesgos, no de prohibiciones directas: las plataformas deben evaluar y mitigar, pero el DSA no establece qué diseños concretos resultan incompatibles con la autonomía del usuario. Además, estas obligaciones reforzadas se aplican exclusivamente a las plataformas de muy gran tamaño, lo que deja fuera a servicios de menor dimensión que pueden emplear igualmente técnicas de diseño persuasivo.

3.2 Reglamento General de Protección de datos (RGPD 2016/679)

El 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, conocido como Reglamento General de Protección de Datos (en adelante, RGPD), constituye la norma de referencia en materia de protección de datos personales en la Unión Europea. Aunque no fue creado específicamente para regular el diseño de las plataformas digitales ni los patrones adictivos, sus disposiciones

resultan directamente aplicables a muchas de las prácticas que conforman el objeto de este trabajo, en la medida en que el funcionamiento de los algoritmos de diseño persuasivo se basa necesariamente en el tratamiento masivo de datos personales de las personas usuarias.

En efecto, los sistemas de recomendación, la personalización del contenido, la publicidad dirigida y los algoritmos solo son posibles mediante la recopilación, análisis y explotación de datos relativos al comportamiento, las preferencias y los hábitos de navegación de cada persona. Por ello, el RGPD ofrece un marco normativo relevante para evaluar la licitud de estas prácticas desde la perspectiva de la validez del consentimiento. A continuación, se analizan las disposiciones más pertinentes.

a) El consentimiento como base legitimadora del tratamiento (artículos 4.11, 6 y 7)

El RGPD sitúa el consentimiento del interesado como una de las bases de legitimación del tratamiento de datos personales (artículo 6.1.a). El artículo 4.11 lo define como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen” (Reglamento (UE) 2016/679, art. 4.11).

El artículo 7 desarrolla las condiciones para que dicho consentimiento sea válido. Establece que el responsable del tratamiento debe poder demostrar que el interesado consintió el tratamiento (apartado 1); que la solicitud de consentimiento debe presentarse de forma claramente distinguible, en un lenguaje claro y sencillo (apartado 2); y que el interesado tendrá derecho a retirar su consentimiento en cualquier momento, debiendo ser la retirada tan sencilla como la prestación del consentimiento (apartado 3).

Desde la perspectiva del objeto de este trabajo, los requisitos del consentimiento en el RGPD plantean una cuestión importante: si las plataformas que emplean técnicas de diseño persuasivo pueden sostener que el consentimiento obtenido de sus usuarios es verdaderamente libre e informado. Cabe plantear si la utilización de diseños que dificultan la opción de rechazo o que hacen la aceptación notablemente más fácil que la denegación puede comprometer el libre consentimiento. En este sentido, el Comité Europeo de Protección de Datos (en adelante, CEPD) ha identificado en sus Directrices

03/2022 sobre los patrones de diseño engañosos en las interfaces de las plataformas de redes sociales diversas categorías de patrones que pueden presentarse en el proceso de obtención del consentimiento en plataformas digitales, entre las que se incluyen la sobrecarga informativa, la ocultación de opciones relevantes, la obstaculización de las alternativas menos invasivas o la apelación a las emociones de la persona usuaria. (CEPD, 2023)

La conexión entre estos *dark patterns* y la validez del consentimiento es evidente ya que, el contexto en el que se solicita la aceptación de la persona está diseñado para orientar su decisión en una dirección predeterminada, por lo tanto, parece que la libertad del consentimiento queda comprometida. Aunque formalmente se cumplan las condiciones del artículo 7, el diseño persuasivo puede afectar la libertad real de la persona.

El CEPD (2023) ofrece un ejemplo ilustrativo de este tipo de prácticas en el contexto del registro en redes sociales:

Durante el proceso de registro, a los usuarios que hacen clic en los botones «omitir» para evitar introducir cierto tipo de datos se les muestra una ventana emergente que pregunta «¿Estás seguro?». Al cuestionar su decisión y, por tanto, hacerles dudar de ella, el proveedor de redes sociales incita a los usuarios a revisarla y a revelar este tipo de datos, como su sexo, su lista de contactos o su foto. En cambio, los usuarios que optan directamente por introducir los datos no ven ningún mensaje que les pida reconsiderar su elección. (p. 23)

b) Principios relativos al tratamiento de datos: licitud, lealtad y transparencia (artículo 5.1.a)

El artículo 5.1.a del RGPD establece que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado. El principio de lealtad tiene importancia para la problemática analizada en este trabajo. A diferencia de la transparencia, que se satisface proporcionando información, la lealtad implica una exigencia material sobre el modo en que se lleva a cabo el tratamiento. La AEPD precisa en su informe de 2024 sobre patrones adictivos que la lealtad “es un principio general que exige que los datos personales no se traten de forma perjudicial, discriminatoria, inesperada o engañosa para el interesado” (AEPD, 2024, p. 38), y concluye que todos los

patrones adictivos son incapaces de cumplir este principio, independientemente del cumplimiento de otros principios de protección de datos (AEPD, 2024).

