# Online choice architecture: impacto del diseño digital en la autonomía contractual del usuario. Inteligencia artificial y vulnerabilidad del usuario digital*

*M.ª Natalia Mato Pacín, Universidad Carlos III de Madrid*

*Resumen:* El trabajo aborda el fenómeno del diseño y de los patrones oscuros en las interfaces en línea desde el punto de vista del Derecho de la Unión Europea y español. Estas prácticas, con un gran impacto en la economía digital debido a la IA y el *big data*, se encuentran en el punto de mira del legislador europeo, con presencia en todas las normas relevantes del sector aprobadas en los últimos años. Tras un breve recorrido por las disposiciones que pueden suponer un límite legal a los patrones oscuros, el núcleo del trabajo se centra en examinar la transformación del concepto de usuario/consumidor en el entorno digital impulsada por la inteligencia artificial y las técnicas de personalización. Se argumenta que el enfoque normativo tradicional en torno al usuario medio podría resultar insuficiente ante la capacidad de la inteligencia artificial para explotar vulnerabilidades y adaptar hasta el extremo la experiencia individual.

*Palabras clave: Legal design*, patrones oscuros, interfaces digitales, protección de datos, prácticas comerciales desleales, servicios digitales, inteligencia artificial, usuario digital vulnerable.

*Zusammenfassung:* Der Beitrag befasst sich mit dem Phänomen der "*dark patterns*" aus der Sicht Rechts der Europäischen Union und des spanischen Rechts. Diese manipulative Gestaltung von Online-Schnittstellen, die dank künstlicher Intelligenz und *big data* große Auswirkungen auf die digitale Wirtschaft hat, steht im Visier des europäischen Gesetzgebers und ist Gegenstand aller einschlägigen sektoralen Verordnungen der letzten Jah-

* Profesora del Departamento de Derecho privado de la Universidad Carlos III de Madrid. Este trabajo se enmarca en el Proyecto de investigación nacional financiado por la Fundación Ramón Areces (XX Concurso Nacional para la Adjudicación de Ayudas a la Investigación en Ciencias Sociales) y titulado "Optimización de la transparencia en los contratos *online* para una innovación económica en la industria minorista: Investigación interdisciplinar a través del análisis jurídico y experimentos empíricos sobre el comportamiento del consumidor", del que la autora es Investigadora Principal.

re. Nach einem kurzen Überblick über die Bestimmungen, die den *dark patterns* rechtliche Grenzen setzen können, wird dem Wandel nachgegangen, den der Begriff des Nutzers/Verbrauchers im digitalen Umfeld – forciert durch künstliche Intelligenz und Personalisierungstechniken – derzeit durchlaufen hat. Es wird dargelegt, dass sich der traditionelle normative Fokus auf den Durchschnittsnutzer als unzureichend erweisen könnte angesichts der Fähigkeit der künstlichen Intelligenz zur Ausnutzung von Schwachstellen und zur genauen Anpassung an die individuellen Erfahrungen der Nutzer.

*Schlüsselwörter: Legal design*, *dark patterns*, Online-Schnittstellen, Datenschutz, unlautere Geschäftspraktiken, digitale Dienstleistungen, künstliche Intelligenz, im digitalen Umfeld verletzlicher Nutzer.

## *A. Introducción:* legal design *y contratación digital*

El punto de partida de este trabajo se ubica en el hecho de que, en el entorno digital, el contacto entre el usuario y el empresario se produce a través de la interfaz del dispositivo que se maneje (*v. gr.* un ordenador, un teléfono móvil, una *Tablet*, un dispositivo conectado). Esta circunstancia convierte a la interfaz en un elemento clave para la comunicación entre ambos y, por lo tanto, también para la comunicación con relevancia legal, especialmente porque en el entorno digital es la única fuente de información.[1]

Así las cosas, en los últimos tiempos está cobrando mucha importancia el diseño de las páginas web y aplicaciones informáticas en lo que se refiere a cómo configurar el proceso de contratación, cómo se integran los -crecientes- requisitos legales de información, cómo se pide el consentimiento, cómo se accede a las condiciones generales o al tratamiento de datos personales, que tienen mucha relevancia en el entorno digital. Hay que tener en cuenta que, desde el punto de vista del comportamiento del usuario, se ha demostrado que el éxito de la comunicación a través de la interfaz no solo depende del contenido de la información -esto es, sobre qué se informa-

1 *J. Luzak*, Tailor-made consumer protection: personalisation's impact on the granularity of consumer information, en: M. Corrales et al. (eds.), Legal design – Integrating business, design and legal thinking with technology, Cheltenham; Northampton: Edward Elgar, 2021, p. 107.

sino también del modo en el que se proporciona dicha información -cómo y cuándo se informa-.[2]

Esta idea de que el diseño es importante también desde el punto de vista jurídico se inscribe en lo que se denomina de manera genérica como *legal design*, un concepto o una disciplina relativamente reciente y de total actualidad que plantea diseñar los procesos con implicaciones jurídicas de una forma más intuitiva, inclusiva y eficiente para todas las partes implicadas.[3] Descendiendo a una definición más concreta del concepto de *legal design,* se podría decir que es la aplicación del diseño al mundo del Derecho, para hacer los sistemas y los servicios jurídicos más centrados en el ser humano y más satisfactorios y fáciles de usar.[4]

Efectivamente, se ha acusado tradicionalmente a los contratos o a la información legal de ser escritos "por abogados para abogados".[5] En este sentido, la idea que subyace detrás del *legal design* residiría en que estos contratos se redactaran o confeccionaran también pensando en los usuarios o destinatarios, esto es, en encontrar un equilibrio entre la necesidad de precisión -que es consustancial al Derecho- y, por otro lado, la facilidad de uso.[6]

Las experiencias en las que se ha aplicado el *legal design* a los contratos son variadas y en diferentes contextos. Es el caso, por ejemplo, de líneas

2 *A.Rossi/R. Ducato/H. Haapio/S. Passera*, When design met law: design patterns for information transparency, Droit de la Consommation, no. 122-123, 2019, pp. 79 y ss.; *O. Seizov/A. J. Wulf/J. Luzak,* The transparent trap: a multidisciplinary perspective on the design of transparent online disclosures in the EU, Journal of Consumer Policy, n. 42, 2019, p. 19.

3 *M. Doherty/M. Corrales/H. Haapio/M. Hagan*, A new attitude to law's empire: the potentialities of legal design", en: M. Corrales et al. (eds.), Legal design. Integrating business, design and legal thinking with technology, Cheltenham; Northampton: Edward Elgar, 2021, pp. 2-3; *M. Hagan*, Law by design, 2016. Disponible en: https://lawbydesign.co/; *E. Vicente Domingo*, Legal design en la redacción e interpretación de los contratos, en: APDC, Derecho de contratos, responsabilidad extracontractual e inteligencia artificial, Madrid: Aranzadi, 2024, pp. 187 y ss.

4 *Hagan,* Design (n. 3).

5 *K. Huovinen*, Better commercial contracts with the application of functional contracting and legal design, en: M. Corrales *et al.* (eds.), Legal design. Integrating business, design and legal thinking with technology, Cheltenham; Northampton: Edward Elgar, 2021, p. 180.

6 *H. Haapio/T. D. Barton/M. Corrales*, Legal design for the common good: proactive legal care by design, en: M. Corrales et al. (eds.), Legal design. Integrating business, design and legal thinking with technology, Cheltenham; Northampton: Edward Elgar, 2021, p. 69.

de tiempo explicando gráficamente un proceso de suscripción, apoyadas en resúmenes destacados y con un lenguaje directo y sencillo;[7] de páginas interactivas para comunicar información sobre protección de datos;[8] o de la representación de cláusulas de un contrato laboral recurriendo a viñetas de cómic, para superar las barreras del idioma de trabajadores de una empresa agrícola en Sudáfrica.[9]

Son diversos los beneficios que la doctrina ha asociado a esta disciplina que conjuga el Derecho y el diseño en el ámbito de la contratación. Teniendo en cuenta que el *legal design* adopta un enfoque de Derecho preventivo o proactivo -centrándose en evitar que surjan problemas innecesarios, más que limitándose a resolver los conflictos jurídicos que ya han surgido-, se ha demostrado que aumenta el entendimiento y el cumplimiento de los contratos, reduce posibles malentendidos y reclamaciones, mejora la experiencia del usuario y aumenta su compromiso y confianza con la marca.[10]

A la vista de todo lo anterior, no es de extrañar que desde todos los sectores empresariales se invierta de manera creciente en el diseño de páginas web, aplicaciones o *software* de tal modo que puedan ofrecer a sus usuarios y clientes una experiencia más sencilla y satisfactoria. Para ello se utilizan patrones de diseño[11] que, mediante el análisis de los sesgos cognitivos y afectivos de los sujetos, anticipan su comportamiento y permiten lograr una configuración de la interfaz (una "arquitectura de elección" u *Online Choice Architecture*, en terminología inglesa)[12] adecuada a los objetivos. El problema reside en que estas técnicas de presentar las distintas opciones en una interfaz pueden no ser neutrales sino estar encaminadas a influir, más o menos sutilmente, en el comportamiento del usuario de tal manera que sus decisiones no sean racionales o coherentes con sus preferencias. No

7 En https://buzzsumo.com/wp-content/themes/brandwatch/src/site--buzzsumo.com/assets/Buzzsumo-Terms-2019-09.pdf.

8 En https://www.visualcontracts.eu/legal/privacy-statement/.

9 En https://creative-contracts.com/clemengold/.

10 *S. Passera/E. Allbon/H. Haapio,* Contract transformation: merging drafting and design to meet the needs of human readers, en: M. Corrales et al. (eds.) Research handbook on contract design, Cheltenham; Northampton: Edward Elgar, 2022, p. 98.

