INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE LAS PERSONAS CONSUMIDORAS: ANÁLISIS Y PROPUESTAS REGULATORIAS

Investigador principal (IP)

Ángel Carrasco Perera

Catedrático de Derecho Civil. UCLM

Equipo investigador

Pascual Martínez Espín

Catedrático de Derecho Civil. UCLM

Blanca Aparicio Araque

Contratada Predoctoral FPU. UCLM

José María Martín Faba

Profesor Ayudante Doctor. UAM

ÍNDICE

ABREVIATURAS

1. Instituciones y autoridades

- **AEPD**: Agencia Española de Protección de Datos
- **AESIA**: Agencia Española de Supervisión de Inteligencia Artificial
- **BdE**: Banco de España
- **CNMC**: Comisión Nacional de los Mercados y la Competencia
- **CNMV**: Comisión Nacional del Mercado de Valores
- **DG Consumo**: Dirección General de Salud Pública, Drogodependencias y Consumo de Castilla-La Mancha
- **DGSFP**: Dirección General de Seguros y Fondos de Pensiones
- **DGT**: Dirección General de Tráfico
- **ENAC**: Entidad Nacional de Acreditación
- **ODA**: Observatorio Digital autonómico (órgano de vigilancia y análisis de riesgos en consumo digital)
- **OMIC**: Oficina Municipal de Información al Consumidor
- **SAE**: Society of Automotive Engineers (Sociedad de Ingenieros de Automoción)
- **TC**: Tribunal Constitucional
- **TS**: Tribunal Supremo
- **UE**: Unión Europea
- **UTIA**: Unidad Técnica de Inteligencia Artificial (unidad constituida dentro de la Asociación de Inteligencia Artificial de Castilla-La Mancha)

2. Normativa europea

- **Directiva (UE) 2018/1808**: Directiva de servicios de comunicación audiovisual
- **Directiva (UE) 2019/2161**: Directiva Ómnibus, modernización de normas de protección de consumidores
- **Directiva (UE) 2023/2225**: Contratos de crédito al consumo
- **Directiva (UE) 2023/2673**: Servicios financieros a distancia
- **Directiva 2005/29/CE**: Prácticas comerciales desleales
- **Directiva 2011/83/UE**: Derechos de los consumidores
- **DRPD**: Directiva (UE) 2024/2853, responsabilidad por productos defectuosos
- **REEDS**: Reglamento (UE) 2025/327, Espacio Europeo de Datos de Salud
- **Reglamento P2B**: Reglamento (UE) 2019/1150, equidad y transparencia en servicios de intermediación en línea
- **RGPD**: Reglamento (UE) 2016/679, protección de datos personales
- **AI Act**: Reglamento (UE) 2024/1689, normas armonizadas en materia de inteligencia artificial
- **RMD/DMA**: Reglamento (UE) 2022/1925, mercados digitales
- **RSD/DSA**: Reglamento (UE) 2022/2065, servicios digitales
- **TFUE**: Tratado de Funcionamiento de la Unión Europea
- **TUE**: Tratado de la Unión Europea

3. Normativa española

- **APLIA**: Anteproyecto de Ley para el buen uso y la gobernanza de la inteligencia artificial
- **CC**: Código Civil
- **CE**: Constitución Española
- **LCD**: Ley 3/1991, de Competencia Desleal
- **LCS**: Ley 50/1980, de Contrato de Seguro
- **Ley 15/2022**: Ley integral para la igualdad de trato y la no discriminación
- **LGCA**: Ley 13/2022, General de Comunicación Audiovisual
- **Ley Hipotecaria (Decreto de 1946)**: Decreto de 8 de febrero de 1946
- **LOPDGDD**: Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales
- **LOSSEAR**: Ley 20/2015, de ordenación, supervisión y solvencia de entidades aseguradoras y reaseguradoras
- **PLAC**: Proyecto de Ley de servicios de atención a la clientela (en tramitación)
- **Real Decreto 729/2023**: Estatuto de la AESIA
- **Real Decreto-ley 24/2021**: Transposición de directivas de la UE en diversas materias
- **Real Decreto-ley 6/2024**: Medidas urgentes ante la DANA
- **TRLGDCU**: Real Decreto Legislativo 1/2007, Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios
- **LCCC**: Ley 16/2011, de contratos de crédito al consumo
- **LCCI**: Ley 5/2019, reguladora de los contratos de crédito inmobiliario
- **Ley 22/2007**: Ley de comercialización a distancia de servicios financieros destinados a consumidores
- **Ley 4/2012**: Ley de contratos de aprovechamiento por turno de bienes de uso turístico
- **Ley 11/2022**: Ley General de Telecomunicaciones
- **Orden EHA/2899/2011**: Orden sobre transparencia y protección del cliente de servicios bancarios

4. Órganos y programas autonómicos

- **EARCD**: Evaluación Autonómica de Riesgos de Consumo Digital
- **EIA/DIC**: Evaluaciones de Impacto Algorítmico / Declaraciones de Impacto en Consumo
- **Registro CLMIA**: Registro autonómico de sistemas de IA con impacto relevante en consumo
- **SIA-C**: Sandbox autonómico IA–consumo
- **TC**: Tribunal Constitucional
- **TS**: Tribunal Supremo

5. Conceptos técnicos y de IA

- **DIC**: Declaración de Impacto en Consumo
- **DPIA**: Documento de Impacto de Privacidad de la IA
- **FRIA**: Fundamental Rights Impact Assessment
- **HCE**: Historia Clínica Electrónica
- **IA**: Inteligencia Artificial
- **SDA**: Sistema automatizado de Decisiones de la Administración pública
- **TIC**: Tecnologías de Información y Comunicaciones
- **VEC**: Vehículo Eléctrico y Conectado
- **VLOP**: Very Large Online Platforms
- **VLOSE**: Very Large Online Search Engines

6. Internacionales

- **FDA**: Food and Drug Administration (EE. UU.)
- **HIPAA**: Health Insurance Portability and Accountability Act (EE. UU.)
- **MHRA**: Medicines and Healthcare products Regulatory Agency (Reino Unido)
- **NHS**: National Health Service (Reino Unido)
- **SNDS**: Sistema Nacional de Datos Sanitarios (Francia)
- **UNESCO**: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
- **STJUE**: Sentencia del Tribunal de Justicia de la Unión Europea

GLOSARIO

1. IA general y consumidor

Análisis Predictivo

El análisis predictivo es una rama de análisis avanzado que hace predicciones sobre resultados futuros utilizando datos históricos combinados con modelado estadístico, técnicas de extracción de datos y aprendizaje automático.

Software

El software es todo componente intangible (y no físico) que forma parte de dispositivos, como computadoras, teléfonos móviles o tabletas y que permite su funcionamiento. El software está compuesto por un conjunto de aplicaciones y programas diseñados para cumplir diversas funciones dentro de un sistema, así como técnicas de filtrado colaborativo, basado en contenido híbrido. Ejemplos de software son los procesadores de texto, como Microsoft Word; sistemas operativos, como Windows; o aplicaciones, como Instagram o WhatsApp.

Sistemas de recomendación

El sistema de recomendación es un sistema total o parcialmente automatizado y utilizado por una plataforma en línea para proponer en su interfaz información específica para los destinatarios del servicio o priorizar dicha información, también como consecuencia de una búsqueda iniciada por el destinatario del servicio, o que determine de otro modo el orden relativo o la relevancia de la información presentada.

Chatbots

Un chatbot es un programa informático que simula la conversación humana con un usuario final. No todos los chatbots están equipados con IA pero los chatbots modernos utilizan cada vez más técnicas de IA conversacional como el procesamiento del lenguaje natural (PLN) para comprender las preguntas de los usuarios y automatizar las respuestas.

Segmentación Dinámica

La segmentación dinámica es una estrategia avanzada de marketing que permite agrupar a los usuarios o clientes en segmentos específicos según sus características, comportamientos e interacciones en tiempo real. A diferencia de la segmentación tradicional, que utiliza criterios estáticos como la edad o el género, la segmentación dinámica analiza datos actualizados continuamente, como las búsquedas recientes, las compras realizadas o las interacciones con un sitio web o aplicación

Personalización Algorítmica

La personalización algorítmica se refiere al uso de la IA para adaptar los mensajes, las recomendaciones de productos y los servicios a los usuarios individuales. Al analizar los datos y aprender del comportamiento de los usuarios, las herramientas con IA pueden crear resultados altamente personalizados que mejoran las experiencias de los clientes y aumentan el compromiso con el cliente, destacando en este sentido el artículo 27 del

Reglamento (UE) 2022/2065. Tal y como se recoge en el DSA Digitales, los destinatarios del servicio deben poder acceder directamente, desde la interfaz en línea en la que se presente el anuncio publicitario, a información sobre los principales parámetros utilizados para determinar que se les presente un anuncio publicitario específico, ofreciendo explicaciones útiles de la lógica utilizada con ese fin, también cuando se base en la elaboración de perfiles.

Visión Artificial

La visión artificial es un campo de la IA que utiliza el aprendizaje automático *(machine learning*) y las redes neuronales para enseñar a los ordenadores y sistemas a obtener información significativa de imágenes digitales, vídeos y otros elementos visuales, y a hacer recomendaciones o tomar medidas cuando ven defectos o problemas.

Procesamiento de Lenguaje Natural (PLN)

El Procesamiento del Lenguaje Natural es el campo de conocimiento de la Inteligencia Artificial que se ocupa de la investigar la manera de comunicar las máquinas con las personas mediante el uso de lenguas naturales, como el español, el inglés o el chino.

Virtualmente, cualquier lengua humana puede ser tratada por los ordenadores. Lógicamente, limitaciones de interés económico o práctico hace que solo las lenguas más habladas o utilizadas en el mundo digital tengan aplicaciones en uso.

Privacidad Algorítmica

La privacidad algorítmica asegura que ningún cliente individual pueda ser identificado o reidentificado, incluso cuando se hacen estadísticas tomando como base de datos obtenidos previamente. Esto implica que los algoritmos deben ser diseñados para preservar la confidencialidad y el anonimato de los datos y los usuarios, lo que incluye la anonimización y seudoanonimización de datos.

Optimización de Precios

La optimización de precios involucra el proceso de establecer precios óptimos que maximicen el volumen de ventas y los ingresos, considerando diversos factores internos y externos. Requiere analizar la dinámica del mercado, el comportamiento del cliente, el panorama competitivo y los costos para encontrar el delicado equilibrio entre capturar el valor del cliente y mantener la competitividad.

Publicidad Programática

La publicidad programática es un modelo de compraventa de espacios publicitarios. Éstos se adquieren de manera automatizada mediante el cruce de datos relevantes para las marcas. Destaca el uso del RTB (real-time bidding), referente a las subastas en tiempo real. Los ejemplos de su uso dependen de los datos de audiencia, siendo recurrente en plataformas más potentes o pujas por espacios publicitarios.

Aprendizaje Automático (Machine Learning)

El *machine learning* es una rama de la IA centrada en entrenar a computadoras y máquinas para imitar el modo en que aprenden los humanos, realizar tareas de forma autónoma y mejorar su rendimiento y precisión a través de la experiencia y la exposición a más datos.

Experiencia del Cliente (CX) Inteligente

La experiencia del cliente, o CX, es una descripción holística de las percepciones de los clientes que resultan de todas sus interacciones con una empresa o marca, ya sea en línea o en la tienda.

La experiencia del cliente implica la gestión de la experiencia del cliente (CXM). CXM hace referencia a las estrategias, las tecnologías y las prácticas para mejorar los resultados comerciales mediante la creación de una experiencia ideal para cualquier persona que interactúe con una empresa.

2. Ia y salud

Diagnóstico Asistido por IA

El diagnóstico asistido por IA es el uso de algoritmos de aprendizaje automático para analizar datos médicos, como imágenes (radiografías, resonancias magnéticas) o historiales clínicos, con el fin de ayudar a los profesionales de la salud a detectar enfermedades en etapas tempranas, identificar patrones complejos y predecir riesgos, mejorando así la precisión y eficiencia del diagnóstico médico.

Medicina Personalizada

En la medicina personalizada**,** conocida también como medicina de precisión, los pacientes son tratados en función de sus circunstancias individuales. Estas circunstancias individuales comprenden principalmente su bagaje genético, su estilo de vida y sus circunstancias personales**.** Su éxito se basa en la caracterización individual del paciente y la realización de pruebas previas adecuadas para determinar qué tratamiento pueden considerarse o no para un paciente concreto.

Bioinformática

La bioinformática es una disciplina científica que utiliza técnicas computacionales para recopilar, almacenar, analizar e interpretar datos biológicos**.** Surge de la necesidad de procesar la enorme cantidad de información generada por las tecnologías modernas en biología molecular, como la secuenciación del ADN, la proteómica o la genómica.

Wearables Médicos

Los “wearables” son el conjunto de aparatos o dispositivos electrónicos que se colocan en el cuerpo e interactúan con el usuario realizando una acción específica. Estos dispositivos inteligentes se caracterizan, principalmente, por estar encendidos de manera ininterrumpida (no necesitan encenderse o apagarse). Además, no requieren la interacción

del usuario para su funcionamiento, lo permite que las personas puedan llevarlo mientras realizan otras tareas

Neurotecnología

La neurotecnología es la tecnología para comprender el cerebro, visualizar sus procesos y controlar, reparar o mejorar sus funciones. La neurotecnología emplea diversas técnicas para registrar la actividad cerebral y estimular partes concretas del mismo.

Historia Clínica Electrónica (HCE)

La HCE la conforma el conjunto de documentos, tanto escritos como gráficos, que hacen referencia a los episodios de salud y enfermedad de una persona, y la actividad sanitaria que se genera con motivo de esos episodios. Tiene que garantizar unas funciones determinadas que van desde la asistencia, la investigación, la gestión clínica y la planificación de recursos asistenciales.

Telesalud

La telesalud, a veces llamada telemedicina, es el uso de tecnologías de comunicación para brindar atención médica a distancia. Estas tecnologías pueden incluir computadoras, cámaras, videoconferencia, internet y comunicaciones satelitales e inalámbricas. Algunos ejemplos de telemedicina incluyen: (i) una "visita virtual" con un profesional de la salud a través de una llamada telefónica o videollamada; (ii) monitoreo remoto del paciente, que permite a su proveedor controlarlo mientras está en casa. Por ejemplo, puede usar un dispositivo que mida su ritmo cardíaco y envíe esa información a su proveedor

Radiología Digital

La radiología digital es una forma avanzada de tecnología de imágenes médicas que utiliza medios digitales en lugar de películas tradicionales para capturar, almacenar y presentar datos radiográficos. Representa un cambio significativo en el diagnóstico por imágenes desde su introducción, mejorando notablemente la calidad de las imágenes, la eficiencia en el manejo de estas y la accesibilidad a la información radiológica. La radiología digital incluye tanto la radiografía digital directa (DR) como la radiografía computarizada (CR).

Robótica Quirúrgica

La cirugía robótica**,** o cirugía asistida por robot, es un método quirúrgico que utiliza herramientas fijadas a un brazo robótico que el cirujano controla mediante un ordenador. Este sistema permite a los cirujanos llevar a cabo procedimientos complicados con mayor precisión, maleabilidad y dominio que con las técnicas tradicionales.

3. IA y comercio

Gestión preventiva de Inventario

La gestión preventiva del inventario es una práctica que anticipa y previene problemas futuros en los niveles de stock, como el exceso que genera costos o la falta de productos que afecta la demanda. Para lograrlo, se basa en el monitoreo constante, la predicción de la demanda, el uso de tecnología, la planificación de compras como el método "justo a tiempo" (*just in time*), y la aplicación de políticas de inventario para mantener un equilibrio óptimo de existencias.

Automatización de Procesos Comerciales

La automatización de procesos empresariales (BPA) es una estrategia que utiliza software para automatizar procesos empresariales complejos y repetitivos. El objetivo principal del BPA es racionalizar las operaciones diarias para que la empresa funcione sin problemas. Estas actividades de "gestión de la empresa" son los procesos básicos que generan ingresos y ayudan a garantizar que la empresa funcione con eficacia, como la tramitación de pedidos o la gestión de cuentas de clientes.