En este sentido, parece que los algoritmos o patrones adictivos que explotan datos de la persona usuaria para prolongar su permanencia en la plataforma son incapaces de cumplir con el principio de lealtad, en la medida en que la persona puede desconocer la forma en que sus propios datos son utilizados para influir en su conducta. La AEPD señala que los proveedores suelen utilizar prácticas adictivas para tratar los datos de las personas usuarias de maneras que contradicen sus expectativas razonables y que pueden implicar usos inesperados o no deseados de sus datos personales. Además, los patrones adictivos podrían tener efectos perjudiciales y nocivos para los usuarios, en particular en lo que respecta al riesgo para el derecho fundamental a la integridad física y psíquica (AEPD, 2024).

c) Protección de datos desde el diseño y por defecto (artículo 25)

El artículo 25 del RGPD consagra el principio de protección de datos desde el diseño y por defecto (conocidos en inglés como *privacy by design* y *privacy by default*). Su apartado 1 establece que el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el del tratamiento mismo, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento. Su apartado 2 añade que el responsable garantizará que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada fin específico del tratamiento, obligación que se aplica a la cantidad de datos recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad (Reglamento (UE) 2016/679, art. 25).

Desde la perspectiva del consentimiento, este artículo es relevante porque establece una obligación que opera en sentido inverso al diseño persuasivo: mientras que los patrones adictivos tienden a configurar los ajustes predeterminados de forma que maximicen la recopilación de datos y la exposición de la persona usuaria, el artículo 25 del RGPD exige precisamente lo contrario. Si una plataforma configura por defecto la máxima personalización algorítmica o la máxima recopilación de datos de comportamiento cabe cuestionar si cumple con esta obligación. La AEPD concluye al

respecto que “la implementación de patrones engañosos y adictivos en un tratamiento de datos es una decisión de diseño contraria a la obligación de protección de datos desde el diseño y por defecto” (AEPD, 2024, p. 35).

d) Decisiones individuales automatizadas, incluida la elaboración de perfiles (artículo 22)

El artículo 22 del RGPD reconoce el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, cuando dicha decisión produzca efectos jurídicos o le afecte significativamente de modo similar (Reglamento (UE) 2016/679, art. 22.1). Este derecho implica que, como regla general, las personas no deben ser sometidas a decisiones adoptadas exclusivamente por medios automatizados si tales decisiones tienen un impacto relevante sobre ellas.

Cuando excepcionalmente se permita este tipo de tratamiento, por ser necesario para un contrato, estar autorizado por ley o basarse en el consentimiento explícito del interesado, el responsable del tratamiento deberá adoptar medidas adecuadas para salvaguardar los derechos del interesado, incluyendo como mínimo el derecho a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión. (Reglamento (UE) 2016/679, art. 22.3).

La aplicación de este precepto al ámbito de los algoritmos de diseño persuasivo no es directa, puesto que los sistemas de recomendación y personalización no adoptan una “decisión” sobre el usuario en el sentido clásico del artículo 22. Sin embargo, cabe preguntarse si la selección algorítmica continua del contenido que se muestra a cada usuario, basada en el perfilado de su comportamiento y diseñada para maximizar su permanencia en la plataforma, no constituye una forma de decisión automatizada que le “afecta significativamente de modo similar” a un efecto jurídico, en la medida en que condiciona su comportamiento, su tiempo y su autonomía.

3.3 Directiva 2005/29/CE sobre prácticas comerciales desleales

La Directiva 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior (DPCD) tiene por objeto contribuir al buen

funcionamiento del mercado interior y alcanzar un elevado nivel de protección de los consumidores mediante la aproximación de las legislaciones de los Estados miembros.

Aunque fue adoptada con anterioridad al auge de las grandes plataformas digitales, su contenido resulta plenamente aplicable al entorno en línea, dado que sus disposiciones son tecnológicamente neutras. La Guía sobre la interpretación de la DCPD a las prácticas basadas en datos y los patrones oscuros en el entorno digital (sección 4.2.7) (Comisión Europea, 2021), dedica un apartado específico en el que señala que la DPCD abarca las fases de publicidad, ventas y ejecución del contrato, incluido el consentimiento para el tratamiento de datos personales y el uso de datos personales para la entrega de contenidos personalizados, así como la rescisión de una relación contractual. Además, la DCPD tiene un amplio ámbito de aplicación: abarca todas las prácticas comerciales de las empresas en sus relaciones con los consumidores y no exige la existencia de una relación contractual o la compra de un producto. Por ejemplo, la DCPD también abarcaría prácticas comerciales tales como captar la atención del consumidor, lo que da lugar a decisiones sobre las transacciones, como seguir utilizando el servicio (por ejemplo, desplazarse por una noticia), ver el contenido publicitario o hacer clic en un enlace. Esta aclaración resulta especialmente relevante para el presente trabajo, ya que confirma que la decisión de la persona usuaria de continuar usando una plataforma digital puede considerarse una “decisión sobre una transacción” a efectos de la DCPD.

Para el objeto de este trabajo, la DCPD resulta relevante en la medida en que su sistema de prohibiciones se articula en torno a la protección de la libertad decisoria del consumidor. El artículo 5 establece la prohibición general de las prácticas comerciales desleales, que se concreta en dos grandes categorías: las prácticas engañosas (artículos 6 y 7), que incluyen tanto las acciones como las omisiones que inducen a error al consumidor, y las prácticas agresivas (artículos 8 y 9), que son aquellas que, mediante el acoso, la coacción o la influencia indebida, merman de forma significativa la libertad de elección del consumidor. La propia DPCD define la “influencia indebida” como “la utilización de una posición de poder en relación con el consumidor para ejercer presión, incluso sin usar fuerza física ni amenazar con su uso, de una forma que limite de manera significativa la capacidad del consumidor de tomar una decisión con el debido conocimiento de causa” (art. 2, letra j).