11 *WorldDCC Foundation/S. Passera/H. Haapio*, Contract Design Pattern Library; *T. D. Barton/H. Haapio/S. Passera/J. Hazard*, Reframing contract design: integrating businesss, legal, design and technology perspectives, en: M. Corrales et al. (eds.) Research handbook on contract design, Cheltenham; Northampton: Edward Elgar, 2022, pp. 40 y 41.

12 *Competition & Markets Authority*, Online Choice Arquitecture. How digital design can harm competition and consumers, Discussion Paper, abril 2022.

hay que olvidar que es en internet donde más expuesto está el usuario y, de hecho, se habla de un nuevo tipo de asimetría de la información, pues a la tradicional situación en la que el empresario tiene más conocimientos que el usuario sobre el producto o servicio comercializado, se añade que el empresario sabe también más sobre el usuario que el propio usuario, como consecuencia de toda la información que genera su actividad en línea.[13] Surgen, así, los conocidos como patrones oscuros o engañosos o *dark patterns o deceptive patterns*, técnicas mediante las que los diseñadores utilizan su conocimiento sobre el comportamiento humano para implementar características o pasos engañosos que no se alinean con lo que es mejor para el usuario.[14]

### *B. Prácticas engañosas o coercitivas que afectan al comportamiento del usuario digital*

No hay una única definición aceptada de patrones oscuros, pues se trata de un concepto amplio que engloba una gran diversidad de prácticas y respecto del que se han intentado diferentes aproximaciones teóricas. Recurriendo a la definición legal que de estas prácticas dispone el Reglamento de Servicios Digitales (RSD, en adelante), se trataría de técnicas que "engañen o manipulen a los destinatarios del servicio o [...] distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas" (art. 25.1).

Del mismo modo, tampoco hay una clasificación oficial o unánime, sino múltiples que ha ido creando la doctrina partiendo de distintos criterios.[15] Sin ánimo de ser exhaustivos, pero sí para ilustrar mínimamente el fenómeno de los patrones engañosos a través de ejemplos prácticos, enumeraremos algunos supuestos de las prácticas más prevalentes en la Unión Europea

13 *E. Mik*, The erosion of autonomy in online consumer transactions, Law, Innovation and Technology, n. 8 (1), 2016, p. 13.

14 Definición tomada de la web de Harry Brignull (https://www.deceptive.design/), quien introdujo el concepto de patrones oscuros en 2010 (aunque en la actualidad se refiere a este fenómeno como "*deceptive designs*").

15 Para más detalle acerca de la definición, tipología y ejemplos con ilustraciones, remitiéndonos a la bibliografía allí citada, veáse *M.N. Mato Pacín*, Aspectos jurídicos del diseño de las interfaces digitales. En especial, los patrones oscuros, Madrid: Boletín Oficial del Estado, 2024, pp. 52, 53 (delimitación); 54-60 (clasificaciones y ejemplos).

según una investigación llevada a cabo en el marco del Programa de Consumidores de la Comisión Europea en 2022:[16]

a) Información escondida o falsa jerarquía: patrón que toma información importante en el proceso y que la esconde visualmente o la ordena de una manera (usando tamaño, color, ubicación, etc.) para promover una opción específica, la preferida por el empresario;
b) Preselección o selección por defecto (*bad default*): práctica que marca por defecto las opciones preferidas por el empresario;
c) Persistencia o *nagging:* el empresario insiste en ciertas acciones -que el usuario no puede definitivamente rechazar- con la intención de que el usuario al final acepte la acción, simplemente para evitar la molestia de las interrupciones;
d) Cancelación difícil o *roach motel*: patrón que se basa en una asimetría entre el momento de contratar y el de dar por terminado un contrato, pues si bien la contratación fue muy sencilla, la cancelación se dificulta sobremanera por la gran cantidad de barreras que existen.

Otros ejemplos de técnicas también usadas en la práctica serían las conocidas como *sneak into the basket* (se añaden a la cesta productos no solicitados y que pueden pasar desapercibidos), *confirmshaming* (técnicas que buscan hacer sentir al usuario culpable o tonto por rechazar una opción), de escasez o urgencia (uso de mensajes alertando de existencias muy limitadas de stock, de que hay muchos usuarios mirando un producto o contadores avisando de que el tiempo que queda para una compra es breve); uso de la influencia social (mensajes informando sobre el comportamiento -compras, visitas- de otros usuarios o sobre afirmaciones realizadas por otros sujetos sobre un producto o servicio, que pueden ser confusas o falsas); *forced actions* (prácticas que obligan al usuario a aceptar ciertas acciones no queridas realmente por él, como, por ejemplo, obligar al usuario a registrarse proporcionando datos como su correo electrónico, fecha de nacimiento o dirección para poder acceder a alguna funcionalidad para la

16 *F. Lupiáñez-Villanueva/A. Boluda/G. L. Bogliacino/L. Lechardoy/T. Rodríguez de las Heras*, Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalisation – Final report, Publications Office of the European Union, 2022.

que realmente no sería técnicamente necesario ese registro, siendo la única finalidad la de proporcionar datos personales).[17]

Algunas de estas maniobras, consistentes en persuadir a los usuarios para que contraten, para que se relacionen con el entorno del empresario en condiciones más beneficiosas para él o para que inviertan allí más tiempo, en mayor o menor medida, siempre han existido, incluso en el entorno físico u *offline*. Pero, en la actualidad, gracias al *big data* y la inteligencia artificial, como se señalará en epígrafes posteriores, el problema se agrava por la cantidad de datos y la personalización tan detallada que pueden llegar a alcanzar intentando explotar cualquier vulnerabilidad del usuario y por la posibilidad de predeterminar con bastante exactitud la reacción de cada usuario a las distintas técnicas de persuasión o engaño y, por tanto, de saber cuáles tienen un mejor funcionamiento para los intereses del empresario.[18] De hecho, son prácticas totalmente extendidas en el ámbito digital y en todos los sectores,[19] que pueden llegar a generar daños tanto individuales (pérdidas económicas y de privacidad o daños psicológicos) como colectivos (fallos de mercado, afectación a la confianza de los usuarios y a la libre competencia).[20]

### *C. Panorámica de los principales límites jurídicos a los patrones oscuros*

A la vista de que estas prácticas tienen potenciales efectos perjudiciales y están presentes en el día a día del entorno digital, cabe plantearse cuál sería el marco normativo para abordar jurídicamente los patrones oscuros en la

17 Sin perjuicio de remitirnos a la bibliografía recogida en la obra citada en la nota pie número 16, donde tratamos más extensamente el fenómeno, de la gran mayoría de las técnicas aquí señaladas se puede encontrar un análisis en *C. Gray/Y. Kou/B. Battles/J. Hoggatt/A.J. Toombs,* The dark (patterns) side of UX design, CHI Conference on Human Factors in Computing Systems, 2018; *J. Luguri/L. J. Strahilevitz*, Shining a light on dark patterns, Journal of Legal Analysis, vol. 13, Working Paper n. 719, 2021; *A. Mathur/J. Mayer/M. Kshirsagar*, What makes a dark pattern…dark?, CHI Conference on Human Factors in Computing Systems, 2021.

18 *Luguri/Strahilevitz*, Shining (n. 17), pp. 49-50.

19 *Lupiáñez-Villanueva* et al., Behavioural (n. 16), pp. 6 y 120.

20 Sobre el impacto individual y colectivo de los patrones oscuros, ver *Mato*, Interfaces (n. 15), pp. 62 y ss.

Unión Europea. Veamos una breve panorámica de las normas que podrían suponer un límite desde el punto de vista del Derecho para estas prácticas.[21]

En primer lugar, si el patrón oscuro afecta a *datos personales*, el Reglamento General de Protección de Datos (Reglamento (EU) 2016/679, en adelante, RGPD), será un claro límite en la medida en que varios de sus principios se verían afectados. Así, algunos patrones oscuros no serían compatibles con los principios de lealtad y transparencia del art. 12 RGPD -que obligan a dar información sobre la recogida y el tratamiento de una manera accesible y clara de entender-, con la obligación de solicitar el consentimiento de forma libre, específica, informada e inequívoca (arts. 4.11 y 7 RGPD) o con el principio de protección de datos desde el diseño y por defecto (art. 25 RGPD). De hecho, tal es la incidencia de estas técnicas en el ámbito de los datos personales que el Comité Europeo de Protección de Datos publicó en 2022 unas Directrices sobre patrones oscuros en las redes sociales (Directrices 03/2022). Por otro lado, los órganos nacionales competentes en materia de protección de datos recurren en ocasiones ya al concepto "patrón oscuro" en los expedientes sancionadores.[22]

No nos movemos exclusivamente en el campo del Derecho de consumo, pero si el usuario es, además, consumidor, lógicamente las *normas de protección al consumidor* pueden dar respuesta a algunas de las técnicas engañosas. Sería el caso, por un lado, de la Directiva 2011/83/EU, sobre derechos de los consumidores, de la Directiva 93/13/EC, sobre cláusulas abusivas en contratos de consumo y, en el caso español, de su transposición en el Real Decreto Legislativo 1/2007, de 16 de noviembre, Texto Refundido de la Ley General para la defensa de consumidores y usuarios (en adelante, TRLGDCU). Sin ánimo de exhaustividad, esto implicaría que patrones que ocultan información que el empresario está obligado a proporcionar al consumidor (*v. gr*. precio total) serían ilícitos por contravenir los requisitos de información precontractual y transparencia (arts. 6 y 8 Directiva 2011/83) del mismo modo que también serían contrarios a la normativa de consumo aquellos patrones que impliquen no pedir un consentimiento separado para productos o servicios adicionales o que usen una casilla premarcada para solicitar el consentimiento (art. 22 Directiva 2011/83). También aquellos

21 No se abordan aquí los concretos mecanismos de tutela procesal que se articulan en cada norma ni otras observaciones sobre el marco normativo, como la interacción entre las normas (a excepción del RSD y la normativa de competencia desleal), o el enfoque individual y colectivo de los remedios, para lo que nos remitimos a *Mato*, Interfaces (n. 15), pp. 115 y ss.; 122 y ss.; 125 y ss.