Optimización de Precios

El *pricing automation* o, en español, la automatización de precios es un sistema de fijación de precios que se sirve de tecnología avanzada para, teniendo en cuenta variables como la demanda, los costes operativos o las preferencias del consumidor, establecer precios y cambios de precios que maximicen los beneficios y satisfagan las expectativas de los clientes.

La implementación de sistemas automatizados de precios permite a las empresas que los utilizan calcular el precio óptimo de venta de forma mucho más precisa que mediante los procesos manuales y adaptar sus estrategias de precios a diferentes segmentos de mercado de forma automática

Trazabilidad Inteligente

La trazabilidad en el contexto de la IA y el aprendizaje automático se refiere a la capacidad de seguir el proceso de entrenamiento de un modelo y rastrear su desempeño y resultados en diferentes etapas del proceso.

La trazabilidad es importante en el aprendizaje automático porque permite a los desarrolladores y usuarios del modelo comprender cómo se ha creado el modelo, qué datos se han utilizado para entrenarlo, qué técnicas de preprocesamiento se han aplicado a los datos, qué algoritmos de aprendizaje automático se han utilizado y cómo se ha evaluado su desempeño.

Predicción de Tendencias

La predicción de tendencias (*trend forecasting*) trata esencialmente en encontrar patrones en nuestro presente para predecir el futuro. Funciona en muchos mercados y hay compañías especializadas en crear reportes sobre lo que vaya a pasar hasta 10 años hacia al futuro. Hay macrotendencias, que se pueden predecir con 2 o 3 años de antelación y

que pueden perdurar hasta por décadas. Están las micro-tendencias que ascienden de forma rápida y son efímeras, durando de uno a dos meses.

4. Inteligencia artificial y sesgos

Sesgo Algorítmico

El sesgo algorítmico tiene lugar cuando los errores sistemáticos en los algoritmos de *machine learning* producen resultados injustos o discriminatorios, y a menudo refleja o refuerza los sesgos socioeconómicos, raciales y de género existentes, siendo inherente a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos o generados cuando los sistemas de despliegan en entornos del mundo real

Sesgo de Datos

El sesgo de datos se produce cuando los sesgos presentes en los conjuntos de datos de entrenamiento y ajuste de los modelos de IA afectan negativamente al comportamiento del modelo, teniendo como resultado una repercusión grave en los derechos fundamentales o dando lugar a algún tipo de discriminación prohibida.

Sesgo de Automatización

El sesgo de automatización se produce cuando las personas confían demasiado en los sistemas automatizados, lo que genera resultados injustos. Los algoritmos sesgados pueden amplificar la discriminación en la contratación, la atención médica y más, perpetuando la desigualdad. Para abordar estos problemas se necesitan datos diversos, transparencia y prácticas éticas.

Equidad Algorítmica

La equidad algorítmica se refiere al diseño y desarrollo de sistemas de IA incluyendo aquellos de aprendizaje automático (ML) que operen de manera justa, equitativa y que no provoquen discriminación. La equidad en este contexto se define como la ausencia de sesgos, que en el campo de la toma de decisiones se define como "cualquier prejuicio o favoritismo hacia un individuo o grupo basado en sus características inherentes o adquiridas", teniendo en cuenta lo establecido en los principios del AI Act y a la Carta de Derechos Fundamentales de la UE.

Auditoría Algorítmica

La auditoría algorítmica se refiere al proceso de evaluar la funcionalidad de las aplicaciones de aprendizaje automático, incluyendo el contexto y propósito de la máquina para evaluar su utilidad y equidad. Estas auditorías ayudan a entender sistemáticamente el surgimiento de sesgos en cada paso del proceso de construcción de modelos. Por ejemplo, la Comisión Australiana de Competencia y Consumo (ACCC) realizó una

auditoría de un motor de búsqueda de hoteles popular, donde encontró que el algoritmo favorecía injustamente a los hoteles que pagaban comisiones más altas en su sistema de clasificación. La Corte Federal ordenó a la empresa pagar sanciones por representaciones engañosas sobre las tarifas de habitaciones de hotel en su sitio web y en publicidad televisiva, destacando la importancia de auditar algoritmos para revelar la lógica que impulsa los resultados de las aplicaciones basadas en IA. Concepto relacionado con el artículo 64 del Reglamento (UE) 2024/1689 (AI Act), referente a las obligaciones de supervisión.

Explicabilidad

La explicabilidad se refiere a la capacidad de un modelo de aprendizaje automático para ser entendido y explicado de manera clara y comprensible por los humanos. La explicabilidad es importante porque muchos modelos de aprendizaje automático son muy complejos y difíciles de interpretar, lo que puede dificultar la comprensión de cómo se llega a las decisiones o predicciones que se hacen. Concepto relacionado con artículo 86 AI Act, el artículo 22 RGPD y STJUE C-203/22 (Dun & Bradstreet).

La explicabilidad es particularmente importante en aplicaciones críticas en las que es necesario comprender cómo se toman las decisiones, como la detección de fraudes o la toma de decisiones médicas. Los modelos de aprendizaje automático que son altamente explicables permiten a los expertos en la materia comprender cómo se toman las decisiones y explicarlas a los demás de una manera comprensible.

Transparencia

La transparencia de IA ayuda a las personas a acceder a la información para comprender mejor cómo se creó un sistema de inteligencia artificial y cómo toma decisiones. Los investigadores suelen describir la IA inteligencia artificial como una “caja negra”, ya que aún puede ser difícil explicar, gestionar y regular los resultados de la IA debido a la creciente complejidad de la tecnología. La transparencia de la IA ayuda a abrir esta caja negra para comprender mejor los resultados de la IA y cómo los modelos toman decisiones.

Sesgo de Selección

El sesgo de selección es el error en la elección de los individuos o grupos que participan en un estudio. Lo ideal sería que los sujetos de un estudio fuesen muy similares entre sí y a la población general de la cual se seleccionan (por ejemplo, todos los individuos con la misma enfermedad o afección). Si hay diferencias importantes, los resultados del estudio pueden no ser válidos.

Sesgo de Confirmación

Está estrechamente relacionado con el sesgo cognitivo humano y el sesgo algorítmico, teniendo lugar cuando la IA se basa demasiado en creencias o tendencias preexistentes en

los datos, duplicando los sesgos existentes e incapaz de identificar nuevos patrones o tendencias.

Mitigación de Sesgos

La mitigación de sesgos es un proceso que busca prevenir y reducir las influencias inconscientes y automáticas que afectan el juicio y la toma de decisiones, distorsionando los resultados. Esto se logra mediante la identificación y corrección de prejuicios personales, culturales o sistemáticos en diversas áreas como la investigación, el desarrollo de la inteligencia artificial o la gestión de negocios, para así lograr decisiones más justas, precisas y equitativas.

Sesgo de Etiquetado

El sesgo de etiquetado tiene lugar cuando las etiquetas que se asignan a los datos de entrenamiento se basan en juicios subjetivos o son aplicadas de forma inconsistente.

IA Responsable

La Inteligencia Artificial Responsable representa un enfoque ético y consciente en el desarrollo y aplicación de tecnologías de inteligencia artificial. Este concepto no solo abarca la eficiencia tecnológica, sino también un compromiso firme con los valores humanos, asegurando que la IA se desarrolle y utilice de manera que respete los derechos humanos y promueva el bien social, todo ello vinculado a las guías de la OCDE y UNESCO sobre ética de IA.

5. Inteligencia artificial en agroalimentación

Agricultura de Precisión

La agricultura de precisión es una estrategia de gestión que recoge, procesa y analiza datos temporales, espaciales e individuales y los combina con otras informaciones para respaldar las decisiones de manejo de acuerdo con la variabilidad estimada, y así mejorar la eficiencia en el uso de recursos, la productividad, la calidad, la rentabilidad y la sostenibilidad de la producción agrícola.

Modelos Predictivos de Cosecha

Los modelos de predicción brindan al empresario agrícola herramientas capaces de leer y procesar datos ambientales (condiciones climáticas, características y aspectos específicos de los cultivos). De esta manera, se obtiene información cuantitativa temprana sobre las condiciones de los cultivos para implementar intervenciones eficaces, eficientes y focalizadas.

Teledetección Inteligente

La teledetección con drones está revolucionando la agricultura moderna, permitiendo una gestión más eficiente, sostenible y rentable de los cultivos. Al aprovechar las ventajas de

esta tecnología innovadora, los agricultores pueden optimizar sus operaciones, aumentar la productividad y contribuir a un uso más responsable de los recursos naturales.

Ganadería Inteligente

La ganadería inteligente es la producción ganadera altamente controlada, precisa y optimizada**.** Facilita una utilización más eficiente de los recursos; un mejor rendimiento, manteniendo el bienestar animal y un impacto ambiental reducido.

Tiene una relación muy estrecha con la ganadería de precisión, ya que se encarga de capturar datos e interpretarlos, usando herramientas informáticas para hacer que las operaciones sean más predecibles y competentes.

Trazabilidad Alimentaria

La trazabilidad alimentaria consiste en rastrear y controlar el paso de los alimentos a lo largo del recorrido que siguen en cuanto a producción, distribución y venta se refiere. Básicamente, la idea es recoger información desde la recogida de la materia prima hasta que los alimentos llegan al consumidor final.

Robótica Agrícola

El objetivo de la robótica agrícola es ayudar al sector en su eficiencia y en la rentabilidad de los procesos. Es decir, la robótica móvil trabaja en el sector agrícola para mejorar la productividad, la especialización y la sostenibilidad medioambiental.

La escasez de mano de obra, mayor exigencia de los consumidores o altos costes de producción son algunos de los factores que han acelerado la automatización de este sector, con el objetivo de reducir costes y optimizar las cosechas.

Clasificación Automatizada

La clasificación de frutas se refiere a la separación de estas según su calidad, tamaño, peso, madurez, color, defectos, cualidades organolépticas y otros criterios relevantes. La clasificación correcta de las frutas es esencial para agregar valor a la cadena productiva y maximizar el rendimiento económico de los productores. La clasificación es una tarea crítica en la cadena de suministro de frutas, ya que ayuda a garantizar que los productos se vendan a precios justos y que los clientes reciban productos de alta calidad que satisfagan sus necesidades. La clasificación suele ser realizada de manera automática con el uso de máquinas de clasificación, diseñadas para identificar y separar las frutas según sus características.

Seguridad Alimentaria Predictiva

La seguridad alimentaria predictiva utiliza modelos matemáticos y análisis de datos para anticipar y prevenir riesgos, como el crecimiento de microorganismos, antes de que ocurran. Esta estrategia se basa en la microbiología y el mantenimiento predictivos para optimizar los procesos, mejorar la calidad y garantizar que los alimentos sean seguros para el consumo desde la producción hasta la distribución.

Planificación Logística

La planificación logística es un plan de acción consensuado por todas las partes implicadas en el que se establecen los objetivos logísticos de la compañía**.** Abarca desde el aprovisionamiento de materias primas necesarias para la producción del producto hasta la gestión de las entregas de mercancía a los clientes. Por ejemplo, se acuerdan los términos de entrega al cliente final, los muelles de carga que se destinarán a un envío, etc.

Análisis de Sostenibilidad

Un informe de sostenibilidad es un documento elaborado por las empresas para comunicar su desempeño en aspectos ambientales, sociales y de gobernanza (ASG, por sus siglas en español, ESG en inglés).

Este informe permite a las organizaciones evaluar y mostrar de manera transparente su impacto en el entorno, sus prácticas éticas y su responsabilidad social corporativa**.**

Etiquetado Inteligente

El etiquetado inteligente utiliza tecnología avanzada que proporciona más información y funciones que los códigos de barras convencionales.

Entre las etiquetas inteligentes se encuentran los códigos QR, los códigos de barras incrustados y las etiquetas RFID (Identificación por Radio Frecuencia). Los códigos QR (Quick Response) pueden ser leídos por máquinas y tienen la capacidad de almacenar grandes cantidades de información a la que se puede acceder mediante diferentes dispositivos. Estos códigos tienen múltiples aplicaciones, como el seguimiento de productos a lo largo de la cadena de suministro, la identificación de objetos, la creación de experiencias de marketing a través de la redirección a una URL específica, la visualización de un menú y la transmisión de información sobre sostenibilidad, entre muchos otros.

Blockchain Agroalimentario

La blockchain alimentaria es una tecnología que utiliza una base de datos descentralizada e inmutable para registrar cada paso del viaje de un alimento, desde su origen hasta el consumidor final. Este sistema crea un historial transparente y seguro de los productos, permitiendo a los consumidores y a las empresas verificar la procedencia, autenticidad y calidad de los alimentos, lo que ayuda a prevenir fraudes y mejora la seguridad alimentaria.

6. Inteligencia artificial en banca

Scoring Crediticio Inteligente

El scoring crediticio es un sistema informático que es utilizado por las entidades financieras para aprobar o denegar créditos, es decir, es un analista de riesgos. En numerosos casos según la puntuación o la valoración que proporcione este método será

concluyente a la hora de que el crédito o préstamo en cuestión sea concedido por el banco o no.

No obstante, también se da la circunstancia que en algunas entidades financieras sirve como guía, pero la aprobación del sistema no es condición *sine qua non* para que se otorgue la operación.

Asistentes Virtuales Bancarios

Son programas que, a través de IA, aprendizaje automático y tecnología por reconocimiento de voz comprenden consultas específicas o personalizadas basadas en voz y texto de los clientes y dan manejo a estas.

Personalización de Servicios Financieros

La personalización de productos financieros consiste en la adaptación de servicios y soluciones bancarias a las características y necesidades individuales de cada usuario. A través del análisis de datos, la inteligencia artificial (IA) y la automatización, las entidades financieras pueden diseñar productos que se ajusten al comportamiento financiero, el riesgo crediticio, las metas de ahorro y los hábitos de consumo de cada cliente.

Gestión Inteligente de Inversiones

Se conoce como inversión inteligente a la estrategia financiera que implica tomar decisiones informadas y cuidadosamente planificadas para maximizar los rendimientos y minimizar los riesgos. Su importancia es decisiva, dado que te permite aprovechar tus recursos y obtener beneficios a largo plazo.

Banca Predictiva

La analítica predictiva es el uso de datos, algoritmos estadísticos y técnicas de *machine learning* para identificar la probabilidad de resultados futuros basados en datos históricos. El objetivo es llegar más allá de saber lo que ha sucedido para proveer la mejor evaluación de lo que sucederá en el futuro.

Ética Algorítmica Financiera

Un análisis sobre la necesidad de contemplar qué tipo de información se utiliza para nutrir los sistemas de inteligencia artificial que se emplean en la salud, la justicia y las finanzas, entre otros tantos ámbitos. La selección de datos puede replicar sesgos y prejuicios que podrían profundizar desigualdades e injusticias.

7. Inteligencia artificial en formación y empoderamiento ciudadano

Alfabetización Digital

La alfabetización digital es la capacidad de usar, comprender, evaluar y crear información usando tecnologías digitales de forma segura y efectiva. Implica tener habilidades para navegar internet, utilizar dispositivos electrónicos, comunicarse online, identificar

noticias falsas y proteger la privacidad, lo cual es fundamental para participar plenamente en la sociedad actual.

Ciudadanía Digital

La ciudadanía digital puede definirse cómo los patrones de comportamiento que conciernen al uso de la tecnología. Estas normas se organizan en nueve áreas generales de comportamiento que tratan de recoger toda la complejidad del concepto y las implicaciones derivadas del buen y mal uso de la tecnología.

IA Educativa

La IA educativa es el uso de tecnologías de IA, como el aprendizaje automático y el procesamiento del lenguaje natural, para mejorar los procesos de enseñanza y aprendizaje. Permite personalizar la educación adaptando los contenidos a las necesidades de cada estudiante, automatizar tareas repetitivas para los docentes, y ofrecer herramientas como tutores virtuales o sistemas de evaluación automatizada.

Plataformas de Participación Inteligente

Una plataforma de participación inteligente es una solución tecnológica que, mediante herramientas digitales, busca mejorar la conexión entre ciudadanos y administraciones públicas para fortalecer la democracia y la gestión de los asuntos públicos. Estas plataformas permiten a los ciudadanos opinar, proponer ideas, evaluar políticas y participar en procesos decisorios, mientras que las administraciones pueden mejorar la transparencia, la eficiencia y la comunicación bidireccional, promoviendo ciudades más inclusivas y resilientes.