La categoría de prácticas agresivas reviste un interés particular para el presente análisis. La Comisión Europea (2021) señala expresamente, en la citada Guía, que el uso de información sobre las vulnerabilidades de consumidores específicos con fines comerciales podría constituir una forma de manipulación en la que el comerciante ejerce una “influencia indebida”, lo que daría lugar a una práctica comercial agresiva prohibida por los artículos 8 y 9 de la DCPD. La propia Guía pone el ejemplo de un comerciante que identifica que un adolescente se encuentra en un estado de ánimo vulnerable debido a acontecimientos de su vida personal y utiliza esa información para dirigirle anuncios basados en emociones en un momento concreto (Comisión Europea, 2021). Este tipo de supuestos evidencia cómo la explotación de datos personales para personalizar la experiencia digital puede traspasar el beneficio comercial y adentrarse en el terreno de la manipulación de la voluntad de la persona usuaria.

La misma Guía emplea el término “patrón oscuro” para referirse a un tipo de estímulo malintencionado, generalmente incorporado en las interfaces digitales, que puede basarse en datos y personalizarse, como ya se había detallado anteriormente. No obstante, la propia Comisión reconoce que el término no tiene una definición jurídica en la Directiva y que la calificación concreta de cada práctica exigiría un análisis caso por caso.

Si, por tanto, como se ha analizado, el propio Derecho del consumo ya identifica los patrones de diseño persuasivo como prácticas potencialmente manipuladoras que pueden comprometer la libertad de elección de la persona, al constituir posibles formas de “influencia indebida” a efectos de la DPCD (Comisión Europea, 2021, sección 4.2.7), con mayor razón cabe cuestionar la validez del consentimiento de la persona usuaria que permanece en una plataforma digital bajo la influencia continuada de esos mismos patrones.

4 MARCO JURÍDICO ESPAÑOL

El marco normativo europeo analizado en la sección anterior se complementa, en el ámbito interno, con disposiciones del ordenamiento jurídico español que resultan igualmente relevantes para la cuestión del consentimiento de la persona usuaria frente al diseño persuasivo de las plataformas digitales. En esta sección se analizan cuatro elementos: la Ley General para la Defensa de los Consumidores y Usuarios, el informe

de la Agencia Española de Protección de Datos sobre patrones adictivos, una resolución administrativa relevante en cuanto a patrones oscuros y, por último, los derechos y principios reconocidos en la Constitución Española que pueden verse afectados por estas prácticas. No se incluye un análisis específico de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, ya que los requisitos del consentimiento relevantes para este trabajo se encuentran directamente en el RGPD, de aplicación directa en todos los Estados miembros y ya analizada en la sección anterior.

4.1 Ley General para la Defensa de los Consumidores y Usuarios

El Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (en adelante, LGDCU), transpone, entre otras, la Directiva 2005/29/CE analizada en la sección anterior.

El artículo 8 reconoce como derechos básicos de las personas consumidoras la protección frente a las prácticas comerciales desleales y el derecho a la información correcta para facilitar la toma de decisiones óptimas para sus intereses (LGDCU, art. 8, letras b y d). Por su parte, el artículo 19.2 establece que las prácticas comerciales de los empresarios dirigidas a las personas consumidoras están sujetas a lo dispuesto en la propia LGDCU y en la Ley 3/1991, de 10 de enero, de Competencia Desleal (en adelante, Ley de Competencia Desleal). Esta remisión es relevante porque la Ley de Competencia Desleal prohíbe tanto las prácticas engañosas como las prácticas agresivas, incluyendo aquellas que utilizan la “influencia indebida” para mermar de forma significativa la libertad de elección de la persona consumidora (Ley 3/1991, arts. 5, 7 y 8). Dado que, como se ha analizado en la sección 3.3, la Comisión Europea (2021) ha señalado que el uso de datos sobre las vulnerabilidades de las personas consumidoras para influir en sus decisiones podría constituir una forma de influencia indebida a efectos de la DPCD, cabe preguntarse si los patrones adictivos empleados por las plataformas digitales podrían calificarse como prácticas comerciales agresivas también en el Derecho español, en la medida en que condicionan la voluntad de la persona usuaria a través del diseño del servicio.

No obstante, ni la LGDCU ni la Ley de Competencia Desleal contienen disposiciones específicas sobre el diseño adictivo de las plataformas digitales. La calificación de los

patrones adictivos como prácticas desleales requeriría un análisis caso por caso, y no existe hasta la fecha jurisprudencia española que haya abordado esta cuestión. La normativa de consumo ofrece, por tanto, un marco general que podría resultar aplicable, pero que no da una respuesta directa al problema que plantea este trabajo: que el consentimiento de la persona usuaria puede verse condicionado por el propio diseño del servicio al que ha consentido.

4.2 Agencia Española de Protección de Datos (AEPD)

4.2.1 *Guía sobre patrones adictivos y engañosos*

En julio de 2024, la AEPD publicó el informe *Patrones adictivos en el tratamiento de datos personales: implicaciones para la protección de datos* (AEPD, 2024). Aunque se trata de un documento de orientación sin carácter vinculante, resulta relevante para el presente trabajo porque es el primer documento de una autoridad de control española que analiza de forma específica cómo el diseño adictivo de las plataformas digitales afecta a la protección de datos y al consentimiento de las personas usuarias.