22 Véase *Mato*, Interfaces (n. 15), pp. 76-77.

diseños que escondan renovaciones o suscripciones automáticas oscuras o con plazos breves para evitarlas (anexo 1(h) Directiva 93/13) o que dispongan la información o la petición de consentimiento de tal manera que una cláusula no negociada no pase el control de incorporación o de transparencia material (arts. 4.2 y 5 Directiva 93/13). Según la normativa española, serían expresamente ilícitos, además, patrones que dificultaran la terminación de un contrato exigiendo formalidades que no son simétricas respecto de las requeridas para darse de alta (arts. 62.2, 62.3 y 87.6 TRLGDCU).

Por otro lado, partiendo de que los patrones oscuros son prácticas que distorsionan o pueden distorsionar el comportamiento del consumidor, parece lógico buscar límites legales en la Directiva 2005/29/CE, de 11 de mayo, sobre *prácticas comerciales desleales* (transpuesta al ordenamiento jurídico español en la Ley 3/1991, de 10 de enero, de competencia desleal -en adelante, LCD-). Aunque esta norma no hace referencia expresa a los patrones oscuros -lógicamente, por el momento en el que fue adoptada-, una Guía sobre la interpretación y aplicación de esta Directiva, publicada por la Comisión Europea en 2021, incluye una sección *ad hoc* sobre esta figura y clarifica que esta norma puede ser usada para debatir la validez de estas prácticas.

Así, la Guía advierte de que algunos patrones oscuros ya están realmente prohibidos de manera expresa en la Directiva en la lista de prácticas comerciales consideradas desleales en todo caso (Anexo I): como ejemplo y entre otras, las prácticas conocidas como de "señuelo y cambio" ("*bait and switch*") -es decir, ofrecer productos a un precio determinado que no se pueden suministrar y luego negarse a aceptar pedidos o realizar entregas en un plazo razonable con la intención de promocionar un producto diferente (núm. 5, 6 Anexo I y arts. 22.1 y 22.2 LCD)- o la táctica de crear urgencia afirmando falsamente que un producto sólo estará disponible durante un tiempo muy limitado, utilizando temporizadores falsos y declaraciones de existencias limitadas en los sitios web (núm. 7 Anexo I, art. 23.4 LCD). En el caso español, también podrían ser prácticas engañosas las pruebas gratuitas engañosas o trampas de suscripción compaginadas con obstáculos para una posterior desvinculación del contrato (arts. 22.2 y 23.4 LCD) y, tras la Directiva 2019/2161, las reseñas falsas o distorsionadas de usuarios con el fin de promocionar los bienes o servicios (art. 27.8 LCD). Por otro lado, otros patrones oscuros podrían encajar en la prohibición de acciones u omisiones engañosas (arts. 6 y 7 Directiva) o prácticas agresivas (arts.

8 y 9 Directiva): acciones engañosas, como el uso de preguntas capciosas y lenguaje ambiguo para confundir al consumidor o el uso de un botón con etiquetado confuso; omisiones engañosas, como información oculta; o prácticas agresivas, como hacer que el usuario se sienta culpable o tonto.[23] Finalmente, como una cláusula de cierre, si el patrón oscuro no encaja en ninguno de estos supuestos, la Directiva prohíbe las prácticas que afectan al comportamiento económico de un consumidor y que son contrarias a lo que exigiría la "diligencia profesional". La Guía de la Comisión expresamente señala que este requisito de la diligencia profesional obligaría al empresario a adoptar medidas adecuadas para garantizar que el diseño de su interfaz no altera las decisiones de los consumidores.[24] Teniendo en cuenta que también apunta que la norma no exige que exista una *intención* de aplicar el patrón oscuro para que estemos ante un acto desleal,[25] el ilícito existirá desde el momento en el que el diseño de la web incluya estas técnicas, con independencia de que el empresario buscara este efecto distorsionador o incluso fuera consciente de él.

A la vista de todo lo anterior, la normativa sobre prácticas desleales podría ser actualmente una de las normas principales para controlar los patrones oscuros (cuando no están involucrados datos personales). Uno de los obstáculos que se le puede achacar es que, más allá de las contadas prohibiciones específicas de la lista negra, en muchos casos es necesario aplicar cláusulas o conceptos generales que necesitan ser especificados caso por caso.

Dentro de un conjunto de normas más reciente en las que el legislador europeo enfrenta ya expresamente la existencia de los patrones oscuros, debemos comenzar por el ya aludido Reglamento 2022/2065, de Servicios Digitales (en adelante, RSD), primera norma que regula de manera explícita esta figura, prohibiendo las técnicas que "engañen o manipulen a los destinatarios del servicio o [...] distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas" (art. 25.1).

Se ha optado, por tanto, por positivizar una definición amplia de patrón oscuro, que se completa con tres supuestos de prácticas específicas que -entendemos, por su habitualidad y especial efecto pernicioso- se ponen

23 *Comisión Europea*, Directrices sobre la interpretación y la aplicación de la Directiva 2011/83/UE sobre los derechos de los consumidores, 2021/C525/01, 2021, p. 101.
24 Comisión Europea, Directrices (n. 23), p. 101.
25 Comisión Europea, Directrices (n. 23), p. 101.

de relieve. Como una enumeración que debemos entender como *numerus apertus* ("en particular", señala el art. 25.3 RSD, al referirse a los supuestos concretos y, por lo tanto, no excluyendo otras), el legislador ha seleccionado para destacar aquellas prácticas que buscan manipular al usuario con el formato de la información, las técnicas de persistencia o *nagging* y las de obstrucción para darse de baja o *roach motel*. Aunque redactado de una manera un tanto inusual, parece que habrá que estar a futuras posibles directrices a las que se refiere la norma para tener un perfil más concreto de los tres supuestos subrayados y para, esperemos, un reconocimiento expreso de más tipologías de patrones oscuros, siguiendo las diversas clasificaciones de la doctrina.

Sin embargo, lo que a primera vista parecería *la* solución a los patrones oscuros, debe matizarse, por dos razones. En primer lugar y, en lo que al ámbito subjetivo de aplicación de la norma respecta, porque, la prohibición del art. 25 RSD no se refiere a todos los prestadores de servicios de intermediación, sino solo a los prestadores de plataformas en línea (Sección 3), y, por otro lado, excluye a los microempresarios y pequeñas empresas (art. 19), aunque los patrones se utilizan por empresarios de todos los tamaños. Parece, por tanto, que el RSD está enfocado a controlar prácticas engañosas que tengan un cierto impacto en la sociedad. En segundo lugar, y más importante, porque, tal y como se recoge en el apartado segundo del art. 25 RSD, la prohibición "no se aplicará a las prácticas contempladas en la Directiva 2005/29/CE".

No es inequívoca la forma de entender esta relación aparentemente excluyente entre ambas normas. Una opción sería entender que se refiere a que no se aplica a ninguna práctica comercial entre empresarios y consumidores[26]. Otra, que hace alusión solo a las prácticas comerciales no cubiertas por la Directiva de prácticas desleales porque, aun siendo prácticas comerciales, no tuvieran esta consideración[27]. Aunque no está claro a qué solución lleva la literalidad del texto, nos parece más razonable la segunda opción. Entender que el art. 25 RSD no se puede aplicar a las prácticas comerciales entre profesionales y consumidores, en general, reduciría considerablemente la utilidad de la prohibición de los patrones oscuros, pues,

26 *B. Raue*, Art. 25 DSA, en: F. Hofmann/B. Raue (eds.), Digital Services Act. Article-by-Article Commentary, Baden-Baden, 2025, pp. 522.

27 *M. J. Sørensen/P. Rott/K. Sein,* Response of the European Law Institute to European Commission's public consultation on digital fairness. Fitness check on EU Consumer Law, European Law Institute, 2023, pp. 9-10.

*a sensu contrario*, solo podría aplicarse a otro tipo de prácticas comerciales, por ejemplo, entre empresarios, o bien a prácticas que no sean comerciales[28]. La segunda interpretación permitiría, sin embargo, más juego para el RSD, pues posibilitaría una cierta relación de complementariedad: técnicas de diseño que no pudieran ser declaradas desleales por la normativa de competencia desleal podrían quedar amparadas, sin embargo, por la definición del art. 25.1 RSD. Esto daría un mayor sentido a la existencia de esta norma y a la prohibición de patrones oscuros: al abordar directa y expresamente el fenómeno de los patrones oscuros, el art. 25 RSD tendría un papel de cláusula de cierre, pues vendría a ser un mecanismo para expulsar aquellas prácticas que pudieran quedar sin control a través de la norma de defensa de la competencia, más limitada porque no contempla expresamente este fenómeno. Además, según la delimitación literal del art. 3.1 de la Directiva de prácticas desleales, el ámbito de aplicación de aplicación de la norma es "las prácticas comerciales desleales entre empresarios y consumidores". Es decir, podría argumentarse que cuando no califican como desleales, no entran dentro del ámbito de la norma.