Inclusión Algorítmica

La equidad algorítmica se refiere al diseño y desarrollo de sistemas de IA incluyendo aprendizaje automático, de forma que operen de manera justa, equitativa y que no provoquen discriminación.

Empoderamiento Informacional

El empoderamiento informacional es la capacidad de reconocer las necesidades de información, encontrar y evaluar críticamente la información de diversas fuentes, y utilizarla de manera efectiva para la toma de decisiones y la resolución de problemas. Implica ir más allá del uso básico de herramientas digitales para desarrollar habilidades cognitivas y críticas que permiten a las personas ejercer control sobre sus vidas y participar activamente en una sociedad cada vez más digital.

Simuladores Cívicos

Un simulador cívico es una herramienta computacional que recrea escenarios de la vida real relacionados con la administración pública o la participación ciudadana, para fines de cálculo, planificación, evaluación o formación. Pueden servir para calcular tasas de impuestos, planificar el uso del territorio, predecir el impacto de decisiones de movilidad o simular procesos para formar a los ciudadanos o funcionarios.

Vigilancia Ciudadana Algorítmica

En el ámbito de las Fuerzas y Cuerpos de Seguridad (FCS), como es el caso de la Guardia Civil, la IA tiene el potencial de ser un poderoso instrumento para mejorar la seguridad pública y proteger a la ciudadanía tanto de los actuales y ya conocidos peligros, como de las potenciales tipologías de delincuencia asociadas a las nuevas tecnologías emergentes. Sin embargo, es muy importante que su uso se haga de manera ética y responsable para evitar que se produzcan abusos o violaciones de derechos fundamentales, siendo crucial establecer límites claros y regulaciones efectivas para ello.

8. Inteligencia artificial, conceptos generales

Caja Negra

Se refiere a un fenómeno que ocurre en muchos sistemas de aprendizaje automático o algoritmos de *deep learning* en redes neuronales, cuyos procesos están ocultos o son complejos de ver. A diferencia de los algoritmos tradicionales, que son programados por humanos, y, por tanto, conocidos y comprensibles, estos sistemas aprenden de manera autónoma a través de procesos de entrenamiento que implican ensayo y error, y resulta difícil para los humanos poder 'mirar dentro' y entender el porqué de los resultados que nos ofrece la IA: qué características tuvo en cuenta, cómo se combinan, qué ha priorizado, etc.

Modelos Interpretables

La interpretabilidad de la IA ayuda a las personas a comprender y explicar mejor los procesos de toma de decisiones que impulsan los modelos de inteligencia artificial (IA).

Los modelos de IA utilizan una compleja red de entradas de datos, algoritmos, lógica, ciencia de datos y otros procesos para obtener conocimientos. Cuanto más complejo sea el modelo, más difícil puede ser para los humanos comprender los pasos que condujeron a sus conocimientos, incluso si esos humanos son los que lo diseñaron y construyeron. Un modelo interpretable es aquel cuyas decisiones pueden ser fácilmente entendidas por los usuarios.

Visualización de Decisiones

En la era digital actual, el análisis de datos se ha convertido en un activo invaluable para las empresas que buscan optimizar sus procesos y mejorar su toma de decisiones. La combinación de esta práctica con la inteligencia artificial (IA) ha revolucionado la forma en que se maneja la información y se extraen *insights* significativos.

El análisis de datos implica la recolección, procesamiento e interpretación de grandes volúmenes de información para identificar patrones, tendencias y oportunidades de mejora. Por otro lado, la IA aporta la capacidad de aprender de estos datos, adaptarse y predecir resultados futuros de manera autónoma.

Al unir estas dos disciplinas, las organizaciones pueden obtener una visión más profunda y precisa de su negocio, lo que les permite tomar decisiones más informadas y

estratégicas. La visualización de datos juega un papel crucial en este proceso, ya que permite presentar la información de forma clara y concisa, facilitando la comprensión y la identificación de *insights* relevantes.

Explicaciones Locales

Las explicaciones locales son las técnicas que permiten explicar las predicciones del modelo en un caso específico o en una instancia de datos. Algunos ejemplos son LIME (Explicaciones locales interpretables de modelos) y SHAP (Valores de Shapley).

Consentimiento Informado

El consentimiento informado para la IA es la manifestación libre, voluntaria y consciente de un usuario para permitir que una IA procese sus datos personales, en pleno conocimiento de cómo se usarán esos datos, conociendo los riesgos y beneficios, y la posibilidad de retirar dicho consentimiento. Este proceso busca proteger la autonomía del usuario, garantizar la transparencia y la confianza, y asegurar el respeto a la dignidad y los derechos de las personas frente al uso de tecnologías de IA.

Documentación Técnica Accesible

La documentación técnica accesible es aquella que está diseñada para que todas las personas, incluidas aquellas con discapacidades, puedan comprenderla, navegarla y utilizarla. Esto se logra utilizando un formato estructurado y semántico, como el uso correcto de encabezados jerárquicos, texto alternativo para imágenes, contraste de color adecuado y marcadores para la navegación, para que las tecnologías de asistencia como los lectores de pantalla puedan procesar la información correctamente.

Automatización Robótica de Procesos (RPA)

La RPA combina la interfaz de programación de aplicaciones (API) y las interacciones de la interfaz de usuario (IU) para integrar y realizar tareas repetitivas entre las aplicaciones empresariales y de productividad. Mediante la implementación de guiones que emulan procesos humanos, las herramientas de RPA completan la ejecución autónoma de diversas actividades y transacciones en sistemas de software no relacionados.

Esta forma de automatización utiliza software basado en reglas para realizar actividades de procesos empresariales en un gran volumen, permitiendo que las personas dispongan de más tiempo para dar prioridad a tareas más complejas. La RPA permite a los directores de sistemas de información y a otros responsables de la toma de decisiones acelerar sus esfuerzos de transformación digital y generar un mayor retorno de la inversión (ROI) de su personal.

Reconocimiento Biométrico

Conocido en inglés como AIDC (Automatic Identification and Capture), el sistema de reconocimiento biométrico es un tipo particular de sistema informático que identifica a una persona basándose en una o más características fisiológicas y/o comportamentales. Estas características se comparan con los datos previamente adquiridos y almacenados en

la base de datos del sistema, utilizando algoritmos y sensores que capturan los datos de entrada.

Cumplimiento Normativo Automatizado (RegTech)

El cumplimiento normativo consiste en asegurar que todas las operaciones y procesos de una empresa se ajusten a las leyes, regulaciones y políticas internas vigentes. De esta manera se minimizan los riesgos legales, se evitan sanciones y se garantiza la confianza de los clientes y socios comerciales.

Optimización de Tesorería

La optimización de tesorería es el proceso de gestionar eficazmente los recursos financieros de una empresa para maximizar su liquidez y minimizar los riesgos. Se trata de asegurar que el dinero esté en el lugar correcto, en el momento adecuado.

Optimización de Riesgo

La optimización del riesgo es el proceso de entender tanto las oportunidades como las amenazas que enfrenta una organización, con el fin de diseñar una estrategia para asumir el riesgo adecuado que permita el crecimiento. Implica un enfoque sistemático para identificar, evaluar, mitigar y monitorear riesgos con el objetivo de minimizar sus consecuencias negativas y maximizar sus impactos positivos, asegurando que se haga de manera eficiente y rentable.

9. Inteligencia artificial y riesgos

Riesgo de Privacidad

Al publicar o facilitar información a través de los distintos servicios online sobre quiénes somos, vivimos, trabajamos, hobbies, gustos, intereses, fotos, vídeos, etc., ponemos en riesgo nuestra privacidad e incrementamos las opciones de ser víctimas de algún tipo de fraude o sufrir las consecuencias negativas de esa exposición, ya sea por daños reputacionales u otros. Los principales riesgos son (i) robo y suplantación de identidad**:** los delincuentes pueden utilizar la información publicada en Internet para robar y suplantar la identidad de una persona y hacer compras fraudulentas, abrir cuentas bancarias, obtener un crédito u otras acciones maliciosas en su nombre; (ii**)** vigilancia**:** las empresas, los ciberdelincuente y resto de usuarios pueden utilizar la información disponible en Internet para usarla en su beneficio; (iii) extorsión**:** los usuarios con malas intenciones pueden usar la información personal de las personas disponible en la Red para hostigarlas, amenazarlas y difamarlas en las redes sociales u otros canales web; (iv) discriminación**:** cualquier persona con acceso a la información publicada puede aprovecharla para discriminar a las personas en función de su género, raza, orientación sexual, ideología, condición física, estatus económico, etc. ; (v) sexting**:** la distribución de fotos y vídeos producidos por uno mismo con connotación sexual, puede suponer una práctica de riesgo ya que la persona que lo recibe podría comprometer tu privacidad si lo redifunde sin tu consentimiento, o no toma las medidas de seguridad adecuadas para salvaguardarla; (vi) doxing**:** publicación de información sobre ti en Internet sin tu

consentimiento; (vii) fraudes y amenazas**:** los ciberdelincuentes pueden enviar mensajes manipulados y personalizados a sus víctimas, teniendo en consideración la información recopilada sobre ellas en Internet, resultando mucho más creíbles, de tal forma que las probabilidades de caer en el engaño sean más altas.

Desinformación Automatizada

La desinformación automatizada es información falsa o engañosa que se difunde de manera intencional y con el objetivo de manipular o engañar a la audiencia. Se trata de un rumor o noticia sin fundamento que se propaga rápidamente a través de las redes sociales y los medios de comunicación.

Dependencia Tecnológica

La dependencia tecnológica o adicción a la tecnología se refiere al comportamiento compulsivo y constante de usar dispositivos tecnológicos de manera que interfiere con las actividades diarias y las relaciones interpersonales. Esta dependencia no solo se limita a las redes sociales o a los videojuegos, sino que abarca cualquier forma de tecnología que involucre la interacción continua con dispositivos electrónicos.

Exclusión Digital

La exclusión digital es la falta de acceso y/o capacidad para utilizar las tecnologías digitales, lo que genera desigualdades y limita la participación plena en la sociedad actual. Se manifiesta en la falta de acceso físico a dispositivos e internet (brecha de acceso), en la falta de habilidades para usarlos (brecha de uso), y en las diferencias en la calidad de la experiencia digital, excluyendo a personas de servicios públicos, oportunidades laborales y actividades sociales.

Opacidad Algorítmica

La opacidad algorítmica es la falta de transparencia en el funcionamiento de un sistema algorítmico, donde no es posible entender cómo llega a sus conclusiones. Esto ocurre a menudo con modelos de inteligencia artificial complejos, conocidos como "cajas negras". La opacidad dificulta la detección de sesgos y la atribución de responsabilidad por decisiones erróneas.

Autonomía No Controlada

La autonomía no controlada se refiere a la falta de control respecto a los niveles de autonomía que ha desarrollado la misma, que plantea importantes dilemas éticos y prácticos. A medida que las IA se vuelven más avanzadas, pueden analizar datos y ejecutar acciones sin intervención humana. Este nivel de autonomía plantea preguntas sobre la seguridad, la ética y la responsabilidad. Ejemplo: Las IA utilizadas en vehículos autónomos deben tomar decisiones en fracciones de segundo para evitar accidentes. La autonomía permite que estos sistemas reaccionen más rápido que los humanos, pero también plantea riesgos si las decisiones no son las correctas.

Sobrecarga Informativa

La sobrecarga informativa es el fenómeno que sufren algunas personas cuando sienten que la información a la que están expuestas es superior a la que pueden asimilar**.** También es conocida por el **té**rmino "infoxicación", que es un neologismo en el que se combinan las palabras "información" e "intoxicación". Este tiene su origen en el concepto *"information overload"*, acuñado en 1970 por el sociólogo Alvin Toffler. Antes de la popularización de Internet, la información era filtrada y contrastada por profesionales que, a su vez, la transmitían a la población. Sin embargo, a medida que aumenta la facilidad de acceso a la información, también lo hace el número de fuentes.

El problema no está realmente en el acceso a la información, sino en que basamos nuestras decisiones en la información que recibimos. Y si no hemos sido capaces de contrastarla, o directamente no es correcta, esto repercutirá en nuestro día a día. Además, la infoxicación o sobrecarga informativa también puede producir efectos psicológicos adversos como estrés y ansiedad.

FRIA

La FRIA, o Evaluación de Impacto de Derechos Fundamentales, es un requisito establecido por el Reglamento de Inteligencia Artificial (RIA) de la Unión Europea. Su objetivo es identificar, analizar y mitigar los posibles efectos negativos que el uso de sistemas de IA puede tener sobre los derechos fundamentales, como el derecho a la no discriminación, la libertad de expresión y la protección de datos personales.

Dark patterns

Los dark patterns son técnicas de diseño engañosas utilizadas en interfaces de usuario para manipular las decisiones del usuario, a menudo en beneficio de la empresa. Estas técnicas pueden incluir la ocultación de información crucial, la presión para realizar acciones no deseadas, y la creación de un entorno que dificulta la toma de decisiones informadas.

CAPÍTULO I. INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE LAS PERSONAS CONSUMIDORAS EN CASTILLA-LA MANCHA

1. La transformación estructural del mercado de consumo digital

La irrupción de la IA en los mercados de bienes y servicios ha producido una transformación profunda. Las personas consumidoras ya no interactúan únicamente con comercios tradicionales, sino con arquitecturas digitales automatizadas que condicionan, orientan o incluso determinan sus decisiones mediante técnicas de predicción, clasificación, segmentación y personalización comercial.

Esta realidad genera una asimetría tecnológica creciente, derivada de tres vectores esenciales:

1. Opacidad algorítmica: los modelos de IA operan mediante procesos internos no accesibles, dificultando la comprensión de la lógica decisoria por parte del consumidor y, en ocasiones, incluso por el propio operador.

2. Dependencia económica y funcional de las plataformas: la concentración del poder computacional y del acceso masivo a datos (first-party y third-party data)[1] sitúa al consumidor en posición estructural de inferioridad.
3. Automatización de decisiones con efectos jurídicos o similares: denegación de crédito, fijación dinámica de precios, despriorización de resultados o limitación del acceso a la atención humana.

El resultado es una vulnerabilidad digital cualitativamente distinta a la tradicional, que exige respuestas regulatorias y de supervisión pública específicas.

1.1. Nuevas dinámicas de riesgo

El análisis doctrinal y jurisprudencial reciente evidencia que los principales riesgos para los consumidores en entornos algorítmicos son:

- Pérdida de autonomía decisoria, favorecida por patrones oscuros[2] (dark patterns), hiperpersonalización no informada o manipulación del diseño.
- Discriminación algorítmica —directa o indirecta— derivada de variables correlacionadas con edad, localización, ingresos o características socioculturales.
- Desventaja estructural frente a proveedores digitales, que controlan los datos, las arquitecturas de elección y los procesos de toma de decisiones automatizados.
- Restricción de derechos: chatbots que impiden el acceso a personal humano; sistemas de reclamación automatizados sin posibilidad real de intervención humana; información precontractual insuficiente (artículo 60 TRLGDCU).
- Riesgos para la privacidad: decisiones basadas en grandes volúmenes de datos, a menudo sin información significativa conforme a los artículos 13–15 RGPD.

1.2. Sectores más afectados

Los efectos de la IA son especialmente intensos en:

- Información precontractual: personalización sin transparencia suficiente (artículos 60 y ss. TRLGDCU).

Fijación de precios: precios dinámicos o personalizados sin indicación de parámetros, prohibidos cuando se basan en discriminación ilícita o explotación de vulnerabilidad (PLAC).

- Servicios digitales: motores de recomendación, marketplaces y plataformas de intermediación.

[1] "First-party data" se refiere a la información que una empresa recopila directamente de sus clientes; mientras que "third-party data" se refiere a la información recopilada por entidades externas, como pueden ser proveedores de marketing o plataformas de rastreo.
[2] En este sentido, véase lo establecido en la Directiva 2005/29/CE y el artículo 25 RGPD (privacidad desde el diseño).

- Atención al cliente: proliferación de chatbots que limitan la intervención humana real y gratuita (Directiva (UE) 2023/2673[3], artículo 16 quinquies).
- Publicidad: segmentación automatizada, microtargeting y generación sintética de contenidos (deepfakes, reseñas generadas por IA).
- Servicios financieros y crédito al consumo: scoring automatizado conforme a la doctrina del TJUE, asunto C-634/21, SCHUFA"[4].