La AEPD define los patrones adictivos como características, atributos o prácticas de diseño que persiguen que las personas usuarias dediquen mucho más tiempo a utilizar las plataformas o lo hagan con un mayor grado de compromiso del esperado, conveniente o saludable para ellas (AEPD, 2024). El informe distingue estos patrones de los patrones engañosos, que son aquellos que llevan a las personas a tomar decisiones no intencionadas respecto al tratamiento de sus datos personales (AEPD, 2024), y concluye que todos los patrones adictivos pueden considerarse al mismo tiempo patrones engañosos, aunque no todos los patrones engañosos son adictivos (AEPD, 2024).

El informe clasifica los patrones adictivos en cuatro grandes categorías de alto nivel. La primera es la acción forzada, que consiste en ofrecer a las personas algo que desean exigiéndoles algo a cambio o engañándolas para que lo hagan de una manera que pueda causarles un perjuicio (AEPD, 2024). Dentro de esta categoría se incluyen varias técnicas, algunas de ellas son: el desplazamiento infinito por la pantalla (lo que en inglés se denomina *scroll* infinito), que permite a la persona desplazarse sin limitaciones por el contenido sin que este llegue a acabarse nunca; la reproducción automática, que inicia el siguiente vídeo o canción sin que la persona lo solicite; o la gamificación, que

incorpora mecánicas propias de los juegos, como puntos, recompensas o clasificaciones, para fomentar el uso continuado de la plataforma (AEPD, 2024).

La segunda categoría es la ingeniería social, que consiste en ofrecer a las personas algo basado en sus sesgos cognitivos o tendencias de comportamiento para manipularlas y llevarlas a tomar decisiones no intencionadas o potencialmente dañinas (AEPD, 2024). Estos solo son algunos ejemplos de ingeniería social, de todos los que podemos encontrar en la guía: la aprobación social, basada en estímulos como los botones de “me gusta” o el número de seguidores, que crean ilusiones de popularidad y llevan a la persona a permanecer conectada para obtener validación; la urgencia, que genera una falsa sensación de necesidad de actuar inmediatamente mediante alertas y notificaciones; el miedo a perderse algo (conocido en inglés como *FOMO: Fear Of Missing Out*), que explota la ansiedad de que otros estén experimentando algo interesante; y las recomendaciones algorítmicas, que personalizan el contenido mostrado a cada persona en función de su comportamiento previo para maximizar su tiempo de conexión. (AEPD, 2024). Este último patrón es, según la AEPD, el que hace un uso más intensivo de los datos personales, ya que cuanto más conozcan los proveedores sobre la persona, más adaptadas serán las recomendaciones y más efectivas para aumentar su tiempo de conexión (AEPD, 2024).

La tercera categoría es la interferencia en la interfaz, que consiste en manipular el diseño visual de la plataforma para promover unas acciones sobre otras o para dirigir la atención de la persona hacia contenidos específicos (AEPD, 2024). Esto incluye el uso de colores, fuentes o diseños que manipulan la atención de la persona, así como el uso de lenguaje persuasivo (ejemplo: un mensaje enviado de parte de la aplicación que dice “¡Conéctate ahora!”) o la sobrecarga de información para dificultar que la persona evalúe las consecuencias de sus decisiones.

La cuarta categoría es la persistencia, que explota el impulso humano innato de terminar las tareas que se han iniciado. Las plataformas utilizan este mecanismo mediante barras de progreso que indican cuánto falta para completar algo, o mediante previsualizaciones de contenido que generan en la persona la necesidad de seguir consumiéndolo. (AEPD, 2024).

Respecto al consentimiento, la AEPD señala que este no sería válido cuando la persona no está debidamente informada de los fines adictivos del tratamiento, cuando no se proporciona mediante un acto afirmativo claro, o cuando la prestación del servicio se supedita al consentimiento para operaciones de tratamiento que no son necesarias para su ejecución (AEPD, 2024). El informe es especialmente contundente en relación con el principio de lealtad del artículo 5.1.a) del RGPD, al afirmar que todos los patrones adictivos son incapaces de cumplir este principio, independientemente del cumplimiento de otros principios de protección de datos (AEPD, 2024).

Por último, dos conclusiones de la AEPD resultan especialmente relevantes para la tesis de este trabajo. En primer lugar, el informe señala que los patrones de diseño adictivos se han vuelto tan sofisticados que son capaces de encontrar y explotar las debilidades o vulnerabilidades de cualquier persona (AEPD, 2024), lo que significa que el problema del consentimiento afecta al conjunto de las personas usuarias y no solo a colectivos específicos. En segundo lugar, la AEPD advierte que en casi todos los escenarios las personas usuarias no pueden desactivar estas características, incluso cuando ellas mismas perciben su influencia o impactos negativos (AEPD, 2024), lo que refuerza la idea de que el consentimiento en este contexto no es verdaderamente libre.

4.2.2 Resolución relevante

En el ámbito español no existe todavía jurisprudencia de los tribunales sobre diseño adictivo de plataformas digitales y validez del consentimiento. No obstante, puede señalarse un precedente administrativo relevante.