Conviene reconocer, no obstante, la incertidumbre que deja esta composición con el epígrafe 2 del art. 25 en vigor. El hecho de que en una cierta parte de los casos no esté claro qué patrones oscuros están cubiertos por la normativa de competencia desleal -o qué intensidad tendrían que presentar algunos para ser relevantes para la normativa de competencia desleal- comporta que, correlativamente, tampoco sepamos qué cubre el RSD, lo que supone un detrimento para la aplicación efectiva de ambas normas: el riesgo de no saber cómo canalizar o argumentar jurídicamente en cada caso puede desincentivar las acciones frente a estas prácticas, siendo el resultado contrario al perseguido. A este obstáculo se ha añadido la dificultad que supondría que las autoridades nacionales competentes en materia de competencia desleal (con transposiciones de la Directiva europea que pueden variar) tengan que pronunciarse primero respecto de si una técnica de diseño es o no desleal y, por tanto, puede o no el RSD ser invocado.[29]. De ahí que estemos de acuerdo con los autores que han

28 Siguiendo a *Raue* Art, 25 DSA (n. 26), p. 524, el campo de aplicación se reduciría a: contratos entre empresarios; actos de consumo en los que el empresario no vende o suministra al consumidor, sino que compra -*v. gr*. compra al consumidor de oro u objetos de segunda mano-; actos que no pretenden influir en el comportamiento económico del consumidor, *v.gr*. la decisión de expresar una opinión.

29 *F. Di Porto/A. Egberts,* The collective welfare dimension of dark patterns regulation, European Law Journal, n. 29, 2023, p. 134.

propuesto la eliminación del apartado 2 del artículo 25 RSD[30]. Al menos el objetivo de controlar los patrones oscuros no se vería menoscabado porque los mecanismos no estarían limitados, es decir, podrían invocarse ambas normas, como ocurre en otros casos aquí analizados.

Sea como fuere, esta es una cuestión a aclarar por parte de unas posibles directrices de la Comisión Europea (en el entendido de que llegarán estas antes que la jurisprudencia) pues sí hay un acuerdo en que la interacción entre ambas normas no es clara y que esto genera incertidumbre.[31] No en vano, esta cuestión concreta fue el problema de coherencia normativa más reportado en el *Fitness Check* del Derecho de digital de consumo de la Unión Europea, cuyos resultados se hicieron públicos en octubre de 2024.[32]

Continuando con el repaso al marco normativo, cabe señalar que en el mismo año que el RSD se había publicado el Reglamento 2022/1925, de Mercados digitales (en adelante, RMD). Si bien esta norma no tiene como objetivo tanto la protección de los usuarios del entorno digital como fomentar un entorno competitivo en la esfera digital, son relevantes en su ámbito de aplicación los patrones oscuros, pues desde el punto de vista colectivo pueden generar fallos de mercado, afectar a la confianza de los consumidores en el mercado digital y afectar a la libre competencia.[33] Así, el RMD no se refiere expresamente a ellos con esta denominación, pero sí contempla ciertas obligaciones relacionadas con el diseño de interfaces y que afectan a las grandes plataformas, los llamados "guardianes de acceso" (*v. gr.* arts. 5.2.d), 5.8, 5.2 *in fine*, 6.3, art. 13.4 y 6 RMD).[34] En cualquier caso y en rigor, si bien es cierto que los patrones oscuros se consideran por el RMD como una práctica a erradicar en la medida en que pueden afectar al comportamiento y toma de decisiones racionales de los usuarios y, por tanto, a la competencia, su potencial como norma a controlarlos se ve limitada, por un lado, de nuevo por su ámbito subjetivo -esto es, solo

30 *Sørensen/Rott/Sein,* Response (n. 27), p. 10; *Di Porto/Egberts*, Collective (n. 29), p. 139.

31 *T. Akhurst/L. Zurdo/R. Rapparini/C. Mautner*, How should the European Union regulate dark patterns?, Sciences Po Chair Digital, Governance and Sovereignty, 2023, pp. 18-19 y 26.

32 *M. Whittle*, Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive. Final Report, European Commission, 2024, p. 31.

33 Sobre el impacto individual y también colectivo de los patrones oscuros, *vid. Mato*, Interfaces (n. 15), pp. 62 y ss.

34 *Mato*, Interfaces (n. 15), pp. 97-99.

obligaría a no usar patrones oscuros a los guardianes de acceso- y, por otro lado, por el hecho de que el patrón oscuro tiene que estar relacionado directamente con los supuestos de hecho de los arts. 5, 6 y 7 RMD para entrar en la prohibición.[35]

Por su parte, en 2023 se aprueban dos normas con ámbitos de aplicación, si bien relacionados con el entorno digital, mucho más acotados que las anteriores, pero que también hacen referencia al fenómeno de las técnicas de diseño engañosas. Nos referimos a la Directiva (UE) 2023/2673, de 22 de noviembre de 2023, relativa a contratos de servicios financieros celebrados a distancia y al Reglamento (EU) 2023/2854, 13 de diciembre, para un acceso justo a los datos y su utilización.

Efectivamente, cada norma, en su ámbito, incluye una prohibición expresa a los patrones oscuros. Lo hace la *Directiva sobre contratos financieros a distancia* en el que sería el nuevo art. 16 *sexies* de la Directiva 2011/83, dirigido a las entidades que prestan dichos servicios financieros a distancia y con una definición idéntica a la recogida en el RSD. Resulta, a nuestro juicio, un acierto mantener una definición más o menos uniforme para evitar distorsiones entre dos normas, que están llamadas a ser complementarias (Cdo. 41): mientras que el RSD se dirige a los prestadores de servicios intermediarios que explotan plataformas en línea, la Directiva 2023/2673 se dirige a los comerciantes que ofrezcan servicios financieros a distancia, sujetos que en la práctica no van a coincidir.

> Aunque en las plataformas en línea se incluyan servicios financieros (*v. gr.* financiación a plazos del precio o línea de crédito), estos son prestados por una entidad diferente: por ejemplo, Amazon ofrece la posibilidad de financiar la adquisición de ciertos productos que pone en el mercado -como vendedor y no solo como intermediario-, pero es Cofidis la entidad que realmente es el proveedor del servicio financiero de pago aplazado.

Por su parte, el *Reglamento de Datos* se ocupa de los patrones oscuros en el art. 6.2.a), dirigido a los terceros que reciban datos de los usuarios generados por dispositivos conectados.

> Un ejemplo en el que sería de aplicación esta prohibición recogida en el art. 6 DA sería el de datos que se ceden a una compañía de seguros sobre, por ejemplo, la conducción de un coche o el uso de un reloj inteligente

35 *E. Mackinnon/J. King*, Do the DSA and DMA have what it takes to take on dark patterns?, Tech Policy Press, June 2023, p. 12.

> o de una aplicación de hacer ejercicio, para que la compañía calcule las cuotas del seguro de coche o del seguro de vida o salud (teniendo en cuenta si conduce más o menos rápido, si hace más o menos ejercicio, cuántas horas duerme, etc.). En este supuesto, el usuario sería el sujeto que usa el coche o reloj inteligente, el titular de los datos sería el fabricante/proveedor del producto o servicio y el destinatario de los datos o tercero sería la compañía de seguros.

Y, cerrando esta breve visión panorámica por los diferentes mecanismos legales de protección frente a los patrones oscuros, si se ha señalado al inicio que hoy en día el peligro de estas prácticas es su potencial impacto a través de interfaces dinámicas y personalizadas, controladas por algoritmos de aprendizaje perfeccionados con la recopilación continua de datos,[36] tiene todo el sentido que el *Reglamento de Inteligencia Artificial* (Reglamento (UE) 2023/2854, de 13 de diciembre; en adelante, RIA) recoja una mención a los patrones oscuros. Lo hace dentro de las prácticas prohibidas, en el art. 5.1, letras a) y b), texto que ha sufrido diversas modificaciones durante la tramitación parlamentaria y respecto del que se pueden resaltar varias apreciaciones: (i) se aporta una cláusula general (sin ejemplos de supuestos concretos) cuyos elementos clave nos recuerdan a los presentes en otras normas -*v. gr.* las ideas de "manipulación" y "engaño"-, si bien se añade una referencia a las una referencia a las "técnicas subliminales", en el sentido de que actúan más allá del umbral de percepción consciente, eludiendo las defensas racionales de una persona contra la manipulación;[37] (ii) en la versión final se ha eliminado el requisito de intencionalidad de afectar el comportamiento de la persona de tal modo que pudiera causar daños -sí presente en la Propuesta inicial-,[38] hecho que valoramos positivamente pues así no se aparta del resto de definiciones legales, porque la intencionalidad es difícil de probar normalmente -más para un consumidor- y, por último, porque el hecho de que los patrones oscuros se incluyan en la

36 *Mackinnon/King*, DSA (n. 35).

37 Como señala la *European Commission*, Approval of the content of the draft Communication from the Commission – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689, February 2025, p. 20, las técnicas subliminales pueden utilizar estímulos emitidos a través de medios sonoros, visuales o táctiles que, aun siendo demasiados breves o sutiles para ser percibidos por el consciente, sí que afectan al subconsciente y son capaces de influir en los estados emocionales o el comportamiento de los usuarios.