La entrada masiva de estas tecnologías justifica una respuesta sistemática, institucional y coordinada desde la administración de consumo autonómica.

2. Un marco jurídico multinivel especialmente complejo

El marco jurídico aplicable a la IA en el consumo es multinivel y combina normas de la UE, legislación estatal y competencias autonómicas. Su comprensión integrada es esencial para definir líneas de actuación públicas sólidas.

2.1. Derecho de la Unión Europea

a) Reglamento (UE) 2016/679 — RGPD

- **Decisiones automatizadas (art. 22):**
  - Prohíbe someter al interesado a decisiones "exclusivamente" automatizadas con efectos jurídicos o similares, salvo excepciones (contrato necesario, autorización legal, consentimiento explícito).
  - Exige **garantías reforzadas**: intervención humana, posibilidad de expresar el punto de vista y de impugnar la decisión.
- **Transparencia y acceso (arts. 13–15):**
  - Debe proporcionarse **información significativa** sobre la lógica aplicada, la importancia y las consecuencias previstas del tratamiento.

[3] Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023, por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia y se deroga la Directiva 2002/65/CE. DOUE núm. 2673, de 28 de noviembre de 2023.

[4] En el ámbito del crédito al consumo, muchas entidades financieras emplean sistemas de scoring automatizado para evaluar la solvencia del consumidor y decidir si conceden financiación. El TJUE, en el asunto C-634/21 (*SCHUFA*), ha establecido que estos sistemas constituyen una decisión automatizada con efectos jurídicos o similares, en el sentido del artículo 22 RGPD, cuando el resultado del scoring determina de manera decisiva la posibilidad de obtener crédito.
Ello implica que la entidad no puede basarse únicamente en algoritmos opacos: debe garantizar derechos reforzados para el consumidor, como la transparencia en la lógica aplicada, la posibilidad de intervención humana real y significativa, y mecanismos para impugnar la decisión. Además, solo puede utilizar datos adecuados, pertinentes y no excesivos, evitando perfiles que deriven de información desproporcionada o no verificada.
Esta doctrina incide directamente en los servicios financieros, imponiendo un estándar más estricto de explicabilidad y control humano en la evaluación automatizada de riesgos, así como mayores garantías frente a decisiones injustas o discriminatorias.

- La "información significativa" no es divulgación del código fuente: es una explicación comprensible de variables, criterios y su peso en el resultado.

- **Evaluación de impacto (art. 35):**
  - Obligatorias cuando exista **alto riesgo** para derechos y libertades, incluidos tratamientos que impliquen perfiles extensivos, uso de **sistemas de IA** en decisiones con efectos relevantes, o monitorización sistemática.
  - Deben documentar medidas de mitigación, supervisión humana y pruebas de robustez.
- **Protección de datos desde el diseño (art. 25):**
  - Impone **privacy by design/by default**: minimización, control de acceso, trazabilidad, separación de funciones (entrenamiento vs. inferencia) y configuraciones por defecto respetuosas.
  - En IA, se traduce en gobernanza de datos de entrenamiento, control de sesgos y auditabilidad.
- **Jurisprudencia TJUE (credit scoring):**
  - El **scoring crediticio** que determina la concesión/denegación de crédito se considera **decisión automatizada** con efectos jurídicos, lo que desencadena las garantías del art. 22 y exige **supervisión humana real y efectiva** (no meramente nominal).

b) Directiva 2005/29/CE — Prácticas comerciales desleales (UCPD)

- **Omisiones engañosas sobre lógica algorítmica:**
  - Ocultar criterios relevantes del algoritmo o su impacto en precio, visibilidad o recomendación puede ser omisión engañosa si altera la decisión del consumidor medio.
- **Manipulación del diseño (dark patterns):**
  - Patrones que empujan a suscripciones, compras o cesiones de datos sin consentimiento informado pueden ser prácticas desleales.
  - El régimen se vio reforzado por la reforma "Omnibus" (Directiva (UE) 2019/2161) con obligaciones de transparencia en mercados en línea, reseñas y personalización de precios.
- **Publicidad encubierta/generated by IA:**
  - La **publicidad generada por IA** debe **identificarse claramente** como tal y evitar atribuir origen humano cuando no exista, para no inducir a error.
  - Reseñas/valoraciones sintéticas que aparentan ser de consumidores reales constituyen práctica engañosa.

c) Directiva (UE) 2019/770 — Contenidos y servicios digitales

- **Falta de conformidad en software/servicios de IA:**
  - Responde por funcionalidades prometidas, rendimiento razonable, **seguridad** y compatibilidad.

- La **IA embebida** en apps/servicios debe cumplir expectativas contractuales y legales.

- **Actualizaciones y seguridad:**
  - Obligación de proporcionar **actualizaciones** (incluidas de seguridad) durante el periodo razonable, evitando degradación funcional o riesgos emergentes.
  - Cambios sustantivos impulsados por IA (p. ej., nuevos modelos) que alteren características esenciales requieren transparencia y, en su caso, consentimiento.

d) Reglamento (UE) 2024/1689 — AI Act

- **Clasificación por niveles de riesgo:**
  - Prohibidos, alto riesgo, riesgo limitado y mínimo, con obligaciones graduadas.
- **Alto riesgo — obligaciones estrictas:**
  - **Documentación técnica**, gestión del ciclo de vida, **gobernanza de datos** (calidad, pertinencia, ausencia de sesgos indebidos), **supervisión humana** efectiva, robustez, precisión y ciberseguridad.
  - Registro y evaluación de conformidad antes de puesta en el mercado.
- **Transparencia en interacción y marcado de contenidos:**
  - Obligaciones de informar cuando el usuario interactúa con IA; **etiquetado de contenidos generados por IA** (incluidos "deepfakes") para no inducir a error.
- **Derecho a explicaciones claras:**
  - Cuando decisiones asistidas por IA impacten derechos fundamentales o intereses esenciales, deben darse **explicaciones inteligibles** del funcionamiento relevante y los factores determinantes.
- **Prohibiciones (art. 5):**
  - Prácticas como **manipulación subliminal**, **explotación de vulnerabilidades**, **puntajes sociales** por autoridades públicas, y ciertos usos de **identificación biométrica remota** (salvo supuestos tasados).
- **GPAI y modelos fundacionales:**
  - Requisitos de transparencia, gestión de riesgos y reporte para modelos de propósito general, especialmente los de **impacto sistémico**.

e) Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo.

Revisión de la Directiva 85/374/CEE:

- La nueva directiva **incluye el software y los sistemas de IA** como "productos", clarificando la **responsabilidad objetiva** por defectos que causen daños.
- Prevén ajustes en carga de la prueba, acceso a evidencias (disclosure) y presunciones en casos de complejidad técnica.

- **Coherencia con el AI Act y el marco de seguridad de productos:**
  - Debe coordinarse con el **Reglamento (UE) 2023/988 — Seguridad general de los productos (GPSR)**, que exige que productos con componentes digitales/IA cumplan requisitos de seguridad, trazabilidad y retirada eficaz.

f) Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023, por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia y se deroga la Directiva 2002/65/CE.

- **Intervención humana real, gratuita e inmediata (art. 16 quinquies):**
  - Derecho del consumidor a **ser atendido por una persona** cuando una decisión se adopte mediante interfaces automatizadas.
  - Impide **cajones de sastre** donde el consumidor queda atrapado en flujos automáticos sin salida humana; exige **canales efectivos** y sin coste.
- **Transparencia reforzada y desistimiento:**
  - Información clara sobre funcionalidades automatizadas, riesgos y vías de reclamación, con **protección adicional** en contratos celebrados a distancia.

g) Reglamento (UE) 2022/2065 — Ley de Servicios Digitales (DSA)

- **Transparencia de sistemas de recomendación:**
  - Debe informarse de los **parámetros principales** y ofrecer opciones significativas (p. ej., ordenación no basada en perfilado).
- **Publicidad y reseñas:**
  - **Identificación clara** del contenido publicitario y del **proveedor**; controles contra **reseñas falsas** y contra contenidos manipulados por IA que induzcan a error.
- **Prohibición de dark patterns:**
  - Prohíbe **patrones de diseño engañosos** que distorsionan la elección del usuario (relevante para interfaces con IA).
- **Obligaciones agravadas para VLOPs/VLOSEs:**
  - Evaluación y mitigación de **riesgos sistémicos** (incluidos los derivados de IA generativa), acceso a datos para supervisión y auditorías independientes.

h) Reglamento (UE) 2022/1925 — Ley de Mercados Digitales (DMA)

- **Gatekeepers y auto-preferencia algorítmica:**
  - Restringe prácticas de **auto-preferencia** y uso cruzado de datos que afecten la visibilidad y elección del consumidor en servicios dominados por algoritmos.
- **Interoperabilidad y portabilidad:**
  - Facilita **portabilidad** y **acceso** a datos, promoviendo competencia efectiva y reduciendo **lock-in** inducido por IA.

i) Reglamento (UE) 2023/2854 — Ley de Datos (Data Act)

- **Acceso y uso de datos de dispositivos/servicios:**
  - Derechos de **acceso** para usuarios a datos generados por el uso, incluidos los requeridos para entrenar o mejorar IA, con salvaguardas.
  - Prohíbe cláusulas abusivas en contratos B2B que limiten indebidamente el uso de datos.
- **Switching cloud e interoperabilidad:**
  - Facilita **cambio de proveedor** y neutraliza bloqueos técnicos que afectan servicios con IA.

k) Reglamento (UE) 2022/868 — Ley de Gobernanza de Datos (DGA)

- **Intermediación de datos y altruismo de datos:**
  - Establece condiciones para **intermediarios** y esquemas de **altruismo** que pueden alimentar sistemas de IA con datos de alta calidad y con garantías.

l) Reglamento (UE) 2023/988 — Seguridad general de los productos (GPSR)

- **Productos con componentes de IA:**
  - Requisitos de **seguridad**, información de riesgos, trazabilidad y retirada/corrección rápida cuando se detecten fallos de **software/IA**.

n) Directiva 2011/83/UE — Derechos de los consumidores (reformada por 2019/2161)

- **Mercados en línea y personalización de precio:**
  - Obliga a informar cuando el precio se **personaliza** usando algoritmos; exige claridad sobre quién es el **vendedor** y sus responsabilidades.
- **Reseñas y verificaciones:**
  - Debe indicarse si el comerciante **verifica** que las reseñas provienen de consumidores reales.

n) Reglamento (UE) 2018/302 — Geoblocking

- **No discriminación injustificada:**
  - Limita prácticas algorítmicas que **segmentan** mercados de forma discriminatoria sin base legal.

2.2. Derecho nacional y autonómico

a) Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU)

Especial relevancia de:

- información precontractual (artículos 60 y ss.),
- prácticas desleales,
- transparencia en precios personalizados (artículos 20 y 97 y reforma proyectada),
- obligaciones de los marketplaces respecto a parámetros de clasificación (artículo 20 y 97 bis).
- Artículo 82: cláusulas abusivas.

b) Ley 3/2019, de Estatuto de las Personas Consumidoras de Castilla-La Mancha

Establece competencias autonómicas en:

- educación y formación,
- inspección,
- información y empoderamiento,
- adopción de medidas preventivas y correctoras.
- Habilita a la Junta Arbitral de Consumo como mecanismo de resolución.

c) Normativa sectorial adicional

- ***Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI-CE)***
  - Artículo destacado: art. 20 sobre comunicaciones comerciales por vía electrónica, que exige identificación clara y prohíbe el envío de comunicaciones no solicitadas sin consentimiento previo.
- ***Ley 34/1988, de 11 de noviembre, General de Publicidad***
  - Regula la publicidad ilícita, engañosa, subliminal y comparativa, así como la acción de cesación.
- ***Ley 3/1991, de 10 de enero, de Competencia Desleal***
  - Regula actos de engaño, confusión, omisión, prácticas agresivas y explotación de la reputación ajena.
- ***Ley 13/2011, de 27 de mayo, de regulación del juego***
  - Establece el marco regulador de los juegos de ámbito estatal, licencias, autorizaciones y régimen sancionador.

d) Referencia comparada: Anteproyecto de Ley de Salud Digital de Cantabria

Este texto autonómico ofrece una arquitectura de gobernanza extrapolable a consumo:

- Autoridad autonómica técnico-jurídica.
- Registros autonómicos interoperables.
- Sandboxes reguladores.
- Protocolos de auditoría y supervisión.

La experiencia comparada demuestra que las CCAA pueden asumir funciones proactivas sólidas en materia de IA.

3. Jurisprudencia esencial para la supervisión de la IA en consumo

3.1. Tribunal Supremo (España)

- STS 241/2013[5] (cláusulas suelo, referente a comprensibilidad contractual): fija el deber de comprensibilidad real y efectiva; aplicable por analogía a decisiones algorítmicas opacas.
- STS 272/2019[6]: refuerza el control sobre publicidad engañosa y veracidad publicitaria; aplicable a contenidos generados por IA.

3.2. Tribunal de Justicia de la Unión Europea

- C-634/21, SCHUFA: establece que el scoring automatizado es una decisión automatizada (artículo 22 RGPD).
- C-203/22, Dun & Bradstreet (2025, pendiente de consolidación doctrinal): el responsable debe ofrecer explicaciones claras, accesibles y con ejemplos; no es admisible invocar secreto comercial para eludir transparencia.
- C-180/96 (Doctrina del principio de precaución, se aplica en materia de salud y medioambiente): habilita auditorías y suspensiones preventivas frente a riesgos graves, aplicable a sistemas algorítmicos.

Esta jurisprudencia sustenta la actuación inspectora autonómica.

4. Modos de actuación de la IA en el mercado de consumo: tipología, efectos y obligaciones

Cuadro sintético corregido

[5] STS (1ª), de lo Civil, Sección Pleno, núm. 241/2013, de 9 de mayo de 2013, rec. 485/2012.
[6] STS (1ª) de lo Civil, núm. 272/2019, de 17 de mayo de 2019, rec. 3899/2016.

Uso de IA	Impacto sobre el consumidor	Normativa aplicable	Evidencia mínima exigible al operador
Motores de recomendación	Alteración de visibilidad y preferencias	RGPD: arts. 13.2.f, 14.2.g, 15.1.h, 22. DSA: arts. 26–28 (parámetros principales de recomendación y transparencia publicitaria). LCD/Dir. 2005/29/CE (omisiones engañosas)	**Logs de ranking:** criterios, pesos y cambios de modelo. Parámetros principales: explicación accesible. Trazabilidad: versiones y auditorías internas
Precios dinámicos / personalizados	Precio distinto para producto idéntico	TRLGDCU: art. 20.1.c (transparencia en personalización de precio; modificado por Omnibus y RDL 8/2024 DF 1ª), arts. 97.1.f y 20.3. Reglamento (UE) 2018/302 (geoblocking): art. 4. LCD/Dir. 2005/29/CE	Historial de precios: por segmento y periodo. Criterios de segmentación: variables utilizadas y justificación. Aviso claro de personalización en el punto de venta
Scoring automatizado	Denegación o encarecimiento de crédito	RGPD: arts. 13.2.f, 14.2.g, 15.1.h, 22, 82. AI Act: Anexo III (crédito como sistema de alto riesgo), arts. 14 (supervisión humana) y 86 (explicaciones). Jurisprudencia TJUE (SCHUFA)	Variables empleadas: lista y relevancia. Explicación comprensible: razones determinantes del resultado. Registro de revisión humana: capacidad real de modificar decisiones
Publicidad algorítmica a menores	Captación predatoria	DSA: art. 28 (prohibición de publicidad basada en perfilado a menores), arts. 26–27 (identificación de publicidad). LGCA: art. 90 y ss. LSSI: art. 20 (comunicaciones comerciales identificadas). LCD/Dir. 2005/29/CE (lista negra: reseñas falsas, engaño)	Pruebas de edad: mecanismos razonables de verificación. Segmentación: evidencias de exclusión de menores. Etiquetado de publicidad y proveedor
Chatbots de atención	Bloqueo del derecho a atención humana	Directiva (UE) 2023/2673: art. 16 quinquies (derecho a intervención humana en contratos a distancia). TRLGDCU: art. 21 (derecho a atención personalizada y eficaz). DSA: art. 12 y 20.6	Registros de escalado: tiempos y resolución. Porcentaje de casos atendidos por humanos. Puntos de salida humana visibles y sin coste

Uso de IA	Impacto sobre el consumidor	Normativa aplicable	Evidencia mínima exigible al operador
		(contacto accesible y reclamaciones). RGPD: art. 22 (decisiones automatizadas)	
Deepfakes y reseñas generadas	Inducción a error	AI Act: obligaciones de marcado de contenidos generados por IA (transparencia). DSA: arts. 26–27 (identificación publicitaria) y controles de reseñas falsas. Ley 34/1988 (LGP) y LCD (3/1991) para publicidad ilícita y engañosa	Sistemas de verificación: procedencia de reseñas y autenticidad. Marcado de IA: señalización visible en contenidos sintéticos. Logs de moderación y retirada

5. Riesgos específicos y estructurales en Castilla-La Mancha

El análisis territorial revela factores diferenciales:

1. Pymes intensamente dependientes de soluciones SaaS, sin capacidad de auditar modelos. En este sentido, destaca la Estrategia Digital de Castilla-La Mancha (2025)
2. Brecha digital rural, que incrementa la vulnerabilidad frente a manipulación digital o discriminación por ubicación.
3. Alta proporción de población envejecida, especialmente susceptible a prácticas opacas o automatizadas.
4. Sectores clave regionales:
    - agroalimentario: necesidad de trazabilidad y gobernanza de datos;
    - turismo: uso generalizado de precios dinámicos (destaca Directiva 2019/2161 en relación con la transparencia en los precios personalizados) con impacto en colectivos vulnerables.