La resolución de la AEPD en el procedimiento PS/00080/2023 (AEPD, 2023) constituye la primera sanción en España por el uso de patrones oscuros. La AEPD sancionó con un total de 12.000 euros a una empresa por tres infracciones distintas: 5.000 euros por infracción del artículo 5.1.a) del RGPD (principio de licitud, lealtad y transparencia), 2.000 euros por infracción del artículo 13 del RGPD (deber de información sobre obtención de datos personales) y 5.000 euros por infracción del artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (normativa sobre *cookies*).

La empresa sancionada empleaba en su página web dos tipos de patrones oscuros en el diseño de la interfaz de configuración de las opciones de privacidad. El primero era un patrón de sobrecarga (denominado en inglés *overloading*), que consiste en presentar a la persona un número excesivo de opciones para generarle fatiga y que acabe compartiendo más datos personales de los que desearía.

El segundo era un patrón de ocultación (denominado en inglés *skipping*), que consiste en diseñar la interfaz de modo que la persona no preste atención a aspectos relacionados con la protección de sus datos o los olvide. En concreto, al acceder al apartado de proveedores, la persona se encontraba con una lista de más de 300 empresas que tenían marcada por defecto la casilla de aceptar el tratamiento de datos por interés legítimo, sin que existiese la opción de rechazar todas de forma conjunta, lo que obligaba a desmarcarlas una a una.

Aunque esta resolución se refiere a patrones engañosos en el diseño de la gestión de cookies y no directamente al diseño adictivo de plataformas, establece un precedente significativo: confirma que la autoridad española de protección de datos puede sancionar prácticas de diseño de interfaces que condicionan las decisiones de la persona usuaria respecto a sus datos personales.

La ausencia de resoluciones o sentencias que aborden específicamente el diseño adictivo y su incidencia sobre el consentimiento confirma que se trata de una problemática que el ordenamiento español todavía no ha afrontado de forma directa.

4.3 Constitución Española

Varios derechos y principios reconocidos en la Constitución Española de 1978 resultan relevantes para la problemática analizada en este trabajo. El artículo 10.1 consagra la dignidad de la persona y el libre desarrollo de la personalidad como fundamento del orden político y de la paz social. El artículo 18 reconoce el derecho fundamental a la intimidad personal y familiar (apartado 1) y establece que la ley limitará el uso de la informática para garantizar la intimidad y el pleno ejercicio de los derechos de los ciudadanos (apartado 4), constituyendo el fundamento constitucional del derecho a la protección de datos personales en el ordenamiento español. El artículo 15 reconoce el derecho fundamental a la integridad física y moral. Por último, el artículo 51.1 establece que los poderes públicos garantizarán la defensa de los consumidores y

usuarios, protegiendo su seguridad, salud y legítimos intereses económicos, si bien se trata de un principio rector de la política social y económica y no de un derecho fundamental directamente invocable.

Estos preceptos resultan relevantes para el presente trabajo porque el diseño adictivo de las plataformas digitales incide en ámbitos protegidos por todos ellos: la libertad de decisión de la persona, la protección de sus datos personales, su bienestar y sus intereses como consumidora. La valoración de esta incidencia será objeto de análisis en la sección 5.

5 ANÁLISIS JURÍDICO Y CRÍTICO

5.1 El consentimiento en plataformas digitales

El consentimiento es el fundamento sobre el que se construye la relación entre las personas usuarias y las plataformas digitales. El Reglamento General de Protección de Datos define en su artículo 4.11 el consentimiento como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen” (Reglamento (UE) 2016/679, art. 4.11). Cuatro requisitos simples: libre, específico, informado e inequívoco.

Sin embargo, la realidad digital es más compleja. Cuando una persona abre una aplicación por primera vez y se encuentra con términos y condiciones de docenas de páginas, la mayoría da a “aceptar” sin leerlos. Formalmente se cumplen todos los requisitos del artículo 4.11, pero Mato Pacín (2024) plantea una pregunta incómoda: ¿si esa aceptación fue obtenida bajo la influencia de técnicas de diseño manipulativo, puede considerarse realmente válida?

Aunque formalmente se cumplan todos los requisitos de validez del consentimiento, el diseño persuasivo puede afectar la libertad real de la persona. Ponce Solé (2023) advierte que sin libertad de atención no hay libertad de pensamiento, y sin ausencia de manipulación no hay voluntad real. Si el entorno digital está diseñado para captar tu atención de formas que no controlas y para influir en tu comportamiento de maneras que no ves venir, entonces el consentimiento que prestas en ese entorno está siendo dado bajo presión, aunque esa presión sea invisible (Ponce Solé, 2023).

La AEPD (2024) es contundente: el consentimiento no sería válido si no está debidamente informado de los fines adictivos, si no se proporciona mediante un acto afirmativo claro, o si la prestación del servicio se supedita a consentimientos innecesarios. La AEPD concluye además que el principio de lealtad, exigido por el artículo 5.1.a del RGPD, tiene una función general y todos los patrones adictivos son incapaces de cumplirlo, independientemente de otro cumplimiento normativo (AEPD, 2024).

Mato Pacín (2024) añade que, en el ámbito digital, la vulnerabilidad es universal: no se trata de que algunos grupos sean más vulnerables, sino de que la personalización algorítmica de técnicas de manipulación intensifica la vulnerabilidad de todas las personas de maneras diferentes. El usuario medio es tan manipulable como cualquier otro cuando el diseño está optimizado para sus vulnerabilidades específicas. La pregunta entonces no es si la persona leyó los términos y condiciones. La pregunta es si la persona tenía realmente la capacidad de decidir libremente cuando toda la arquitectura del entorno digital estaba diseñada para influir en esa decisión.