38 En el texto definitivo se habla de que las técnicas se hayan incluido "con el objetivo *o el efecto* de alterar de manera sustancial […]" (la cursiva es nuestra).

web del empresario -dentro de su ámbito de control- nos parece suficiente para exigir al empresario que responda por los diseños que menoscaben o afecten negativamente al comportamiento del consumidor, aunque fuese con un comportamiento culpable o negligente, sin exigir intención;[39] (iii) si bien inicialmente el ámbito de la Propuesta a los daños físicos o psíquicos individuales, en la versión definitiva se eliminaron estos adjetivos -acertadamente, en nuestra opinión-[40], aunque sí que se exige que los daños sean "considerables", en la idea, entendemos, de dejar fuera de la prohibición técnicas de diseño que pueden estar más cerca de estrategias de marketing que de conductas ilícitas; el problema sí estará en cómo medir cuándo unos daños -económicos, físicos o psíquicos- tienen esa mínima entidad requerida.

> En las directrices recientemente publicadas acerca de la interpretación del art. 5 del Reglamento de Inteligencia Artificial, la Comisión Europea ha identificado varios aspectos que podrían tenerse en cuenta para evaluar el daño. Así, sin perjuicio de que hay que estar al contexto y las circunstancias individuales de cada caso, podría tenerse en cuenta la gravedad del daño (*v. gr*. combinación de varios tipos de daño), los efectos acumulativos, la escala e intensidad (*v. gr.* si afecta a un gran número de personas), el perfil de los -potenciales- afectados (*v. gr*. niños, personas con discapacidad) o la duración y reversibilidad (*v. gr.* no es igual un perjuicio temporal que uno duradero o uno reversible que otro que no lo es).[41]

Por último, (iv) es una novedad relativa que expresamente se tenga en cuenta a los patrones oscuros en relación con grupos que podrían ser vulnerables, pues es algo que no ocurre -al menos no tan abiertamente en el propio texto de la norma- en otros casos. Concretamente, se refiere a grupos vulnerables "debido a su edad, discapacidad o una situación social económica específica" (art. 5.1 b) RIA).

---

39 Este hecho ha sido confirmado por las Directrices sobre las prácticas prohibidas en el Reglamento de Inteligencia Artificial publicadas por la Comisión Europea el pasado febrero de 2025 (*European Commission*, IA (nota 37), pp. 21 y 24).

40 *M. Veale/F. Zuiderveen,* Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International, n. 4, 2021, p. 99; *N. Smuha/E. Ahmed-Rengers/ A. Harkens/W. Li/J. Maclaren/R. Piselli/K. Yeung,* How the EU can achieve legally trustworthy: A response to the European Commission's Proposal for an Artificial Intelligence Act, agosto 2021, pp. 21, 56; *Mato*, Interfaces (n. 15), p. 105.

41 *European Commission*, IA (n. 37) pp. 30-31.

## D. El impacto de la Inteligencia Artificial y el usuario vulnerable en el entorno digital

### I. La Inteligencia Artificial y la rápida evolución hacia nuevas fórmulas de manipulación

Como se había señalado, las técnicas de diseño que pretenden persuadir a los consumidores para que contraten, para que se relacionen con el entorno del empresario en condiciones más beneficiosas para él o para que inviertan allí más tiempo, no son exclusivas del entorno digital y siempre han existido. Pero el fácil tratamiento de una gran cantidad de datos y la personalización a la que da lugar permiten explotar cualquier vulnerabilidad del usuario, elementos que hacen de estos patrones unas técnicas especialmente interesantes para los empresarios.[42]

Efectivamente, por un lado, la interacción de los usuarios con aparatos continuamente conectados a internet permite al empresario obtener una gran cantidad de información sobre su comportamiento; por otro, el uso de algoritmos automatizados basados en la inteligencia artificial y el uso de nuevas herramientas de análisis le posibilita procesar los datos a una gran velocidad y escala y personalizar la experiencia del usuario de una manera muy detallada.[43] Esto hace que se pueda desarrollar una experiencia de usuario más eficiente desde un punto de vista positivo para este, pero también que puedan diseñar los distintos elementos de la interfaz digital de una manera personalizada al perfil del usuario, explotando sus vulnerabilidades al dirigirse a ellos (por ejemplo, teniendo en cuenta dónde viven, si sufren alguna enfermedad vulnerable, si padecen adicciones, su situación económica o según su situación emocional en ese momento concreto).[44]

---

42 *Luguri/Strahilevitz,* Shining (n. 18), pp. 49 y 50; *Comisión Europea*, Directrices (n. 24), p. 100; *S. Cámara Lapuente*, Nuevos perfiles del consentimiento en la contratación digital en la Unión Europea: ¿navegar es contratar (servicios digitales "gratuitos")?, en: F. Gómez Pomar/I. Fernández Chacón (eds.), Estudios de derecho contractual europeo, Navarra: Aranzadi, 2022, p. 388.

43 *Competition & Markets Authority*, Online Choice Arquitecture. How digital design can harm competition and consumers. Discussion Paper. April 2022, p. 45; *OECD*, Consumer vulnerability in the digital age, OECD Digital Economy Papers, nº 355, June 2023, p. 23.

44 *OECD*, Dark commercial patterns, OECD Digital Economy Papers, nº 336, October 2022, p. 29.

> Así, se ha visto cómo se podría establecer qué tipo de preguntas engañosas funcionan con un usuario según su perfil y utilizarlas, descartando las que no obtienen resultados; qué usuarios pueden caer más fácilmente en subscripciones o compras trampa; quién invertiría más tiempo en buscar la vía para ejercitar sus derechos aunque estuviera oculta y quiénes, por el contrario, desistirían rápidamente; quiénes se quejarían y quiénes no; quiénes se sentirían afectados por técnicas que buscan hacerles sentir culpables y sobre quiénes no tendrían efecto esa estrategia en ese momento concreto.[45]

Además, el empresario puede optimizar de forma continua la interfaz de una manera relativamente fácil, rápida y con bajo coste -sobre todo a diferencia del entorno físico- a través de las conocidas como "pruebas A/B", esto es, pruebas que consisten en ensayar diferentes variantes de diseño de una interfaz con un número relevante de usuarios y averiguar qué cambio en el comportamiento de los usuarios provoca cada decisión de diseño.[46]

En definitiva, los patrones oscuros no son un fenómeno nuevo, pero, gracias a la configuración del mercado digital actual, tienen un efecto mayor que antes en este propio entorno y, desde luego, una mayor eficacia que en el mundo físico. De hecho, las nuevas fórmulas de manipulación basadas en logaritmos y que se valen de una personalización al detalle para explotar sesgos cognitivos de una manera mucho más encubierta son un claro ejemplo de la vertiginosa evolución del entorno digital, con efectos también en lo que a la regulación de la prohibición de los patrones oscuros se refiere.

Así las cosas, se está pasando de unos "trucos" estáticos de diseño de la interfaz a estrategias dinámicas más sofisticadas. En este sentido, se ha propuesto por algunos autores una clasificación transversal de patrones oscuros basada en la visibilidad del patrón. Así, se podría hablar de "patrones visibles" (aquellos fácilmente detectables en la interfaz, como *pop ups* insistiendo en una opción o casillas premarcadas por defecto), "*darker patterns*" (aquellos que son algo más sutiles, no perceptibles de inmediato, como ocultar el botón para retirar el consentimiento, hacer caminos más largos

45 *N. Helberger/O. Lynskey/H. W. Micklitz/P. Rott/M. Sax/J. Strycharz*, EU Consumer protection 2.0. Structural asymmetries in digital consumer markets, March 2021, pp. 110-111.

46 *S. Rieger/C. Sinders*, Dark patterns: regulating digital design. How digital design practices undermine public policy efforts & how governments and regulators can respond, Stiftung Neue Verantwortung, May 2020, pp. 9 y 15.

con múltiples clics para las opciones menos deseadas por el empresario o apartados difíciles de encontrar) y "*the darkest patterns*" (esto es, fórmulas más insidiosas de manipulación basadas en logaritmos sofisticados y no siempre perceptibles por los destinatarios -como el uso de mensajes subliminales a través de sonidos o imágenes solo detectables por el subconsciente- y fórmulas basadas en la personalización extrema).[47]

Una muestra de estas nuevas fórmulas de manipulación sería la emisión de estímulos a través de medios sonoros, visuales o táctiles que sean demasiado breves o sutiles para ser percibidos. Es el caso de imágenes o textos que parpadean brevemente durante la reproducción de un vídeo o mensajes verbales a bajo volumen o enmascarados por otros sonidos, y que son técnicamente visibles o audibles pero que parpadean lo suficientemente rápido o son tan sutiles que la mente no los registra, aunque sí son capaces de influir en actitudes, estados emocionales o comportamientos.[48] Pensemos, por ejemplo, en un sistema de IA que detecta el aburrimiento de un usuario en una experiencia digital y que emite entonces un sonido que es imperceptible pero que está diseñado para prolongar el uso.[49] Y la misma idea, con mayor recorrido posiblemente, podría aplicarse en el uso de un casco o un accesorio en un videojuego.[50] De la misma manera, se pueden combinar diversas técnicas, personalizando exhaustivamente la experiencia del usuario en un sentido negativo, explotando debilidades o vulnerabilidades como, por ejemplo, presentar a un usuario que se ha detectado que es disléxico partes de la interfaz con una redacción intrincada o enrevesada buscando precipitar determinadas acciones, como contratar o desistir de dar por terminado el contrato.[51] También sería el caso de mensajes de urgencia o escasez que se muestran en momentos estratégicamente elegidos a un usuario que realiza habitualmente apuestas en línea -pues está demostrado que a las personas que apuestan les afectan más este tipo de mensajes- o de cualquier otra técnica que manipule eficazmente al usuario en función del estado de ánimo que esté teniendo en ese momento concreto (deprimido, enfadado, feliz) o de su perfil (un usuario con una adicción).