Estos elementos justifican una respuesta autonómica específica, dentro de sus competencias.

6. Hacia un sistema autonómico de alerta temprana y supervisión algorítmica

Para las OMIC y la inspección regional se propone un sistema de triaje, basado en preguntas guía:

- ¿La decisión es automatizada o lo parece (denegación, variación de precio, priorización)?
- ¿Existen opacidades sobre los parámetros?
- ¿Indicios de discriminación por edad, ingresos o ubicación?
- ¿La interacción se realiza exclusivamente mediante chatbot?
- ¿El contenido parece sintético o manipulado mediante IA generativa?
- ¿Se ha negado el derecho a intervención humana (artículo 16 quinquies Directiva 2023/2673)?
- ¿Se han utilizado datos sin información suficiente o sin base jurídica válida?

Una respuesta afirmativa obliga a escalar el caso a la Unidad Técnica de IA (UTIA) conforme a los criterios desarrollados en capítulos posteriores. Es importante mantener una coordinación periódica con la AESIA (en base al Real Decreto 729/2023). Por último, deben remitirse informes periódicos al Observatorio Digital Autonómico.

7. Conclusión general del capítulo

Este Capítulo I establece los fundamentos conceptuales, jurídicos y operativos que justifican:

- la intervención pública autonómica,
- la necesidad de mecanismos institucionales propios (unidad técnica, registros, observatorio, protocolos para OMIC),
- y la adopción de metodologías de supervisión coherentes con el RGPD, el AI Act, el DSA, el TRLGDCU y la Ley 3/2019.

A diferencia de los capítulos finales —donde se adopta un formato sintético y ejecutivo—, esta sección ofrece una base doctrinal exhaustiva, necesaria para la comprensión del resto del informe.

CAPÍTULO II. COMPETENCIAS Y MARCO INSTITUCIONAL AUTONÓMICO

I. MARCO COMPETENCIAL: UNIÓN EUROPEA, ESTADO Y CASTILLA-LA MANCHA

1. Objetivo

En este epígrafe se analizan las competencias legislativas de la Unión Europea, el Estado español y la Comunidad Autónoma de Castilla-La Mancha en materia de protección de los consumidores ante los riesgos que plantea la IA. El objetivo es delimitar qué políticas puede emprender cada nivel de gobierno y, sobre todo, clarificar el alcance de la actuación autonómica en este ámbito.

2. Unión Europea

El artículo 4.2 f) TFUE establece que la protección de los consumidores es una competencia compartida entre la UE los Estados miembros. Además, el artículo 12 TFUE impone la obligación de integrar las exigencias de protección de los consumidores en la definición y ejecución de todas las políticas y acciones de la Unión. Por su parte, el artículo 169 TFUE dispone que la Unión contribuirá a garantizar un alto nivel de protección de los consumidores, protegiendo su salud, seguridad e intereses económicos y promoviendo su derecho a la información, a la educación y a organizarse para la defensa de sus intereses. Destaca también el artículo 114 TFUE en cuanto a la armonización del mercado interior.

Sobre este marco normativo, la política de protección de los consumidores y usuarios se encuentra atribuida de manera prácticamente exclusiva a las autoridades de la Unión, con el único límite del principio de subsidiariedad (artículo 5.3 TUE), cuya operatividad es incierta[7]. Probablemente esta concentración competencial se deba a que la UE no sólo busca con sus políticas elevar el nivel de protección de los consumidores, sino también evitar que regulaciones nacionales divergentes generen una fragmentación normativa que obstaculice el mercado interior (artículo 114 TFUE).[8]

Obsérvese que la armonización del derecho de protección de los consumidores se está realizando a través de directivas, que, con el objetivo de evitar barreras al comercio interior, impiden que los Estados miembros puedan aumentar el nivel de protección de los consumidores[9]. Así ocurre con normas que buscan proteger a los consumidores cuando interviene la IA en determinados aspectos de la contratación de consumo. Por ejemplo, el TRLGDCU incorporó, a través del Real Decreto-ley 24/2021, por el que se transpone la Directiva (UE) 2019/2161[10], la obligación de que, en los contratos a distancia, el empresario informe al consumidor, antes de la celebración del contrato, de si el precio ha sido personalizado mediante decisiones automatizadas (artículos 20.1 c) II y 97.1 f) TRLGDCU). Asimismo, el propio TRLGDCU establece, también como resultado de la transposición de la Directiva (UE) 2019/2161, que, en la contratación a distancia, los proveedores de mercados en línea deben facilitar al consumidor información general sobre los parámetros principales que determinan la clasificación de las ofertas resultantes de una búsqueda y sobre la importancia relativa de esos parámetros (artículos 20.3 y 97 bis 1 a) TRLGDCU).

---

[7] Formalmente se trata de una competencia compartida, aunque la UE la ejerce de forma intensa.
[8] *Vid*. Á. CARRASCO PERERA, "§ 1. Relación jurídica y contrato de Derecho de Consumo", en *Derecho de Consumo: materiales, fundamentos, aplicaciones* (Dir. Á. CARRASCO), 2022, Aranzadi, p. 42.
[9] *Vid*. G. HOWELLS / N. REICH, *Study on the extent of harmonisation of EU consumer law,* Parlamento Europeo, 2010 [https://www.europarl.europa.eu/meetdocs/2009_2014/documents/imco/dv/study_howells_reich_/study_howells_reich_en.pdf]
[10] Modifica la Directiva 2011/83/UE y la 2005/29/CE.

Cuando una directiva establece un régimen de armonización plena, como ocurre en el caso de los preceptos citados, los Estados miembros no pueden apartarse de su regulación, ni siquiera para aumentar el nivel de protección del consumidor. No obstante, cuando la propia directiva autoriza expresamente a los Estados a mantener o introducir disposiciones más exigentes o restrictivas, supuesto menos frecuente, esta facultad debe ejercerse dentro de los límites del Derecho de la Unión, entre los que se encuentra la unidad del mercado interior. Un ejemplo se encuentra en el artículo 16 sexies de la Directiva 2011/83/UE, introducido por la Directiva (UE) 2023/2673. Según el legislador comunitario, dado que los *dark patterns* presentan una elevada complejidad técnica y riesgos significativos para los consumidores, la Directiva admite que los Estados miembros mantengan o introduzcan disposiciones más estrictas sobre elementos engañosos en las interfaces, a modo de excepción al principio general de armonización plena, siempre que sean compatibles con el Derecho de la Unión[11].

Por otra parte, en los últimos años, la Unión ha complementado esta armonización mediante reglamentos que, aunque no forman parte estrictamente del derecho de consumo, inciden en la protección de las personas consumidoras ante ciertos riesgos de la IA. Así ocurre con el RGPD, el RSD o el RMD, entre otros. Los reglamentos de la Unión son directamente aplicables y los Estados sólo pueden apartarse de ellos en la medida en que el propio reglamento lo autorice, lo que será raro. Así sucede, por ejemplo, en el artículo 8 del RGPD, relativo a las condiciones del consentimiento del menor en servicios de la sociedad de la información: la edad general se fija en 16 años, pero se permite a los Estados establecer una edad inferior, sin que pueda situarse por debajo de los 13 años. Destaca también el artículo 25 referente a la protección de datos desde el diseño.

En esta lógica de preservación del mercado interior se inscribe el AI Act. Como reglamento de la Unión, es de aplicación directa en todos los Estados miembros, aunque delega en ellos el desarrollo de determinados aspectos, como se examinará en el epígrafe II de este capítulo. Conviene subrayar que el AI Act tampoco forma parte de la normativa de protección al consumidor en sentido estricto. La finalidad del AI Act, en cambio, es garantizar el buen funcionamiento del mercado interior, fijando requisitos armonizados para el desarrollo, la comercialización, la puesta en servicio y el uso de sistemas de IA, sin perjuicio de que así "se promueva una IA fiable y centrada en el ser humano, protegiendo la salud, la seguridad y los derechos fundamentales" (artículo 1). De hecho, el artículo 2.9 AI Act aclara que el Reglamento se entiende "sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión en materia de protección de los

[11] En un sentido parecido, el artículo 1.3 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), precisa que dicha Directiva "completará el ordenamiento jurídico comunitario aplicable a los servicios de la sociedad de la información, sin perjuicio del nivel de protección, en particular, de la salud pública y de los intereses del consumidor, fijados tanto en los instrumentos comunitarios como en las legislaciones nacionales que los desarrollan, *en la medida en que nos restrinjan la libertad de prestar servicios de la sociedad de la información*".

consumidores y de seguridad de los productos". También reseñable el artículo 5 del AI Act, referente a las prohibiciones de sistemas de IA.

Así pues, el marco jurídico de la Unión Europea ofrece a los Estados miembros un margen muy limitado para dictar normas propias de protección de los consumidores cuando la materia ha sido armonizada. Esta limitación responde esencialmente a tres factores: (i) la frecuente utilización de directivas de armonización plena en ámbitos vinculados al mercado interior, que excluyen niveles de protección nacionales superiores, salvo habilitación expresa; (ii) la exigencia de que cualquier disposición más estricta permitida por una directiva sea compatible con el Derecho de la Unión y con el correcto funcionamiento del mercado interior; y (iii) el recurso cada vez más habitual a reglamentos, directamente aplicables y con escasos espacios de adaptación nacional. En consecuencia, el papel normativo de los Estados miembros en materia de protección al consumidor, tanto a nivel central como regional, queda restringido a los ámbitos de flexibilidad que el propio Derecho de la Unión deja abiertos, mientras que, fuera de ellos, la regulación nacional debe alinearse estrictamente con las exigencias derivadas de la armonización y del funcionamiento del mercado interior.

3. Estado español

El artículo 51 CE eleva la defensa de los consumidores a la categoría de principio rector del ordenamiento jurídico. No obstante, este precepto no atribuye por sí mismo una competencia legislativa exclusiva al Estado ni a las Comunidades Autónomas. La competencia en materia de protección de los consumidores depende del reparto previsto en los artículos 148 y 149 CE y de su interpretación por el TC, de modo que no constituye un título competencial autónomo, sino un objetivo que debe alcanzarse a través de los títulos sectoriales existentes[12].

El Estado ostenta competencia en materia de protección al consumidor siempre que se ampare en alguno de los títulos competenciales previstos en el artículo 149.1. CE, como la igualdad de todos los españoles (artículo 149.1.1 CE), la legislación mercantil, civil y procesal (artículo 149.1.6 y 8 CE), las bases de la ordenación de crédito, banca y seguros (artículo 149.1.11), las bases y coordinación de la planificación general de la actividad económica (artículo 149.1.13 CE), la sanidad exterior, las bases y la coordinación general de la sanidad y la legislación sobre productos farmacéuticos (artículo 149.1.16 CE) o las bases del régimen jurídico de las administraciones públicas y el procedimiento administrativo común (artículo 149.1.18 CE); así como el artículo 149.1.10 CE, referente a las estadísticas para fines estatales. De hecho, en ejercicio de alguna de estas competencias se aprobó el TRLGDCU (*vid*. DF 1.ª), cuyo artículo 1 aclara que su contenido sistematiza la normativa general de protección de los consumidores en el ámbito de las competencias del Estado. Asimismo, en ejercicio de algunas de esas competencias, el Estado ha promulgado otras normas sectoriales de protección al

[12] SSTC 71/1982, de 30 de noviembre y 15/1989, de 26 de enero.

consumidor, como la LCCC (*vid*. DF 5.ª), la LCCI (v*id*. DF 13.ª), la Ley 22/2007[13] (*vid*. DF 1.ª), la Ley 4/2012[14] (*vid*. DF 1.ª), la Ley 11/2022[15] (*vid*. DF 2.ª) o la Orden EHA/2899/2011[16] (*vid*. DF 4.ª).

Nótese que prácticamente toda la normativa de consumo derivada del Derecho de la Unión regula distintos aspectos de *los contratos de consumo.* Así pues, el grueso del Derecho de consumo está conformado por *normas excepcionales de Derecho privado contractual*.[17] En consecuencia, el Estado es el poder territorial competente para dictar normas de *Derecho privado de protección al consumidor,* debido a su competencia en legislación civil, mercantil y procesal (artículo 149.1.6 y 8 CE), sin perjuicio de las limitaciones derivadas del Derecho de la Unión antes expuestas. Por ello, las Comunidades Autónomas con competencias en materia de protección al consumidor no son competentes para dictar normas de *Derecho privado contractual* cuando la parte destinataria sea un consumidor[18].

En lo que es objeto de regulación por el AI Act, la capacidad de los Estados miembros está limitada, de modo que solo pueden dictar normas en los aspectos que el AI Act remite a los Estados miembros o deja a su discreción. Así, el capítulo XII del AI Act establece un marco sancionador y exige que los Estados regulen las sanciones y otras medidas de ejecución. Además, el AI Act introduce mecanismos de gobernanza a escala de la Unión destinados a armonizar la aplicación de la normativa, mientras que a escala nacional impone a los Estados la obligación de designar autoridades competentes, incluidas las autoridades notificantes y de vigilancia de mercado, y de regular sus funciones de conformidad con el Reglamento. El AI Act también prevé que los Estados miembros deben realizar otras funciones como la alfabetización en materia de IA; el apoyo a la innovación y, en particular, el establecimiento de espacios controlados de pruebas para la IA con el fin de facilitar la innovación, el desarrollo, la prueba y la validación de los sistemas de IA (artículo 57 AI Act).

En cumplimiento de alguno de estos mandatos, el Ministerio para la Transformación Digital y de la Función Pública ha elaborado el APLIA[19], que establece un régimen sancionador y regula la gobernanza nacional prevista en el AI Act. El APLIA se dicta al amparo principalmente de los artículos 149.1.1 y 13 CE, que atribuyen al Estado las competencias sobre las condiciones básicas que garanticen la igualdad de todos los

[13] La Ley 22/2007, de 11 de julio, regula la comercialización a distancia de servicios financieros destinados a los consumidores, buscando proteger sus derechos y garantizar la transparencia en las transacciones. BOE núm. 166, de 12 de julio de 2007.
[14] Ley 4/2012, de 25 de junio, de medidas administrativas y fiscales. BOE núm. 166, de 12 de julio de 2012.
[15] Ley 11/2022, de 28 de junio, General de Telecomunicaciones. BOE núm. 155, de 29 de junio de 2022.
[16] Orden EHA/2899/2011, de 28 de octubre, de transparencia y protección del cliente de servicios bancarios. BOE núm. 261, de 29 de octubre de 2011.
[17] *Vid*. Á. CARRASCO PERERA, "§ 1. Relación jurídica y contrato de Derecho de Consumo", en *Derecho de Consumo: materiales, fundamentos, aplicaciones* (Dir. Á. Carrasco), 2022, Aranzadi, pp. 45-46.
[18] Á. CARRASCO PERERA, "§ 1. Relación jurídica y contrato de Derecho de Consumo", en *Derecho de Consumo: materiales, fundamentos, aplicaciones* (Dir. Á. Carrasco), 2022, Aranzadi, p. 55.
[19] Anteproyecto de Ley para el buen uso y la gobernanza de la IA, referenciado anteriormente.

españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y las bases y coordinación de la planificación general de la actividad económica. En consecuencia, es probable que las Comunidades Autónomas no puedan desarrollar normativa propia en los ámbitos que el AI Act reserva a los Estados miembros, dado que ello podría socavar las competencias estatales en materia de condiciones básicas de igualdad de todos los españoles (artículo 149.1.1 CE) y de bases y coordinación de la planificación general de la actividad económica (artículo 149.1.13 CE).