5.2 Límites e insuficiencias de la regulación vigente

El Derecho europeo ha intentado responder a este problema. El artículo 25 del Reglamento de Servicios Digitales establece que

los prestadores de plataformas en línea no diseñarán, organizarán ni gestionarán sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio de manera que distorsione u obstaculice sustancialmente su capacidad de tomar decisiones libres e informadas (Reglamento (UE) 2022/2065, art. 25.1).

Parece claro: se prohíbe exactamente lo que se ha analizado.

Sin embargo, existen limitaciones significativas. El artículo 25.2 establece que “la prohibición del apartado 1 no se aplicará a las prácticas contempladas en la Directiva 2005/29/CE o en el Reglamento (UE) 2016/679” (Reglamento (UE) 2022/2065, art. 25.2). Esto crea un problema de solapamiento: si una práctica ya está cubierta por la Directiva sobre Prácticas Comerciales Desleales o por el RGPD, el DSA no entra. Esta multiplicidad de regulación puede generar lagunas si cada norma asume que las otras cubren el problema.

El artículo 27 del DSA requiere transparencia en sistemas de recomendación: las plataformas deben explicar cómo funcionan sus algoritmos y permitir intervención del

usuario (Reglamento (UE) 2022/2065, art. 27). Pero Llaneza (2019) señala un problema real: aunque formalmente una plataforma permita ver parámetros algorítmicos y modificarlos, la mayoría de las personas nunca irá a esos ajustes, y la plataforma lo sabe. La información está disponible pero no es accesible en términos reales. La mera información sobre parámetros algorítmicos puede no ser suficiente para garantizar libertad de consentimiento cuando el sistema está diseñado para maximizar retención y tiempo de uso.

El RGPD establece principios de protección que deberían funcionar. El artículo 5.1.a consagra lealtad en el tratamiento de datos personales (Reglamento (UE) 2016/679, art. 5.1.a). La AEPD concluye que todos los patrones adictivos incumplen este principio independientemente de cualquier otro cumplimiento normativo. (AEPD, 2024)

El artículo 25 del RGPD obliga a protección de datos desde el diseño y por defecto (Reglamento (UE) 2016/679, art. 25). Esto significa que los ajustes predeterminados deberían minimizar recopilación de datos, no maximizarla. Pero casi todas las plataformas configuran por defecto máxima personalización algorítmica y máxima recopilación de comportamiento. La AEPD observa que la implementación de patrones engañosos constituye decisión de diseño contraria a esta obligación. El problema reside en la ejecución: hay poco control sobre cumplimiento efectivo, y las plataformas tienen poco incentivo para cambiar algo que les funciona comercialmente.

El artículo 22 del RGPD reconoce el derecho a no ser objeto de decisiones basadas únicamente en tratamiento automatizado (Reglamento (UE) 2016/679, art. 22). Pero cabe preguntarse si la selección algorítmica continua de contenido, basada en perfilado de comportamiento y diseñada para maximizar permanencia en plataforma, no constituye una forma de decisión automatizada que afecta significativamente la autonomía de la persona.

En el nivel nacional, la Ley General para la Defensa de los Consumidores y Usuarios ofrece protecciones contra prácticas desleales incluyendo manipulación, pero no contiene disposiciones específicas sobre diseño adictivo de plataformas digitales. No existe jurisprudencia española que haya abordado esta cuestión específicamente. La Directiva sobre Prácticas Comerciales Desleales identifica como prohibidas aquellas que explotan vulnerabilidades para manipular (Directiva 2005/29/CE), y como se ha analizado en la sección 3.3, ya identifica patrones de diseño persuasivo como prácticas

potencialmente manipuladoras que pueden comprometer libertad de elección. Con mayor razón cabe cuestionar validez del consentimiento cuando la persona permanece en plataforma bajo influencia continuada de esos patrones.

En el plano constitucional, la Constitución Española reconoce derechos directamente relacionados: el artículo 10.1 protege dignidad y libre desarrollo de la personalidad; el artículo 18 reconoce derecho a intimidad y establece que la ley limitará uso de informática para garantizarla; el artículo 15 protege integridad física y moral; el artículo 51.1 impone mandato de protección de consumidores. Pero estos derechos están reconocidos sin herramientas específicas para protegerlos frente a diseño adictivo. Barrio Andrés (2025) advierte que, aunque se reconoce desde diversos foros urgencia de definir marco jurídico que garantice derechos digitales, cuando examinamos la Constitución, estas protecciones no aparecen de forma clara. Algunos sugieren que la Constitución misma necesitaría reforma expresa para responder adecuadamente a estos retos (Barrio Andrés, 2025).

6 CONCLUSIONES

Para finalizar el trabajo, se da resolución a las cuestiones planteadas al principio:

¿Son jurídicamente lícitas las técnicas de diseño persuasivo utilizadas por las plataformas digitales a la luz del Derecho vigente?