47 Proponen esta clasificación *M. Leiser/C. Santos*, Dark patterns, enforcement and the emerging digital design Acquis: manipulation beneath the interface, European Journal of Law and Technology, vol. 15, no. 1, 2024, pp. 5 y ss.
48 Con más detalle en *European Commission*, IA (n. 37), pp. 21.
49 *Leiser/Santos*, Dark (n. 47), p. 18.
50 *European Commission*, IA (n. 37), p 21.
51 *Leiser/Santos*, Dark (n. 47), p. 13.

Y esto, de manera continua, pues el sistema de IA se está retroalimentando, aprendiendo y reajustándose de manera permanente en tiempo real.

El RSD y el RMD se han centrado quizás más en los patrones oscuros estáticos o más "tradicionales" alrededor de la interfaz del dispositivo que se maneje -por ser los primeros en ser aplicados y estar extendidos en el entorno digital-, pero, como se puede vislumbrar con los ejemplos apuntados, algunas de las nuevas prácticas manipuladoras que existen o que pueden llegar a aplicarse son dinámicas y exceden de este ámbito. De ahí que algunas voces hayan considerado conveniente que la Comisión Europea aclare el concepto de "interfaz" utilizado por estas normas, dejando claro que tiene una amplitud suficiente como para abarcar también a estas prácticas que no pertenecen tanto -o no solo- a la cara visible de la interfaz del producto o aplicación digital con la que interactúa el usuario, sino que están incrustadas en capas más profundas (en la arquitectura del sistema) o que no requieren una superficie para interaccionar (*v. gr.* voz, realidad virtual).[52] El Reglamento de Inteligencia Artificial, por su parte, tiene lógicamente más potencial para abarcar estos patrones más oscuros basados en logaritmos (*the darkest patterns*). De hecho, las directrices que acaban de ser publicadas por la Comisión Europea sobre el art. 5 del Reglamento expresamente contemplan las técnicas subliminales sensoriales y no necesariamente derivadas de la interacción con una interfaz tradicional (por ejemplo, las interfaces emergentes máquina-cerebro a través de un casco que detecta la actividad cerebral y, en general, técnicas de manipulación subliminal sofisticada que influyen eficazmente en el comportamiento humano de forma subconsciente).[53]

A la vista de este escenario y ante los rápidos avances tecnológicos, es necesario que, sin perjuicio de determinadas prohibiciones más concretas (definidas a través de directrices, por ejemplo), se prevean otras legales articuladas de una manera lo suficientemente amplia como para dar cabida a nuevas realidades, evitando que las normas queden desfasadas al poco tiempo de su publicación.

Por otro lado, no ha pasado desapercibida una dificultad añadida para el control de ciertas técnicas basadas en algoritmos sofisticados, que no es sino su difícil detección y la necesidad de demostrar la relación de causalidad entre la práctica y un potencial daño. De este modo, el hecho

52 *Leiser/Santos*, Dark (n. 47), pp. 6, 17; *Akhurst et al.*, Regulate (n. 31), p. 19.
53 *European Commission*, IA (n. 37), p. 21.

de que estos patrones más oscuros no hayan tenido una gran presencia en un estudio que analiza las resoluciones que dictadas en materia de patrones oscuros ha llevado a pensar que no es que no existan, sino que no se detectan.[54] Así las cosas, se ha puesto de manifiesto la necesidad de que los organismos reguladores inviertan en tecnología para poder supervisar y rastrear a gran escala este tipo de prácticas[55]. También que se apoyen en otras obligaciones legales recientemente impuestas -de transparencia, de evaluación periódica o de adopción de medidas de mitigación de riesgos por parte de los empresarios, que pueden facilitar su tarea- o que, a modo pedagógico y disuasorio, se etiqueten los patrones sancionados y se publiquen los detalles de procesos, acciones y sanciones.[56]

En este sentido, es de resaltar que los mecanismos de control previstos en las distintas normas legales de aplicación a los patrones oscuros son tanto individuales como colectivos. Normas como el RGPD o las Directivas 2011/83 y 93/13, sin perjuicio de que también tengan una dimensión colectiva, prevén acciones que tienen como objetivo tutelar el interés particular del individuo afectado -bien ante los tribunales, bien ante un órgano administrativo-. Sin embargo, las nuevas normas que se han aprobado recientemente en la Unión Europea -*v. gr.* RSD, RIA; por supuesto, RMD- parecen pensar más en la dimensión colectiva de la protección: se centran en crear autoridades administrativas competentes que tienen facultades de investigación y de ejecución y cumplimiento de la normativa mediante sanciones económicas, pero no tienen tanto en mente proteger al individuo que ha podido ver afectado su interés en una transacción concreta. Siendo necesarias, pertinentes y relevantes las acciones individuales, consideramos que esta otra dimensión colectiva de la protección, "desde el sistema", es fundamental para abordar un fenómeno como los patrones oscuros, especialmente si tenemos en cuenta las peculiaridades y complejidades que comporta la inteligencia artificial y el desarrollo de la tecnología. Estamos ante prácticas cuya relevancia individualmente considerada quizás, en algunos casos, pueda ser escasa pues, por ejemplo, puede que no se haya producido daño económico o puede que el usuario no sea si quiera consciente -de hecho, las técnicas menos evidentes son las más dañinas y eficaces-. Pero estas técnicas sí tienen una gran trascendencia si se pone el foco en el daño o coste que generan a nivel colectivo. De ahí que el enfoque preventivo,

54 *Leiser/Santos*, Dark (n. 47), p. 29.
55 *Leiser/Santos*, Dark (n. 47), pp. 28, 30.
56 *Leiser/Santos*, Dark (n. 47), p. 30.

el control "desde el sistema", sea fundamental. Y de ahí también que el de los patrones oscuros no sea un caso en el que el mercado resuelva los abusos por sí solo, pues, salvando los casos más burdos, la reputación no discrimina eficazmente ni expulsa del mercado a las empresas que incluyen estas técnicas en sus interfaces porque, insistimos, el usuario ni siquiera suele ser consciente.

Por otro lado, la alta personalización de las técnicas de diseño tiene asimismo efectos en la aproximación al concepto del usuario destinatario a fin de aplicar los límites legales, pues intensifica la vulnerabilidad de *todo* usuario, sea o no vulnerable desde el punto de vista más tradicional del concepto.

## II. El usuario digital vulnerable. Usuario medio y personalización.

El perfil de sujeto que se tiene en cuenta para la aplicación de normas de protección al consumidor es, de manera general, el del conocido como "consumidor medio", esto es, en palabras del TJUE, aquel normalmente informado y razonablemente atento y perspicaz (por todas, sentencia del TJUE de 30 de abril de 2014, asunto C-26/13, caso *Kásler*). Sin embargo, desde hace tiempo se viene cuestionando la idoneidad de este concepto para abarcar a todos los perfiles de consumidores existentes en la realidad, pues en la práctica algunos de ellos pueden tener problemas para entender o asimilar la información que se les proporciona, para seguir el proceso de contratación o, en general, para tomar decisiones acordes con sus intereses. En definitiva, ciertos grupos de consumidores son más susceptibles a prácticas desleales o abusivas que otros y menos capaces de protegerse por sí mismos frente a ellas.[57] Surge, así, el concepto de consumidor vulnerable frente al de consumidor medio.

Aunque no hay una única y común definición de vulnerabilidad del consumidor,[58] podemos partir de la definición de "consumidor vulnerable" de la Comisión Europea, que lo identifica como aquel que, "como consecuencia de sus características sociodemográficas, sus características de comportamiento, su situación personal o su entorno de mercado: corre un mayor riesgo de experimentar resultados negativos en el mercado; tiene

57 *Helberger et al,* Structural (n. 45), p. 5.

58 *European Commission*, Consumer vulnerability across key markets in the European Union. Final report, January 2016, *p. 39.*

una capacidad limitada para maximizar su bienestar; tiene dificultades para obtener o asimilar información; es menos capaz de comprar, elegir o acceder a productos adecuados; o es más susceptible a determinadas prácticas comerciales".[59]

En algunas de las normas citadas en epígrafes anteriores hay alusiones directas a este fenómeno. Alguna previa a la reciente preocupación europea, como es el hecho de que el art. 5.3 Directiva 2005/29/EC y el correlativo art. 4.3 LCD tengan en cuenta, por contraste con el consumidor medio, la perspectiva de ciertos grupos de consumidores para valorar la susceptibilidad de que una práctica distorsione su comportamiento económico. La vulnerabilidad vendría dada aquí, según reza el último precepto, por "presentar una discapacidad, por tener afectada su capacidad de comprensión o por su edad o su credulidad".[60]

Por su parte, de manera más reciente y en el TRLGDCU español se ha introducido en el art. 3, párrafo 2º, el concepto de "personas consumidoras vulnerables", concepto abordado de una manera muy amplia pues se refiere a "aquellas personas físicas que, de forma individual o colectiva, por sus características, necesidades o circunstancias personales, económicas, educativas o sociales, se encuentran, aunque sea territorial, sectorial o temporalmente, en una especial situación de subordinación, indefensión o desprotección que les impide el ejercicio de sus derechos como personas consumidoras en condiciones de igualdad".