4. Castilla-La Mancha

Las Comunidades Autónomas han asumido competencias en materia de protección del consumidor a través de sus Estatutos de Autonomía, al amparo del artículo 143.3 CE, que les permite asumir competencias no atribuidas expresamente al Estado[20]. En el caso de Castilla-La Mancha, el artículo 32.6 de su Estatuto de Autonomía, aprobado por la Ley Orgánica 9/1982, de 10 de agosto, establece que, en el marco de la legislación básica del Estado y en los términos que esta disponga, corresponde a la Junta de Comunidades el desarrollo legislativo y la ejecución en materia de defensa de los consumidores y usuarios[21], de acuerdo con las bases y la ordenación de la actividad económica general, la política monetaria del Estado y las bases y coordinación general de la sanidad, en los términos de lo previsto en los artículos 38, 131 y 149.1.11, 13 y 16 CE.

En ejercicio de esta competencia, y conforme al artículo 9.2 del Estatuto de Autonomía, las Cortes de Castilla-La Mancha han aprobado sucesivamente la Ley 3/1995, de 9 de marzo, la Ley 11/2005, de 15 de diciembre, y, finalmente, la vigente Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras en Castilla-La Mancha [22], dictada expresamente al amparo del artículo 32.6 del Estatuto de Autonomía y en desarrollo de la legislación básica estatal.

Nótese que resultarían inconstitucionales normas autonómicas, dictadas al amparo de la competencia en materia de protección a los consumidores, que innoven en materia de contratos, que incidan en la legislación procesal o que afectan a la unidad de mercado, pues esos ámbitos corresponden en exclusiva al Estado conforme al artículo 149.1 CE[23]. Ahora bien, la limitación competencial de las Comunidades Autónomas en materia de protección al consumidor ni siquiera deriva del reparto competencial interno, sino de la armonización plena impuesta por el Derecho de la Unión Europea, que vincula por igual al Estado y a las Comunidades Autónomas.

---

[20] M. J. Reyes López, *Manual de Derecho privado de consumo* (3.ª ed.), 2022, Wolters Kluwer (formato electrónico).
[21] Es preciso indicar que la competencia es de desarrollo legislativo y ejecución, no de normativa básica.
[22] Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras en Castilla-La Mancha. DOCM núm. 64, de 1 de abril de 2019.
[23] SSTC 26/2012, de 1 de marzo; 54/2018, de 31 de octubre; 3/2019, de 31 de enero; 72/2021, de 18 de marzo; y 20/2024 de 8 de octubre.

Por ello, Castilla-La Mancha no puede aprobar normas que amplíen o reduzcan el contenido de las obligaciones de información precontractual establecidas en los artículos 20.3, 97.1 f) y 97 bis.1 a) TRLGDCU, que proceden de la Directiva (UE) 2019/2161, la cual establece un marco de armonización plena para la información que deben ofrecer los comerciantes que celebran contratos a distancia y los mercados en línea. Salvo en los supuestos expresamente permitidos, los Estados no pueden mantener ni introducir disposiciones más estrictas, so pena de fragmentar el mercado interior, lo que excluye cualquier margen autonómico adicional. Y en caso de que los Estados miembros tuvieran tal margen, en España, la competencia legislativa probablemente la tendrá el Estado en virtud de su competencia en legislación civil, mercantil, procesal, condiciones básicas que garanticen la igualdad de todos los españoles, planificación general de la actividad económica, ordenación del crédito, banca y seguros, etc.

Un ejemplo claro de extralimitación sería que una comunidad autónoma impusiera la obligación al proveedor del mercado en línea de ofrecer información detallada sobre cada parámetro empleado para determinar la clasificación de las ofertas[24]. También sería contrario al régimen de armonización plena exigir la identificación de parámetros concretos (edad, género, localización, historial de compras, etc.) o imponer la forma en que debe explicarse la importancia relativa de cada uno. Se iría así más allá de los previsto en el artículo 97 bis TRLGDCU, que procede de una Directiva de armonización plena. De igual modo, en materia de precios personalizados, la comunidad autónoma no puede ampliar ni reducir la obligación prevista en los artículos 20 o 97.1 f) TRLGDCU, que exige al comerciante que contrata a distancia informar al consumidor de forma clara y comprensible cuando el precio se determine mediante decisiones automatizadas. Sería incompatible, por ejemplo, imponer la identificación de los datos personales concretos utilizados para fijar el precio, detallar el algoritmo o modelo empleado, indicar el porcentaje de influencia de cada variable, establecer plazos específicos de comunicación o añadir advertencias adicionales en la interfaz. Con ello se pasaría de la obligación general de transparencia fijada por el TRLGDCU a un deber específico y cerrado, alterando la uniformidad europea establecida por la Directiva 2019/2161. En consecuencia, no resultaría aplicable la jurisprudencia constitucional que autoriza a las comunidades autónomas a reforzar la protección del consumidor mediante mayores exigencias informativas, ya que dicha línea jurisprudencial se refiere a supuestos en los que la norma estatal no deriva de una armonización europea.[25] Evidentemente, tampoco puede una comunidad autónoma regular los requisitos técnicos de los sistemas de IA, que serán objeto del AI Act, ni ejercer funciones de vigilancia de mercado que correspondan a las autoridades designadas conforme al futuro APLIA.

Aunque las Comunidades autónomas no pueden regular requisitos técnicos de los sistemas de IA ni obligaciones contractuales armonizadas, sí pueden actuar en materia de alfabetización, inspección y formación. Así, la Comunidad Autónoma puede promover campañas de alfabetización digital dirigidas a los consumidores, que por ejemplo

[24] En este sentido, destacan las SSTC 88/1986, de 1 de julio, 352/1983, de 1 de julio y 62/1991, de 22 de marzo.
[25] *Vid*. STC 119/2018, de 31 de octubre.

adviertan de que el orden de resultados puede estar condicionado por pagos publicitarios o algoritmos de recomendación y que los precios ofertados pueden haber sido personalizados automatizadamente en base a datos personales del consumidor. Puede también emprender campañas de formación del personal inspector en los derechos que asisten al consumidor cuando la IA interviene en la comercialización de bienes, productos y prestación de servicios, para que dichos inspectores puedan ejercer su función de constatar el cumplimiento de la normativa[26]. También podría dictar normas en materia de inspección, formación y alfabetización digital. Sobre lo qué puede hacer Castilla-La Mancha en este ámbito trataremos en los epígrafes III y IV de este capítulo.

Finalmente, conviene señalar que algunas Comunidades Autónomas ya han aprobado normativa específica en materia de IA, pero su enfoque no es la protección de los consumidores en el mercado, sino la regulación del uso de la IA en el ámbito de la propia Administración autonómica. Así, la Ley 2/2025, de 2 de abril, para el desarrollo e impulso de la inteligencia artificial en Galicia, establece principios de uso ético y confiable en la Administración pública gallega, crea órganos de gobernanza, fija un marco para el registro y verificación de sistemas y habilita un entorno controlado de pruebas antes del despliegue. En la misma línea, el Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura, adopta medidas urgentes para implantar la IA en la Administración autonómica, prevé una estrategia regional de IA y la creación de un sandbox regulatorio[27]. El Decreto 98/2025, de 22 de julio, por el que se regula el uso de la IA en la Administración del Principado de Asturias y su sector público, regula el uso de la IA en toda su Administración y sector público, fijando principios de transparencia, trazabilidad, supervisión humana y minimización de sesgos, estableciendo procedimientos de verificación previa y abriendo el entorno de pruebas al sector privado. Finalmente, el Anteproyecto de Ley Andalucía Digital, de 15 de octubre de 2024, incluye un título completo sobre automatización e IA, con requisitos técnicos, códigos éticos, impulso de proyectos estratégicos y la creación de un Centro de Inteligencia Artificial de Andalucía.

II. GOBERNANZA EN MATERIA DE IA

1. Objetivo

En este epígrafe explicamos qué autoridades europeas y nacionales intervienen en la aplicación del AI Act, partiendo de que dicho Reglamento exige que los Estados miembros designen autoridades competentes —incluidas autoridades notificantes y de vigilancia del mercado— y de que el APLIA concreta cuáles son en España. A partir de ahí, se expone qué funciones desempeñan cada una de ellas.

[26] *Vid*. Cap. VII, sobre formación y campañas.
[27] Vid. Cap. VIII, sobre la creación de un sandbox autonómico en Castilla-La Mancha.

2. Autoridades Europeas

En primer lugar, la *European AI Office* es el órgano técnico creado por la Comisión Europea para desarrollar los conocimientos especializados y las capacidades de la Unión en materia de IA. Sus funciones incluyen coordinar la aplicación del AI Act, proporcionar asistencia técnica y servir de apoyo a los Estados miembros para garantizar una implementación uniforme en toda la Unión (artículo 64 AI Act).

En segundo lugar, el Consejo Europeo de IA es el principal foro de coordinación y asesoramiento, creado en base al artículo 65 del AI Act. Está integrado por un representante de cada Estado miembro y cuenta con el Supervisor Europeo de Protección de Datos como observador. Su función es facilitar la aplicación coherente del AI Act en toda la Unión, coordinando a las autoridades nacionales competentes, apoyando actividades conjuntas de vigilancia de mercado, recopilando y difundiendo conocimientos técnicos y mejores prácticas, y emitiendo recomendaciones y dictámenes sobre interpretación, aplicación y posibles revisiones del AI Act. Además, contribuye a armonizar las prácticas administrativas y promueve la alfabetización en IA y la cooperación internacional, para lo cual establece subgrupos permanentes de cooperación entre autoridades de vigilancia de mercado y organismos notificados (artículos 65 y 66 AI Act).

En tercer lugar, el foro consultivo constituye el espacio de participación de las partes interesadas, garantizando una representación equilibrada de industria, pymes, sociedad civil y mundo académico, que se convierte en un instrumento de garantía para la participación equilibrada de la sociedad civil. Nombrado por la Comisión, asesora al Consejo de IA y a la Comisión, elabora dictámenes y recomendaciones, puede crear subgrupos de trabajo para cuestiones específicas y presenta un informe anual de sus actividades (artículo 67 AI Act).

Finalmente, el grupo de expertos científicos independientes está formado por especialistas seleccionados por su competencia técnica y su independencia, mediante acto de ejecución de la Comisión, y que estará centrado en modelos de IA de propósito general, Este grupo apoya a la Oficina de IA en la identificación de riesgos sistémicos de modelos de IA de uso general, en el desarrollo de herramientas para su evaluación y clasificación, y en la asistencia a las autoridades de vigilancia de mercado, incluidas las actividades transfronterizas y los procedimientos de salvaguardia de la Unión (artículo 68 AI Act). El AI Act permite que los Estados miembros accedan a estos expertos para reforzar sus propias actividades de garantía del cumplimiento, en condiciones establecidas por la Comisión, incluida la posibilidad de imponer tasas para recuperar costes (artículo 69 AI Act).

3. Autoridad notificante en España: Secretaría de Estado de Digitalización e Inteligencia Artificial

La autoridad notificante es la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad[28], así como de su supervisión (artículo 3.19 AI Act). Cada Estado miembro nombrará o constituirá al menos una autoridad notificante (artículo 28.1 AI Act).

En España, se prevé que la Secretaría de Estado de Digitalización e Inteligencia Artificial[29], a través de la Dirección General de Inteligencia Artificial, sea la autoridad notificante a los efectos de lo dispuesto en el artículo 28.1 AI Act, como órgano responsable de establecer los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión (artículo 4.2 APLIA). La autoridad notificante será competente para el ejercicio de la potestad sancionadora de los organismos notificados[30] recogidos en el artículo 99.4 sección e) APLIA (artículo 4.1 APLIA).

No obstante, la evaluación y la supervisión de los organismos notificados se realizarán por el organismo nacional de acreditación de conformidad con el Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la ENAC como organismo nacional de acreditación de acuerdo con lo establecido en el Reglamento (CE) n.º 765/2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos, en virtud del artículo 28.2 del AI Act (artículo 4.3 APLIA).

Cuando se compruebe que un organismo notificado previamente designado ya no satisface los requisitos establecidos en el artículo 31 AI Act, la Secretaría de Estado de Digitalización e Inteligencia Artificial o la Entidad Nacional de Acreditación (ENAC), en su caso, retirará la designación, previa tramitación del correspondiente procedimiento administrativo, con audiencia al interesado, e informará de ello a la Comisión Europea y a los demás Estados miembros de acuerdo con lo recogido en el artículo 36 del AI Act (artículo 4.4 APLIA).

Además, corresponde a la Secretaría de Estado de Digitalización e Inteligencia Artificial la designación del representante en el Consejo de IA establecida en el artículo 65.3 AI Act (artículo 5 APLIA). Asimismo, corresponden a la Secretaría de Estado de Digitalización e Inteligencia Artificial las comunicaciones a la Comisión sobre las identidades y funciones de las autoridades de vigilancia de mercado que establece el artículo 70.2 del AI Act

[28] "Organismo de evaluación de la conformidad": un organismo que desempeña actividades de evaluación de la conformidad de terceros, como el ensayo, la certificación y la inspección (artículo 3.21 AI Act).
[29] Está pendiente de aprobación definitiva, atendiendo al APLIA.
[30] "Organismo notificado": un organismo de evaluación de la conformidad notificado con arreglo AI Act y a otros actos pertinentes de la legislación de armonización de la Unión (artículo 3.22 AI Act).

4. Autoridades de vigilancia del mercado en España

4.1. Disposiciones generales

Cada Estado miembro establecerá o designará al menos una autoridad de vigilancia del mercado (artículo 70.1 AI Act).

En España, las autoridades de vigilancia del mercado serán competente para el ejercicio de la potestad sancionadora respecto de los proveedores de sistemas de IA y de modelos de IA de uso general, los proveedores potenciales de sistemas de IA y de modelos de IA de uso general que realicen pruebas en condiciones reales antes de la introducción en el mercado o puesta en servicio, los responsables del despliegue de sistemas de IA, los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca, los representantes autorizados de proveedores no establecidos en la Unión, y los importadores y distribuidores de sistemas de IA (mencionados en artículo 3.1 APLIA).

Además, corresponde a las autoridades de vigilancia del mercado todas las funciones de vigilancia, inspección y sanción de los sistemas de IA establecidas en el Capítulo IX AI Act (artículo 6.10 APLIA). En efecto, las autoridades de vigilancia del mercado realizarán las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control. El personal funcionario adscrito a las unidades administrativas competentes que realicen la inspección tendrá la consideración de autoridad pública en la instrucción de los procedimientos sancionadores (artículo 7.1 APLI). Las autoridades de vigilancia de mercado podrán ser asistidas por la Agencia Española de Supervisión de Inteligencia Artificial, creada por Real Decreto 729/2023 (AESIA), así como, de acuerdo con los actos delegados de la Comisión, por los expertos descritos en el artículo 69 AI Act, en las labores de supervisión y control que les asigna el AI Act (artículo 7.2 APLI).

Por otra parte, en cualesquiera supuestos en los que las decisiones o las actuaciones de una autoridad de vigilancia puedan afectar a los intereses o a las competencias de otras, deberá aquella recabar informe de estas antes de resolver (artículo 6.1 APLIA).

4.2. La Agencia Española de Supervisión de Inteligencia Artificial

La AESIA se adscribe al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Esta Agencia Estatal cumplirá con el objeto, fines y funciones atribuidas a la misma en el Estatuto que se aprueba por Real Decreto 729/2023, de 22 de agosto.