Formalmente, no. El Derecho vigente las prohíbe. El artículo 25.1 del DSA establece explícitamente que los prestadores no pueden diseñar interfaces que "engañen o manipulen" de forma que "distorsione u obstaculice sustancialmente" la capacidad de decidir libremente (Reglamento (UE) 2022/2065, art. 25.1). El Reglamento General de Protección de Datos exige en su artículo 5.1.a que los datos se traten en base al principio de lealtad (Reglamento (UE) 2016/679, art. 5.1.a), y la Agencia Española de Protección de Datos ha concluido que todos los patrones adictivos son incapaces de cumplir este principio, independientemente de cualquier otro cumplimiento normativo (AEPD, 2024). La Directiva sobre Prácticas Comerciales Desleales, a su vez, prohíbe expresamente la "influencia indebida" (Directiva 2005/29/CE, 2005, art. 5) y la Comisión Europea ha identificado los patrones de diseño persuasivo como una forma de manipulación que constituye práctica comercial agresiva (Comisión Europea, 2021).

Existe, por tanto, una prohibición expresa en múltiples niveles del ordenamiento jurídico.

Sin embargo, existe una distancia significativa entre la prohibición formal y la aplicación práctica. En primer lugar, no hay jurisprudencia que haya condenado específicamente prácticas de diseño adictivo, lo que deja un vacío de precedente a la interpretación de estas normas. En segundo lugar, el artículo 25.2 del DSA establece que esta prohibición no se aplicará a prácticas ya cubiertas por el RGPD o la Directiva sobre Prácticas Comerciales Desleales (Reglamento (UE) 2022/2065, art. 25.2), lo que genera incertidumbre sobre cuál es la regulación aplicable en cada caso. En tercer lugar, debido a esta insuficiencia, las plataformas pueden alegar un cumplimiento meramente formal. Sin embargo, a la luz de todo lo expuesto en este trabajo, no debería considerarse así, ya que, aunque “informen”, soliciten el “consentimiento” o desarrollen algoritmos “transparentes”, continúan utilizando técnicas de manipulación diseñadas por expertos y optimizadas mediante inteligencia artificial. Por tanto, en la práctica puede parecer que cumplen con las exigencias legales, pero en realidad no es así. La falta de un control efectivo y de sanciones proporcionadas frente a estas situaciones provoca que el riesgo jurídico derivado del uso de estas técnicas siga siendo bajo para las plataformas.

¿Es válido el consentimiento de la persona usuaria cuando las plataformas digitales utilizan diseños persuasivos para influir en su comportamiento?

No. Para que el consentimiento sea válido según el RGPD debe ser libre, específico, informado e inequívoco (Reglamento (UE) 2016/679, art. 4.11). Este trabajo ha demostrado que ninguno de estos requisitos se cumple realmente cuando el entorno digital está diseñado para manipular.

No es libre porque la arquitectura de la interfaz ejerce influencia indebida sobre la decisión. No es específico porque las solicitudes de consentimiento son generales y no especifican los fines adictivos que persiguen los patrones de diseño (Mato Pacín, 2024). La AEPD (2024) señala que el consentimiento no sería válido cuando “no está debidamente informado de los fines adictivos del tratamiento”. No es informado porque la persona no entiende realmente cómo funcionan los algoritmos que manipulan su comportamiento, ni qué datos sobre ella están siendo utilizados para optimizar esa manipulación. El propio trabajo demuestra en la sección sobre “privacy fatigue” que la

sobrecarga informativa genera lo opuesto a información efectiva: agotamiento que lleva a aceptar sin reflexionar. No es inequívoco porque los patrones oscuros que el trabajo analiza obligan a la persona a realizar acciones que no desearía hacer si el entorno fuera neutral. La acción de “aceptar” no expresa verdaderamente la voluntad de la persona, sino la presión del entorno diseñado. (Mato Pacín, 2024).

¿En qué medida el marco normativo actual permite abordar los efectos derivados del diseño algorítmico persuasivo?

La respuesta es de forma insuficiente. El marco normativo reconoce el problema de varias maneras: el DSA lo prohíbe, el RGPD requiere lealtad, la DPCD identifica manipulación, la Constitución protege derechos relacionados, entre otras. Sin embargo, este reconocimiento múltiple no resulta en una protección efectiva.

El análisis identifica varias deficiencias. Primero, los solapamientos regulatorios que crean vacíos: el artículo 25.2 del DSA excluye prácticas ya cubiertas por el RGPD o la DPCD, lo que genera un efecto paradójico donde cada norma asume que otras están cubriendo el tema, resultando en que ninguna lo haga completamente.

Segundo, conceptos indeterminados que requieren análisis caso por caso sin criterios claros. El DSA prohíbe diseño que "distorsione sustancialmente" la capacidad de decidir, pero no define operativamente qué significa "sustancial". De igual forma, la DPCD habla de "influencia indebida" sin especificar cómo identificarla en el contexto del diseño algorítmico personalizado.

Tercero, la ausencia de jurisprudencia que interprete estas normas y condene específicamente el diseño adictivo y persuasivo. Esto deja un vacío de precedentes que guíe la aplicación normativa.

Cuarto, la falta de reconocimiento explícito de derechos digitales en la Constitución Española. Aunque la Constitución protege la libertad de pensamiento, la integridad moral y el libre desarrollo de la personalidad, no menciona explícitamente "derechos digitales".