En tercer y último lugar y, además, ya específicamente circunscrita a los patrones oscuros, la Propuesta de Reglamento de IA pone el foco en la necesidad de protección especial de ciertos grupos de personas, identificados por su "edad o discapacidad física o mental". Es de notar, sin embargo, que en el texto definitivo del Reglamento se han modificado los criterios y se hace referencia a la "edad, discapacidad o a una situación social o económica específica", ampliando -desde nuestro punto de vista, correctamente- el concepto a través de otros factores nuevos.

Algún autor, respecto de la versión de la Propuesta inicial, reclamó ampliar la referencia a grupos vulnerables para incluir a todas las características protegidas del art. 21 de la Carta de los Derechos Fundamen-

59 *European Commission*, Vulnerability (n. 58) (la traducción es nuestra).

60 Se pone el acento en características personales, *European Commission*, Vulnerability (nota 58), p. 44; *N. Helberger/M. Sax/J. Strycharz/H. W. Mickiltz*, Choice architectures in the digital economy: Towards a new understanding of digital vulnerability, Journal of Consumer Policy, 2022, vol. 45, p. 178.

> tales de la Unión Europea (2000/C 364/01), esto es: sexo, raza, color, orígenes étnicos o sociales, características genéticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual.[61] Consideramos, no obstante, que la redacción del RIA es más adecuada pues incluye un criterio que podría englobar los señalados, de ser relevantes. En este sentido, como respaldo a esta idea, las Directrices de la Comisión Europea recientemente publicadas han aclarado que con la categoría "situación socioeconómica específica" se pretende abarcar, en principio, características relativamente estables y a largo plazo, aunque las circunstancias transitorias -como el desempleo temporal, el sobreendeudamiento o la situación migratoria- también pueden incluirse. Un ejemplo podría ser el uso de algoritmos predictivos de IA para dirigir ofertas de productos financieros depredadores a personas que vivan en códigos postales de bajos ingresos y que se encuentren en una situación financiera desesperada, explotando así su susceptibilidad y causándoles un importante perjuicio financiero.[62]

Siguiendo esta línea, el análisis del comportamiento de los usuarios mediante experimentos empíricos ha permitido identificar algunas de estas características como relevantes para la eficacia de los patrones oscuros. A tal efecto, la edad es un factor a tener en cuenta, bien porque el sujeto pertenezca al colectivo de adultos mayores -se asocia con una disminución de la capacidad de toma de decisiones debido al deterioro cognitivo, potenciada en el entorno digital-,[63] bien por tratarse de niños o jóvenes -por la falta de experiencia como consumidores y por la menor capacidad para resistir la influencia de elementos persuasivos, aunque los identifiquen, potenciándose estos riesgos en el mundo digital respecto del *offline*-.[64] En este sentido, resalta la Comisión Europea que los niños son especialmente susceptibles a la manipulación debido a su inmadurez cognitiva y socioemocional y a que son muy impresionables. No tienen el desarrollo suficiente para evaluar de forma crítica los contenidos persuasivos o para resistirse a determinadas prácticas.[65]

---

61 *Smuha et al*, AIA (n. 40), pp. 22 y 56.
62 *European Commission*, IA (n. 37), pp. 37-38.
63 *OECD*, Vulnerability (n. 43), p. 18; *Lupiáñez-Villanueva et al*, Behavioural (n. 16), pp. 6 y 121; *European Commission*, IA (n. 37), pp. 35-36 y 40.
64 *OECD*, Vulnerability (n. 43), p. 21; *OECD*, Patterns (n. 44), p. 28.
65 *European Commission*, IA (n. 37), pp. 34-35 y 39-40.

Por otro lado, si bien la situación social o económica no aparece en rigor explícitamente como tal identificada en muchos de los estudios, sí que podría vincularse a nuestro juicio en algunos casos con otro factor que se señala repetidamente como relevante para generar vulnerabilidad frente a prácticas de diseño engañosas. Nos referimos al nivel formativo del usuario: se ha concluido en diversos experimentos que aquellos sujetos con menos estudios son más susceptibles de ser afectados por los patrones oscuros, tanto los más agresivos como aquellos más suaves.[66]

> En el texto principal hemos hecho referencia a la edad e, indirectamente, a la situación socioeconómica del usuario. De los criterios identificados por las distintas normas, nos faltaría aludir a la discapacidad, pero -al menos, hasta donde sabemos- no hay estudios sobre patrones oscuros y discapacidad. Entendemos que el concepto discapacidad engloba un conjunto de situaciones muy dispares y que, por tanto, no es fácil reflejar esto en un estudio con resultados concluyentes. No relacionado con la discapacidad, pero sí con rasgos de la personalidad, *Luguri/Strahilevitz,* Shining concluyen que ciertos rasgos como ser extrovertido o no ser muy concienzudo hacen que el sujeto sea más propenso a verse afectado por los patrones oscuros menos agresivos.[67]

Llegados a este punto, cabe plantearse la utilidad de la figura del consumidor o usuario medio en el ámbito digital y, en lo que aquí concierne, respecto de los patrones oscuros. El origen de las dudas reside en que, de acuerdo con las evidencias científicas, todos los usuarios tienen sesgos y corren el riesgo potencial de ser manipulados, independientemente de su edad, ingresos o formación.[68] Así, estudios realizados concluyen que todos los sujetos -tanto usuarios medios como vulnerables- son susceptibles de verse afectados por prácticas engañosas y solo aquellos individuos formados y con conocimientos en la materia concreta (ya sea por formar parte de la industria, del mundo académico, de asociaciones de consumidores o ser responsables políticos) habrían presentado un mayor nivel de conciencia frente a las técnicas empleadas.[69] De hecho, de este último estudio citado

66 *Luguri/Strahilevitz,* Shining (n. 17), pp. 27-28; *OECD*, Patterns (n. 44), p. 28; *Lupiáñez-Villanueva et al*, Behavioural (n. 16), p. 121.
67 *Luguri/Strahilevitz,* Shining (n. 17), pp. 28-29.
68 *C. A. Zac/Y. H. Huang/A. Moltke/C. Decker/A. Ezrachi*, Dark patterns and consumer vulnerability, August 2023, p. 3.
69 *Lupiáñez-Villanueva et al*, Behavioural (n. 16), p. 120.

se deriva que los consumidores parecen aceptar su presencia como parte normal de la experiencia y se acostumbran a ellos.

Puestas así las cosas, se ha dicho que el usuario medio es "un prototipo no realista" de usuario, pues los mercados digitales se caracterizan por desequilibrios estructurales y por diseños que persiguen explotar los distintos sesgos,[70] y los experimentos demuestran que tener sesgos es la regla general y no la excepción.[71] Aunque en un contexto diferente, el propio TJUE ha aceptado a finales de 2024 y por primera vez el concepto de consumidor "de racionalidad limitada", afectado por sesgos cognitivos, que podrán ser tenidos en cuenta en algún caso si pueden afectar al consentimiento de una persona normalmente informada y razonablemente atenta y perspicaz (STJUE de 14 de noviembre de 2024, *Compass Banca*, C-646/22).[72]

Por lo tanto, la vulnerabilidad es arquitectónica en la sociedad digital porque el diseño de las distintas elecciones digitales por las que se navega está pensado para interferir o incluso crear vulnerabilidades,[73] efecto potenciado, además, por el hecho de que se esté continuamente recopilando datos, llevando a cabo experimentos y haciendo ajustes en función de los resultados, para optimizar los patrones de comportamiento.[74] La personalización se ha revelado, así, como una fuente de influencia en el comportamiento y una nueva forma de asimetría de informaciónque afecta a todos los usuarios: el empresario sabe mucho más del consumidor que a la inversa, con el agravante de que el mensaje del empresario, gracias a la personalización, genera una mayor sensación de credibilidad.[75]

El tratamiento jurídico de los patrones oscuros no puede ignorar esta evidencia empírica. Partiendo de esta premisa, se comprenderá que el punto de referencia para valorar la licitud de un patrón oscuro no puede ser el de un usuario informado y perspicaz del mundo fuera de línea -que no debería verse afectado por trucos de diseño porque es capaz de tomar decisiones racionales- porque el comportamiento difiere cuando este usuario se

70 *Zac et al*, Dark (n. 68), p. 3.
71 *V. Stango/J. Zinman*, We are all behavioural, more or less: A taxonomy of consumer decision making, NBER Working Paper no. 28138, November 2020, p. 1.
72 Sobre este concepto, *vid. S. Cámara Lapuente*, Tres personajes en busca de transparencia (objetiva), *Almacén de Derecho*, 13 de diciembre de 2024.
73 *Helberger et al,* Structural (n. 45), p. 19.
74 *Helberger et al,* Structural (n. 45), p. 18; *Luguri/Strahilevitz,* Shining (n.17), pp. 49-50.
75 *OECD*, Vulnerability (nota 43), p. 23.

mueve en el entorno digital actual.[76] A la hora de regular a futuro y a la hora de aplicar el marco normativo existente, hay que tener en cuenta cómo realmente se comportan los usuarios y que no hay usuario medio que no pueda volverse vulnerable.[77] En definitiva, a nuestro juicio, esto tiene dos consecuencias. Por un lado, implica que cuando se valore la licitud de una práctica desde una perspectiva abstracta hay que bajar el listón de exigencia del usuario medio en el ámbito digital (o del usuario medio dentro de un grupo delimitado -*v. gr.* niños o adolescentes y videojuegos-). En segundo lugar, que cuando se valora la repercusión de una práctica en el contexto de una acción particular en la que ha habido una personalización tal que haya influido en el efecto, habrá que tener en cuenta esas circunstancias concretas (y no las de un usuario medio genérico).