Se prevé que la AESIA sea el Punto de contacto único de acuerdo con lo establecido en el artículo 70.2 AI Act, de forma que sea la encargada de “comunicar a la Comisión la identidad de las autoridades notificantes y de las autoridades de vigilancia del mercado y

las funciones de dichas autoridades, así como cualquier cambio posterior al respecto" (artículo 6.2 APLIA).

Asimismo, se prevé que la AESIA sea la autoridad de vigilancia del mercado de los siguientes sistemas de IA (artículo 6.2 APLIA):

a) Los que realicen prácticas de IA prohibidas recogidas en los apartados a), b), c), e) y f) del artículo 5.1 AI Act, siempre que los sistemas no se utilicen a los efectos de la garantía del cumplimiento del derecho, la gestión de fronteras, y la justicia o los procesos democráticos.

b) Los sistemas de IA de alto riesgo descritos en el Anexo III AI Act, apartado 1, relativo al ámbito de la biometría, siempre que los sistemas no se utilicen a los efectos de la garantía del cumplimiento del derecho, la gestión de fronteras, y la justicia o los procesos democráticos, y excluyendo, en consonancia con el Anexo III.1 a) AI Act, los sistemas para identificación biométrica remota cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser.

c) Los sistemas de IA de alto riesgo descritos en el Anexo III AI Act, apartado 2, relativo al ámbito de infraestructuras críticas.

d) Los sistemas de IA de alto riesgo descritos en el Anexo III AI Act, apartado 3, relativo al ámbito de la educación y formación profesional.

e) Los sistemas de IA de alto riesgo descritos en el Anexo III AI Act, apartado 4, relativo al ámbito del empleo y gestión de las personas trabajadoras.

f) Los sistemas de IA de alto riesgo descritos en el Anexo III AI Act, apartado 5, relativo al ámbito de los servicios y prestaciones esenciales, exceptuando aquellos descritos en la letra b) y c), relativos a sistemas para la evaluación de solvencia o calificación crediticia y a los de evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud, respectivamente.

g) Los sistemas de IA que no se categoricen como prohibidos o de alto riesgo, cuando puedan incumplir el deber de transparencia u otra obligación establecida en la normativa aplicable en materia de IA.

Como veremos más adelante, la AESIA actúa como autoridad de vigilancia de mercado para de los sistemas de IA de alto riesgo asociados a los productos regulados por actos legislativos de armonización, cuando las autoridades de vigilancia del mercado para los sectores armonizados comuniquen a la ASEIA la carencia de medios técnicos, financieros y humanos idóneos para la supervisión (artículo 6.7 APLIA).

Además, con carácter excepcional y cuando sea necesario para evitar o mitigar las consecuencias derivadas de incidentes graves causados por sistemas de IA, la AESIA

promoverá, coordinará o adoptará cuantas medidas sean necesarias, con la colaboración de las autoridades de vigilancia de mercado que se describirán a continuación, con la Comisión Europea y de acuerdo con sus respectivas competencias (artículo 6.12 APLIA).

Por otro lado, las autoridades de vigilancia de mercado presentarán a la AESIA, con carácter anual o a petición de la Agencia, un informe sobre el estado de sus recursos financieros y humanos, incluyendo una evaluación de su idoneidad (artículo 6.14 APLIA).

Asimismo, la AESIA podrá prestar, en el ámbito del AI Act, asistencia técnica a las autoridades de vigilancia de mercado competentes, incluyendo la tramitación de expedientes y el posible ejercicio de potestades públicas o administrativas, en los términos que se establezcan en los oportunos convenios de colaboración (artículo 6.15 APLIA).

Por último, la AESIA será la autoridad nacional competente responsable de establecer el espacio controlado de pruebas para la IA de obligada creación en virtud del artículo 57.1 AI Act (artículo 9 APLIA).

4.3. Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos

Se designa a la AEPD y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, como autoridades de vigilancia del mercado de los siguientes sistemas de IA (artículo 6.3 APLIA):

a) Los que realicen prácticas de IA prohibidas recogidas en los apartados d), g) y h) del artículo 5.1 AI Act.

b) Los sistemas de IA de alto riesgo descritos en el Anexo III.1 AI Act, relativo al ámbito de la biometría, cuando los sistemas se utilicen a los efectos de la garantía del cumplimiento del derecho o la gestión de fronteras, excluyendo, en consonancia con el Anexo III.1 a) AI Act, los sistemas para identificación biométrica remota cuya única finalidad sea confirmar que una persona física concreta es la persona que afirma ser.

c) Los sistemas de IA de alto riesgo descritos en el Anexo III.6 AI Act, relativo al ámbito de la garantía del cumplimiento del derecho, y las prácticas prohibidas de IA que recaigan en este ámbito.

d) Los sistemas de IA de alto riesgo descritos en el Anexo III.7 AI Act, relativo al ámbito de migración, asilo y gestión del control fronterizo, y las prácticas prohibidas de IA que recaigan en este ámbito.

4.4. Banco de España y Comisión Nacional Mercados y Valores

Se designa al BdE y a la CNMV como autoridades de vigilancia del mercado, en el área de competencia que cada una ostenta en relación de la supervisión financiera de entidades financieras con arreglo a la legislación relativa a la supervisión de servicios financieros, de los sistemas de IA de alto riesgo descritos en el Anexo III.5 b) AI Act, relativo a sistemas del ámbito de la evaluación de solvencia o calificación crediticia (artículo 6.4 APLIA).

4.5. Dirección General de Seguros y Fondos de Pensiones

Se designa a la DGSFP en el área de competencia que ostenta con arreglo a la legislación relativa a la supervisión de seguros de vida y de salud, como autoridad de vigilancia del mercado de los sistemas de IA de alto riesgo descritos en el Anexo III.5 c) AI Act, relativo a sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud (artículo 6.5 APLIA).

4.6. La Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial

Se designa a la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial como autoridad de vigilancia del mercado de los sistemas de IA de alto riesgo descritos en el Anexo III.8.a) AI Act, relativo a los ámbitos de la administración de justicia, y las prácticas prohibidas de IA que recaigan en este ámbito (artículo 6.6 APLIA).

4.7. Junta Electoral Central

Se designa a la Junta Electoral Central como autoridad de vigilancia del mercado de los sistemas de IA de alto riesgo descritos en el Anexo III.8.b) AI Act, relativa a procesos democráticos, así como las prácticas prohibidas de IA que recaigan en este ámbito (artículo 6.6 APLIA).

4.8. Autoridades de vigilancia del mercado para productos regulados por legislación armonizada y competencia residual de la AESIA

Las autoridades de vigilancia del mercado designadas en virtud de los actos legislativos enumerados en el anexo I, sección A AI Act, actuarán como autoridades de vigilancia del mercado de los sistemas de IA de alto riesgo asociados a los productos regulados por dichos actos legislativos de armonización (artículo 74.3 AI Act).

Como expusimos, cuando una de estas autoridades de vigilancia del mercado comunique a la AESIA carencia de medios técnicos, financieros y humanos idóneos para la supervisión, inspección y sanción de sistemas de IA, asumirá tales funciones la Agencia, garantizando la coordinación con la autoridad sectorial de vigilancia del mercado pertinente, hasta que dicha autoridad comunique disponer de los medios idóneos para ejercer las funciones de vigilancia, inspección y sanción (artículo 6.7 APLIA).

4.9. Competencia de secretaria de Estado de Digitalización e IA en materia de vigilancia de mercado

Para el resto de los casos no contemplados anteriormente, o en caso de nuevas áreas de supervisión de IA establecidas por la Comisión a través de actos delegados de acuerdo con artículo 7.1 AI Act, corresponderá a la Secretaría de Estado de Digitalización e Inteligencia Artificial, por Resolución de la persona titular, la designación de otras autoridades de vigilancia del mercado diferentes de las establecidas en el presente artículo, incluyendo el supuesto previsto en el párrafo 2º del artículo 74.3 AI Act. Dicha designación exigirá la previa evaluación de la idoneidad de los medios financieros y humanos asignados (artículo 7.8).

4.10. Coordinación de las autoridades de vigilancia del mercado

Con el fin de garantizar una actuación uniforme, coordinada y eficaz en el desarrollo de las actuaciones que les atribuye el APLIA, las autoridades de vigilancia del mercado se suministrarán e intercambiarán cualquier información operativa que asegure la adecuada coordinación en el ejercicio de sus funciones.

En las actuaciones de inspección, vigilancia y control de lo dispuesto en el AI Act, las autoridades de vigilancia del mercado tendrán especialmente en cuenta los hallazgos e intercambios producidos en el contexto del Comité Europeo de Inteligencia Artificial y, en todo caso, las directrices sobre la aplicación del mencionado Reglamento que, según éste describe en su artículo 96, elabore la Comisión (artículo 8.1 APLIA).

A efectos de coordinación, las autoridades de vigilancia del mercado informaran, en un plazo no superior a 72 horas, a través del sistema Safety Gate contemplado en el Reglamento de Seguridad de Productos, o cualquier otro que lo sustituya, de lo siguiente (artículo 8.2 APLIA): a) Informarán sobre los incidentes graves, de acuerdo con los artículos 73 y 76 AI Act; b) Ante la identificación de un riesgo presentado por un sistema de IA, cuando la autoridad de vigilancia del mercado estime que la infracción excede el territorio nacional, informarán sobre la evaluación del sistema, las medidas correctoras dictadas al operador y, en su caso, las medidas provisionales adoptadas, de acuerdo con el artículo 79 AI Act; c) Cuando la autoridad de vigilancia del mercado estime que es de alto riesgo un sistema de IA que el operador clasificó como no de alto riesgo, y que la utilización del sistema no se circunscribe al territorio nacional, informará sobre la evaluación del sistema, las medidas correctoras dictadas al operador y, en su caso, las

medidas provisionales adoptadas, de acuerdo con el artículo 80 AI Act; d) Cuando la autoridad de vigilancia del mercado concluya que un sistema de IA de alto riesgo que es conforme con el AI Act presenta riesgos para la salud o la seguridad de las personas, los derechos fundamentales u otros aspectos de protección del interés público, informará con detalle sobre las conclusiones obtenidas, de acuerdo con el artículo 82 AI Act.

Las autoridades de vigilancia del mercado harán uso del sistema de información y comunicación del artículo 34 del Reglamento 2019/1020, de 20 de junio de 2019, de Vigilancia del Mercado y de la Conformidad de los Productos, con el fin de intercambiar datos sobre cuestiones relativas a la aplicación del AI Act y de otra legislación de seguridad de producto que pueda ser de aplicación en el ejercicio de sus funciones (artículo 8.3 APLIA).

La AESIA podrá poner en marcha las medidas que resulten más adecuadas para lograr la efectiva coordinación de las actuaciones orientadas a la prevención de los riesgos y a la aplicación del régimen de supervisión de sistemas de IA establecido en el AI Act (artículo 8.4 APLIA).

A efectos de garantizar dicha coordinación, se crea la Comisión mixta de coordinación de autoridades de vigilancia del mercado a efectos de asegurar la aplicación de las competencias definidas en APLIA. La AESIA ostentará su presidencia, la secretaría y la gestión del órgano (artículo 8.5).

Sin perjuicio de las medidas de coordinación y colaboración que se establezcan reglamentariamente, las autoridades de vigilancia del mercado designadas bajo el APLIA intercambiarán la información anual sobre las actividades que realicen para garantizar la elaboración del informe anual que se establece como obligación en los artículos 5 y 6 del AI Act.

III. POSIBLES LÍNEAS DE ACCIÓN LEGISLATIVA POR PARTE DE CASTILLA LA MANCHA

1. Modificación de la Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras de Castilla-La Mancha

La actualización de la Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras de Castilla-La Mancha en materia de IA debe situarse siempre dentro del marco competencial autonómico y respetando los límites fijados por la normativa europea y estatal. En este contexto, es posible introducir modificaciones en el Estatuto que "refuercen" los derechos de las personas consumidoras frente al uso de sistemas de IA en las relaciones de consumo.

2. Nuevos derechos

El artículo 5 de la Ley 3/2019 reconoce los nuevos derechos de los consumidores, que se añaden a los básicos del artículo 4. Se podría añadir un apartado 10 al artículo 5 con este contenido:

"10. En las relaciones de consumo en que los empresarios elaboren perfiles mediante tratamiento automatizado de datos personales, las personas consumidoras tendrán derecho:
a) A recibir información clara y accesible sobre la existencia de dicho tratamiento automatizado.
b) A conocer los criterios utilizados para la determinación de precios personalizados basados en tratamiento automatizado de datos personales.
c) A ser informadas de que la presentación, recomendación o clasificación de ofertas se realiza mediante procedimientos automatizados, así como de los principales parámetros que los determinan.
d) A solicitar intervención de una persona y a obtener una revisión humana cuando una decisión automatizada produzca efectos significativos en sus intereses económicos."

3. Protección intereses económicos y sociales

El artículo 22 de la Ley 3/2019 promueve el empoderamiento financiero y digital de las personas consumidoras. Así, podría ser oportuno añadir un nuevo apartado 3 al artículo 22, con la siguiente redacción:

"3. Las administraciones públicas con competencias en materia de consumo impulsarán programas de alfabetización digital dirigidos a que las personas consumidoras comprendan el funcionamiento básico de los sistemas de inteligencia artificial utilizados en las relaciones de consumo, en particular los relativos a la personalización de precios y a los sistemas de recomendación y clasificación de ofertas".

4. Información y transparencia

El artículo 27 regula la información a la persona consumidora. Podría añadirse al final del apartado 1 lo siguiente:

"Estos principios serán igualmente aplicables a la información facilitada a las personas consumidoras cuando intervengan sistemas automatizados o de inteligencia artificial en la presentación, clasificación o recomendación de bienes y servicios."

El artículo 29, relativo a la información del precio o contraprestación, podría modificarse en el sentido de añadir un apartado 5 del siguiente tenor:

"5. Cuando el precio ofrecido a la persona consumidora haya sido personalizado mediante la utilización de sistemas automatizados o de inteligencia artificial, las administraciones

públicas con competencias en materia de consumo desarrollarán iniciativas de información y sensibilización que permitan a las personas consumidoras identificar y comprender este fenómeno y sus efectos en la decisión de compra."

El artículo 31, sobre precios dinámicos, podría reformarse en el siguiente sentido:

"Siempre que no provoque efectos contraproducentes sobre la competencia efectiva y, por ende, sobre las propias personas consumidoras, las administraciones públicas con competencias en materia de consumo garantizarán la transparencia en las transacciones sujetas a precios dinámicos, incluidos los supuestos en que tales precios se determinen mediante sistemas automatizados o de inteligencia artificial."

5. Atención al consumidor

El artículo 36 de la Ley 3/2019, de 22 de marzo, regula los servicios de atención a las personas consumidoras por parte de las empresas. Así, podría añadirse un nuevo apartado con la siguiente redacción:

"7. Cuando la atención a las personas consumidoras se preste mediante sistemas automatizados o de inteligencia artificial, las empresas deberán informar de forma clara de esta circunstancia. En todo caso, la persona consumidora tendrá derecho a solicitar y obtener, si lo desea, atención humana en la tramitación de su queja o reclamación, con el fin de garantizar la efectividad en la defensa de sus derechos."

6. Control de la información

El artículo 41, sobre información de los bienes, productos y servicios, podría modificarse, incluyendo un apartado 6 del siguiente tenor:

"**6.** Asimismo, cuando la información, publicidad o comunicación comercial dirigida a las personas consumidoras se genere total o parcialmente mediante sistemas de inteligencia artificial, las administraciones públicas con competencias en materia de consumo velarán porque se advierta expresamente de esta circunstancia, promoviendo además acciones informativas y educativas que permitan a las personas consumidoras comprender su alcance y efectos en la toma de decisiones de consumo."

7. Actuaciones informativas y divulgativas

El artículo 43, sobre actuaciones informativas y divulgativas en materia de consumo, podría ser modificado, en el sentido de añadir un apartado 4 con el siguiente contenido:

"4. Las administraciones públicas con competencias en materia de consumo impulsarán actuaciones de información y divulgación dirigidas específicamente a explicar a las personas consumidoras el funcionamiento y los posibles efectos de los sistemas de inteligencia artificial en las relaciones de consumo. Estas actuaciones incluirán campañas de sensibilización en medios de comunicación y redes sociales sobre prácticas como la personalización de precios y la clasificación automatizada de ofertas, fomentando la comprensión crítica de estas herramientas y sus implicaciones en la toma de decisiones de consumo."