Como resultado, el trabajo demuestra que, aunque existe un marco normativo a nivel europeo y español, su aplicación es insuficiente para proteger efectivamente a la persona usuaria. Para que el marco normativo sea efectivo, sería necesario: garantizar su aplicación rigurosa, llenar las lagunas conceptuales identificadas, crear jurisprudencia

y posiblemente actualizar el marco constitucional para reconocer expresamente los derechos digitales. Además, también sería interesante establecer mecanismos de control más allá de esto, como por ejemplo: la obligación de cambios en el diseño, el derecho de los usuarios a conocer realmente cómo están siendo manipulados por algoritmos y cómo se están utilizando sus datos, entre otros.

Investigar este tema me ha resultado muy interesante porque estamos ante problemas jurídicos completamente nuevos que el Derecho aún está aprendiendo a abordar. A pesar de las limitaciones encontradas, el análisis revela que existen un montón de preguntas jurídicas que requieren atención: cómo garantizar realmente la libertad del consentimiento, cómo hacer efectivas las prohibiciones existentes, cómo actualizar conceptos jurídicos para la era digital.

Queda mucho trabajo por hacer en este ámbito. Las cuestiones planteadas en este trabajo demuestran que el Derecho tiene aún que desarrollar respuestas adecuadas a un fenómeno que solo acaba de empezar. Pero este análisis ha intentado contribuir a visibilizar un problema que es urgente y que requiere ser abordado de forma seria por la comunidad jurídica.

7 REFERENCIAS

- Agencia Española de Protección de Datos. (2022, 19 de mayo). *Dark patterns: Manipulación en los servicios de Internet*. <https://www.aepd.es/prensa-y-comunicacion/blog/dark-patterns-manipulacion-en-los-servicios-de-internet>
- Agencia Española de Protección de Datos. (2023). *Resolución del procedimiento sancionador PS/00080/2023*. https://www.aepd.es/informes-y-resoluciones/resoluciones?search_api_fulltext=PS%2F00080%2F2023+&sort_bef_combine=fecha_firma_DESC
- Agencia Española de Protección de Datos. (2024). *Patrones adictivos en el tratamiento de datos personales: implicaciones para la protección de datos*. <https://www.aepd.es/guias/patrones-adictivos-en-tratamiento-de-datos-personales.pdf>
- Agencia Española de Protección de Datos. (2025). *Bienvenida a la Agencia*. <https://www.aepd.es/la-agencia/bienvenida-la-agencia>
- Barrio Andrés, Moisés. (2025). *Manual de derecho digital* (4ª edición). Tirant lo Blanch.
- Comisión Europea. (2021). *Comunicación de la Comisión — Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior* (2021/C 526/01). Diario Oficial de la Unión Europea, C 526, 1-129. [https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021XC1229\(05\)](https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021XC1229(05))
- Comité Europeo de Protección de Datos. (2023). *Directrices 03/2022 sobre los patrones de diseño engañosos en las interfaces de las plataformas de redes sociales: cómo reconocerlos y evitarlos* (Versión 2.0). 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

- Lee, Kah-Wee. (2014). [Reseña del libro *Addiction by Design: Machine Gambling in Las Vegas*, de N. D. Schüll]. *Technology and Culture*, 55(1), 278-280.
<https://doi.org/10.1353/tech.2014.0015>
- Llaneza, Paloma. (2019). *Datanomics: todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos* (1.ª ed.). Planeta - Deusto.
- Mato Pacín, Maria Natalia. (2024). *Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros*. Agencia Estatal Boletín Oficial del Estado. https://www.boe.es/biblioteca_juridica/publicacion.php?id=PUB-PR-2024-330
- Mill, John Stuart. (1859). *On liberty*. John W. Parker and Son.
- Parlamento Europeo. (2023). *Resolución de 12 de diciembre de 2023 sobre el diseño adictivo de los servicios en línea y la protección de los consumidores en el mercado único de la UE* (2023/2043(INI)).
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_ES.html
- Ponce Solé, Juli. (2023). Derecho, *nudging* digital y manipulación: patrones oscuros, inteligencia artificial y derecho a una buena administración (Alejandra Boto Álvarez, Traducción). *Anuario de la Red Eurolatinoamericana de Buen Gobierno y Buena Administración*, (3).
<https://dialnet.unirioja.es/servlet/articulo?codigo=8890050>
- Schüll, Natasha Dow. (2012). *Addiction by design: Machine gambling in Las Vegas*. Princeton University Press.

Normativa

- Constitución Española. 27 de diciembre de 1978 (España).
[https://www.boe.es/eli/es/c/1978/12/27/\(1\)/con](https://www.boe.es/eli/es/c/1978/12/27/(1)/con)
- Directiva 2005/29/CE del Parlamento Europeo y del Consejo. Relativa a las prácticas comerciales desleales. 11 de mayo de 2005 (Unión Europea).
<http://data.europa.eu/eli/dir/2005/29/oj>

Ley 3/1991, de 10 de enero, de Competencia Desleal (España).
<https://www.boe.es/eli/es/l/1991/01/10/3/con>

Real Decreto Legislativo 1/2007. Por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios. 16 de noviembre de 2007 (España). <https://www.boe.es/eli/es/rdlg/2007/11/16/1/con>

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Relativo a la protección de datos personales. 27 de abril de 2016 (Unión Europea).
<http://data.europa.eu/eli/reg/2016/679/oj>

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo. Relativo a un mercado único de servicios digitales. 19 de octubre de 2022 (Unión Europea).
<http://data.europa.eu/eli/reg/2022/2065/oj>