Pues bien, esta composición podría tener cabida en la normativa actual. Los criterios para ser considerado consumidor vulnerable en la Directiva 2005/29/CE y en su transposición a la española LCD son limitados -discapacidad, edad, credulidad- y, como hemos visto, no todas las vulnerabilidades de la sociedad digital encajan en ellos. Si el supuesto no se subsume en esas rígidas categorías, quedaría aplicar la regla general del consumidor medio, aunque estimamos que, en línea con lo expuesto, habría que reconsiderar el hecho de que el punto de referencia para valorar si un patrón oscuro afecta o no al comportamiento del consumidor -y, en su caso, en qué medida lo hace- sea el del consumidor medio, entendido en el sentido tradicional del concepto. Pero, en este punto, las Directrices de la Comisión Europea sobre la interpretación y aplicación de la Directiva 2005/29/CE, publicadas en diciembre de 2021, pueden ayudar a adaptar la aplicación del concepto de consumidor medio y los criterios de vulnerabilidad a la realidad de los patrones oscuros mostrada. Primero, porque en el apartado relativo a "Prácticas basadas en los datos y patrones oscuros" se aclara que el valor de referencia del consumidor medio o vulnerable "puede modularse en función del grupo destinatario" e, inclusive, "si la práctica es muy personalizada, puede incluso formularse desde la perspectiva de una sola persona que haya estado sujeta a la personalización específica".[78] Es

76 Esta última diferencia entre lo que los usuarios toleran en el mundo en línea y fuera de él la señala *Mik*, Erosion (n. 13), p. 36.

77 *Mik*, Erosion (n. 13), p. 34; *Sørensen/Rott/Sein,* Response (n. 27), p. 8; *OECD*, Vulnerability (n. 43), p. 28.

78 *European Commission*, Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair

decir, se está permitiendo eliminar la perspectiva del consumidor medio hasta el punto de que se acepta la valoración caso por caso de la influencia de una práctica en un supuesto concreto, si fuera necesario. Y, en segundo lugar, porque también rebaja la rigidez de los criterios para ser considerado consumidor vulnerable, señalando que esas características "son indicativas y no exhaustivas" y reconociendo lo que han venido demostrando los experimentos, es decir, que la vulnerabilidad (también de la Directiva sobre prácticas desleales) es un concepto "dinámico y situacional" y que, por tanto, algunos consumidores pueden no ser vulnerables en unos contextos y sí en otros, especialmente en el entorno digital.[79]

En cuanto al RSD, la norma no contrapone "usuario medio" y "usuario vulnerable" sino que prohíbe, en general, los patrones oscuros, entendiendo que todos los usuarios pueden verse afectados por ellos y, por tanto, merecen protección. Si bien se ha señalado en la doctrina que, aunque la norma no explicita el punto de referencia, con carácter general parece que sería el de un destinatario del servicio medio, también se ha advertido acerca del mandato del legislador de tener en cuenta la evidencia científica en materia de comportamiento económico en la protección de los usuarios y acerca del hecho de que si la plataforma adapta una práctica a un usuario -la personaliza- el efecto en cada usuario debe ser considerado individualmente.[80]

Por su parte, las autoridades de vigilancia del mercado competentes en la aplicación del Reglamento de Inteligencia Artificial -otra de las normas claves en la prohibición de determinados patrones oscuros- también deben evaluar las circunstancias de una determinada técnica partiendo del "individuo medio", tal y como aclara la Comisión Europea en sus directrices publicadas en febrero de 2025, para mantener, precisamente, la coherencia con la Directiva de prácticas desleales, a la que -señala- pretende complementar. Pero, del mismo modo, si la manipulación fuera muy adaptada o personalizada o con efectos perjudiciales sobre grupos vulnerables específicos, podrían examinarse esas técnicas desde la perspectiva de la persona concreta, evaluando en qué medida el sistema de IA era capaz de menoscabar su autonomía individual en casos concretos y en qué medida se ha producido o era probable que se produjera un daño considerable.[81]

---

business-to-consumer commercial practices in the internal market, December 2021 (2021/0 526/01), p. 100.

79 *European Commission*, Guidance (n. 78), p. 100.

80 *Raue,* Art. 25 DSA (n. 26), pp. 511 y 512.

81 *European Commission*, IA (n. 37), p. 26.

Con este enfoque, la línea entre usuario vulnerable y usuario medio puede llegar a desdibujarse,[82] pero esto no sería sino consecuencia de, por un lado, las características y naturaleza del entorno digital (en el que el usuario medio presenta ciertas vulnerabilidades estructurales) y, por otro y en su caso, de la personalización exhaustiva de las prácticas. Es decir, respecto a esto último, consecuencia de que se pierda, en cierto modo, el sentido del concepto de "usuario medio", como concepto que surgió -en su versión de "consumidor medio"- para lograr un equilibrio entre la necesidad de proteger a los usuarios, por un lado, y de facilitar a los empresarios comercializar sus productos o servicios atendiendo a un estándar objetivo, por otro: si el empresario se ha podido dirigir al usuario de manera personalizada "gracias" a la tecnología, es este el estándar -el personalizado, con sus vulnerabilidades concretas- el que hay que tener en cuenta para valorar esa interacción y no el de un usuario medio. En cualquier caso, no se trata de no reconocer que determinados colectivos puedan estar especialmente desprotegidos frente a los patrones oscuros por sus características o posición, sino de ser conscientes -a la hora de configurar y aplicar los límites legales- de que, incluso aun no estando dentro de esos colectivos, también puede haber situaciones en las que el diseño de las interfaces, tal y como se está desarrollando en la actualidad, se aprovecha de una vulnerabilidad del usuario, coyuntural o no.

De hecho, aunque no en un supuesto en el ámbito digital, el TJUE ha reconocido recientemente y por primera vez -sentencia de 14 de noviembre de 2024, asunto C-646/22- que en ciertos casos el consumidor medio de la Directiva 2005/29 (el *homo economicus*, perfectamente racional en la toma de sus decisiones) puede verse afectado por sesgos cognitivos que pueden alterar su comportamiento y pasar a ser el consumidor de racionalidad limitada. Es decir, ha puesto la semilla para entender que, efectivamente, no siempre el consumidor medio es racional.

### *E. Conclusiones*

El diseño de las interfaces digitales tiene un demostrado impacto en la autonomía contractual del usuario, lo que ha llevado a que la disciplina conocida como *legal design*, que pretende un equilibrio entre la precisión jurídica y la usabilidad de los contratos y la información legal, haya expe-

82 Así lo señala también *OECD*, Vulnerability (n. 43), p. 32.

rimentado un auge en los últimos años en este ámbito. Sin embargo, los conocimientos acerca del comportamiento humano sobre los que se asienta este campo de estudio pueden enfocarse también en un sentido opuesto, es decir, buscando manipular o engañar al usuario en la toma de sus decisiones. Una de las manifestaciones de este fenómeno la constituyen los patrones oscuros.

A pesar de que, como se ha visto, el marco normativo de la Unión Europea ofrece un amplio abanico de herramientas para abordar legalmente estas prácticas engañosas, persisten desafíos respecto de su aplicación y eficacia para dar cobertura al fenómeno. En buena parte estos desafíos vienen generados por la inteligencia artificial y la personalización extrema que esta facilita, dando lugar a nuevas técnicas de manipulación tan difíciles de detectar como, por tanto, de contrarrestar. Ante esta vertiginosa evolución, se plantea la necesidad de contar con un marco regulatorio susceptible de adaptarse (por ejemplo, vía directrices europeas) a las más modernas y sofisticadas prácticas de patrones oscuros que van ideando e implementando las empresas. En este sentido, nos parece que se trata, este, de un caso en el que hay un riesgo evidente de que el Derecho vaya por detrás de la realidad. La actualización del marco jurídico requiere de una inversión de los organismos reguladores en tecnología para supervisar, rastrear y sancionar estas técnicas, pero, aun así, la rápida evolución tecnológica y los nuevos escenarios que se plantean hacen difícil asegurar un control eficaz y sin fisuras. En todo caso, se subraya la importancia de los mecanismos de control colectivos -sin perjuicio de los individuales- para abordar este problema.

Además, el concepto tradicional del "usuario medio" se muestra insuficiente, por sí mismo, para abordar en exclusiva la realidad de las técnicas de manipulación o coacción digital. Por un lado, porque los trucos de diseño digital influyen de manera general en que no siempre se tomen decisiones racionales. Por otro lado, porque la inteligencia artificial y su enfoque altamente personalizado puede adaptar la arquitectura del sistema para aprovechar las vulnerabilidades de cada usuario individualmente considerado. Así, si bien no se puede renunciar a establecer categorías de usuarios para facilitar la aplicación de la normativa, esta realidad debe tenerse en cuenta. Cuando se valore si un patrón oscuro en el ámbito digital es lícito o no, se deben ajustar a la baja las expectativas de comportamiento del usuario medio. Si no, prácticamente ninguna técnica sería ilícita. Y si la personalización de la práctica ha sido relevante, son esas circunstancias específicas y no las de un usuario promedio genérico las que habrá que

considerar. La viabilidad de estos planteamientos tiene respaldo: por un lado y aunque en otro contexto, el TJUE ha reconocido recientemente la existencia -con consecuencias jurídicas- del consumidor de racionalidad limitada; por otro, las directrices europeas que aclaran la aplicación de algunas de las normas más relevantes en la materia aceptan la posibilidad de adoptar, en su caso, la perspectiva de un usuario concreto.