8. Educación y formación

Se podría añadir una nueva letra f) al apartado 1 del artículo 44, sobre educación y formación en materia de consumo, con el siguiente contenido:

"f) El conocimiento y la comprensión de los sistemas de inteligencia artificial aplicados al consumo, incluyendo la forma en que inciden en la fijación de precios personalizados, en la clasificación y recomendación de ofertas, con el fin de dotar a las personas consumidoras de competencias digitales que les permitan adoptar decisiones de compra libres e informadas.»

9. Requisitos de las ofertas

El artículo 54 de la Ley 3/2019, relativo a la oferta, promoción y comunicación comercial, podría modificarse para incluir un apartado 4 del siguiente tenor:

"4. Cuando la oferta, promoción o comunicación comercial dirigida a las personas consumidoras sea generada o personalizada mediante sistemas de inteligencia artificial, deberá advertirse expresamente de esta circunstancia de forma clara y comprensible, a fin de garantizar la transparencia en la relación de consumo."

10. Infracciones

En infracciones leves (artículo 140) podría añadirse un apartado 25 con la redacción que sigue:

«25. No informar de forma clara a la persona consumidora de que la atención, comunicación comercial u oferta recibida se realiza mediante sistemas automatizados o de inteligencia artificial, cuando así lo exija esta ley».

En infracciones graves (artículo 141) podría añadirse un apartado 39 con esta redacción:

«39. No garantizar a la persona consumidora el acceso a atención humana cuando esta lo solicite tras haber sido atendida por un sistema automatizado o basado en inteligencia artificial, conforme al artículo 36.7».

IV. OTRAS LÍNEAS DE ACTUACIÓN AUTONÓMICA

1. Intervención administrativa en el marco estatal

Los artículos 96, 97 y 98 de la Ley 3/2019 ofrecen a Castilla-La Mancha la posibilidad de reforzar la protección de las personas consumidoras frente al uso de la IA mediante una actuación coordinada con las políticas estatales y con otras comunidades autónomas.

En primer lugar, en virtud del artículo 96, la Junta podría integrarse en proyectos piloto estatales que tengan que ver con sistemas de IA que puedan afectar al consumidor. Así, podría participar en proyectos con la AESIA y la Dirección General de Consumo.

En segundo lugar, el artículo 97 habilita a la Junta para elaborar, en coordinación con otras administraciones, protocolos de actuación frente a la publicidad digital generada por IA. Estos protocolos podrían establecer criterios comunes para detectar comunicaciones comerciales engañosas o manipuladoras en redes sociales, así como mecanismos para requerir explicaciones claras a los operadores cuando los anuncios o clasificaciones de productos se generen de manera automatizada. La formalización de convenios con la Agencia Española de Consumo, Seguridad Alimentaria y Nutrición permitiría homogeneizar procedimientos de inspección en todo el territorio estatal, evitando desigualdades de tutela entre comunidades autónomas.

Por último, conforme al artículo 98, Castilla-La Mancha podría impulsar la colaboración interautonómica en materia de consumo digital, favoreciendo el intercambio de información sobre reclamaciones relacionadas con algoritmos de recomendación, precios personalizados o denegación automatizada de servicios. Podría plantearse, por ejemplo, la creación de un Observatorio Interautonómico de Consumo e Inteligencia Artificial, integrado por comunidades limítrofes como Madrid, Valencia o Andalucía, que recopile datos sobre prácticas comerciales basadas en IA y publique informes periódicos. Esta red serviría para detectar patrones de riesgo comunes, coordinar inspecciones conjuntas y elaborar guías formativas para el personal inspector.

De este modo, la Junta no asumiría funciones estatales de control técnico de la IA —que corresponden al AI Act—, pero sí reforzaría la aplicación práctica de los derechos de las personas consumidoras mediante cooperación institucional, protocolos comunes y proyectos de inspección coordinada

2. Intervención administrativa en el marco autonómico

Los artículos 99 y 100 de la Ley 3/2019 permiten que la Junta de Comunidades de Castilla-La Mancha integre la protección frente a los riesgos de la IA en las políticas públicas de consumo y en el funcionamiento de los recursos públicos de consumo (oficinas, servicios de mediación, inspección y arbitraje).

En desarrollo del artículo 99, los Planes Estratégicos de Consumo que debe aprobar la consejería en cada legislatura podrían incorporar un capítulo específico sobre entornos digitales e IA. Dicho capítulo podría incluir: (i) Objetivos medibles (por ejemplo, "aumentar en un 30 % el nivel de comprensión de los consumidores sobre precios dinámicos personalizados en un plazo de cuatro años", con encuestas periódicas de seguimiento). (ii) Indicadores concretos de evaluación, como número de reclamaciones recibidas vinculadas a IA, número de inspecciones digitales realizadas o grado de satisfacción de los consumidores con las explicaciones recibidas sobre sistemas automatizados. (iii) Medidas transversales coordinadas a través de la Comisión Regional de Coordinación interdepartamental prevista en el artículo 99.3. Por ejemplo, esta Comisión podría aprobar protocolos comunes para vigilar la transparencia de las ofertas automatizadas, coordinar campañas conjuntas con la Consejería de Educación sobre alfabetización digital y establecer mecanismos de alerta temprana de prácticas comerciales engañosas basadas en IA.

Por su parte, el artículo 100 faculta a los recursos públicos de consumo para recibir y tramitar reclamaciones, realizar mediación y desarrollar actuaciones de vigilancia de mercado. Sobre esta base, podrían adoptarse medidas como: (i) Implantar un protocolo autonómico de reclamaciones vinculadas a decisiones automatizadas, que permita registrar en un formulario electrónico campos específicos como "precio personalizado", "denegación automatizada de servicio" o "clasificación/recomendación de productos". (iii) Incluir en las campañas anuales de vigilancia de mercado controles específicos sobre prácticas de IA. Por ejemplo, supervisar si los portales de comercio electrónico informan correctamente sobre personalización de precios, comprobar si los sistemas de recomendación respetan los principios de transparencia del TRLGDCU y detectar "patrones oscuros" en interfaces digitales. (iv) Capacitar al personal de las OMIC y oficinas supramunicipales en la identificación de conflictos relacionados con IA, mediante formación en derechos digitales. (v) Elaborar un Directorio de recursos de consumo especializados en IA, como permite el artículo 100.2, de forma que los ciudadanos sepan qué oficinas disponen de personal capacitado o de mediadores con experiencia en conflictos vinculados a decisiones automatizadas.

De este modo, Castilla-La Mancha podría, sin necesidad de reformar la Ley 3/2019, usar los artículos 99 y 100 para diseñar planes estratégicos con metas concretas y reforzar su red de recursos de consumo, dotándola de instrumentos específicos frente a los riesgos derivados de la IA.

3. Administración local

Los artículos 101 a 107 de la Ley 3/2019 ofrecen a las entidades locales un margen para intervenir en materia de consumo. En el terreno de la IA, la aplicación práctica debe adaptarse a la realidad de Castilla-La Mancha, donde predominan el pequeño comercio, las pymes y el consumo presencial, de modo que la IA incide sobre todo a través de plataformas digitales de alcance nacional o global a las que también acceden los consumidores locales.

En este marco, los ayuntamientos pueden centrar su acción en informar y canalizar reclamaciones. El artículo 101 les permite desarrollar campañas de sensibilización sencillas en materia digital, por ejemplo, incluir en sus programas de consumo mensajes sobre precauciones al comprar en línea, cómo identificar precios que pueden haber sido personalizados, etc.

Las OMIC, previstas en el artículo 102, son el cauce más eficaz para recoger incidencias. Su papel no sería auditar algoritmos, sino registrar reclamaciones vinculadas a sistemas automatizados y remitirlas a la Junta para su tratamiento conjunto.

El artículo 103 permite formalizar convenios de colaboración. En la práctica, podría articularse una red piloto con OMIC de capitales de provincia para concentrar los casos relacionados con IA, elaborar estadísticas comunes y facilitar que la Junta disponga de información consolidada.

La previsión de red y mapa de consumo de los artículos 104 y 105 podría aprovecharse para detectar patrones de reclamaciones en entornos digitales sin necesidad de exigir a cada municipio que despliegue capacidades técnicas específicas.

Finalmente, el artículo 107 sobre atención interdisciplinar permite que las OMIC que ya trabajan en ámbitos como la intermediación hipotecaria o la vulnerabilidad energética integren también un módulo básico de información sobre riesgos digitales y derechos frente a decisiones automatizadas, en colaboración con la Junta y con asociaciones de consumidores.

4. Vigilancia de mercado, inspección y sanción

En materia de IA, las competencias autonómicas en inspección y control del mercado presentan importantes limitaciones. La vigilancia de mercado, la evaluación de la conformidad y la potestad sancionadora respecto de los requisitos técnicos de los sistemas de IA corresponden a las autoridades estatales designadas en aplicación del AI Act y del futuro APLIA.

No obstante, el hecho de que el control técnico de los sistemas de IA corresponda a las autoridades estatales o sectoriales no excluye la actuación autonómica en el ámbito de la defensa de las personas consumidoras. El artículo 108 de la Ley 3/2019 atribuye a la Junta de Comunidades la realización de actuaciones de inspección, vigilancia y control de

mercado para comprobar que las empresas cumplen con la legislación vigente en materia de derechos e intereses de las personas consumidoras. Estas actuaciones incluyen la posibilidad de requerir información, realizar estudios, controles y análisis, y llevar a cabo inspecciones de todos los bienes y servicios puestos a disposición de los consumidores, con especial atención a los destinados a colectivos vulnerables.

En el ámbito de la IA en las relaciones de consumo, esta competencia puede traducirse en verificar que los empresarios que operan en la región informan de manera clara y comprensible cuando los precios han sido personalizados mediante decisiones automatizada, o que se facilitan los criterios generales que determinan la clasificación de productos o servicios en buscadores y plataformas en línea.

Además, los apartados 6 y 7 del artículo 108 obligan a la Junta a actuar coordinadamente con las corporaciones locales y otros órganos de inspección de la Administración autonómica, publicando anualmente un Plan de Inspección. Este instrumento puede incluir controles específicos sobre personalización de precios, priorización de ofertas, uso de sistemas de recomendación y cumplimiento de las obligaciones de transparencia en entornos digitales.

Los artículos 110 y 111 atribuyen al personal inspector amplias facultades para acceder a datos, documentos e incluso bases de datos relevantes, así como para realizar inspecciones in situ o efectuar compras de prueba. Estas potestades pueden emplearse para supervisar sistemas basados en tratamiento automatizado, por ejemplo, comprobando la transparencia de los sistemas de recomendación, la personalización de precios o la existencia y adecuación de mecanismos de intervención humana en decisiones automatizadas.

Cuando se detectan incumplimientos que afecten a consumidores de la región, la Comunidad Autónoma puede incoar y resolver procedimientos sancionadores. Sin embargo, el TRLGDCU establece que, en caso de infracciones que afecten de forma generalizada a consumidores en varias comunidades autónomas y comprometan la unidad de mercado, la competencia sancionadora pasa a la Administración General del Estado (artículo 52 bis.5 TRLGDCU). Asimismo, en sectores regulados, como crédito al consumo, servicios financieros o seguros, la potestad sancionadora corresponde a las autoridades supervisoras sectoriales (BdE, CNMV, DGSFP, etc.)[31].

En definitiva, aunque la Comunidad Autónoma no puede verificar la conformidad técnica de los sistemas de IA ni sancionar directamente el incumplimiento del AI Act, sí puede garantizar el respeto tanto de los derechos de información como del derecho a obtener intervención humana en decisiones automatizadas. Para ello puede actuar de manera preventiva mediante la vigilancia del mercado y, en su caso, sancionar las infracciones detectadas dentro de su ámbito competencial.

[31] Vid. E. CORDERO LOBATO, "Tipificación y concurrencia de infracciones de consumo", en Derecho de consumo: materiales, fundamentos, aplicaciones (Dir. Á. CARRASCO PERERA), 2023, Aranzadi, pp. 579-600.

5. Resolución extrajudicial

La Ley 3/2019 ya prevé herramientas de resolución extrajudicial (artículos 123 a 129) que pueden adaptarse sin grandes reformas para afrontar conflictos derivados del uso de sistemas de inteligencia artificial en el consumo.

5.1. Reclamaciones

En virtud del artículo 125, la Junta puede aprovechar la hoja de reclamaciones electrónica para incluir casillas específicas que permitan identificar si el problema del consumidor procede de una decisión automatizada (por ejemplo, la denegación de un crédito, una facturación automática errónea de la luz o el teléfono, o el rechazo automático de un pedido en una plataforma online). Esto no requiere crear un sistema nuevo, sino añadir esas categorías al formulario. Asimismo, puede exigirse que las empresas digitales faciliten un canal de contacto efectivo para reclamaciones —mediante una dirección postal o un correo electrónico claramente identificable—, evitando que la atención al consumidor quede reducida exclusivamente a un chatbot.

5.2. Mediación

El artículo 127 faculta a Castilla-La Mancha a promover que los conflictos relacionados con IA se resuelvan preferentemente mediante mediación. Para ello, puede informar a los consumidores de que, cuando sufran una denegación automatizada de un contrato, un precio personalizado o una clasificación opaca de ofertas, pueden acudir a mediación antes de plantear acciones judiciales. Las OMIC y las asociaciones de consumidores pueden recibir estas reclamaciones y derivarlas al sistema de mediación, del mismo modo que hacen con otros conflictos de consumo. En sectores de servicios básicos (electricidad, gas o telecomunicaciones), la Junta puede impulsar su utilización cuando los errores o controversias se originan en procedimientos automatizados, como puede ocurrir en casos de facturación errónea.

5.3. Arbitraje

La Junta de Comunidades de Castilla-La Mancha puede impulsar formación específica para los árbitros de consumo en relación con los derechos de las personas consumidoras cuando interactúan con sistemas de IA. Con esta medida, los árbitros estarán mejor preparados para valorar reclamaciones vinculadas a decisiones automatizadas, sin necesidad de crear órganos nuevos ni modificar la estructura del sistema arbitral existente (artículos 128 y 129).

6. Promoción: Información, formación y educación

Los artículos 130 a 135 de la Ley 3/2019 refuerzan el eje preventivo de la política de consumo mediante campañas informativas, estudios, educación y promoción de buenas prácticas. Este marco resulta especialmente adecuado para abordar los riesgos y oportunidades de la IA en las relaciones de consumo.

El artículo 130 obliga a la Administración regional a llevar a cabo campañas informativas y actividades de difusión para promover el conocimiento de los derechos de las personas consumidoras, en particular sobre nuevos bienes y servicios que puedan afectar a sus intereses económicos y sobre percepción de riesgos. En aplicación de este precepto, Castilla-La Mancha puede lanzar campañas de educación digital que expliquen qué es la personalización de precios, cómo funcionan los sistemas de recomendación en línea o cuáles son los derechos de los consumidores frente a decisiones automatizadas significativas.

El artículo 131 permite impulsar estudios y encuestas sobre hábitos de consumo, así como la creación de observatorios y foros de reflexión. Esto habilita la puesta en marcha de observatorios regionales de IA y consumo, con el fin de detectar patrones de riesgo en la personalización de ofertas, discriminaciones algorítmicas o problemas de accesibilidad digital para colectivos vulnerables.

El artículo 132 establece el deber de promover programas educativos en materia de consumo, con objetivos de formación crítica y libre elección. Este mandato puede concretarse en iniciativas de alfabetización algorítmica desarrolladas en colaboración con centros educativos, de modo que niños y jóvenes conozcan sus derechos cuando intervienen sistemas automatizados en el consumo digital, comprendan la lógica básica de estos procedimientos y dispongan de herramientas para tomar decisiones informadas.

El artículo 133 contempla la formación continua de consumidores, profesionales del consumo y agentes económicos. Aquí se abre la posibilidad de formar específicamente al personal de las OMIC y de la Inspección de Consumo sobre derechos digitales, transparencia algorítmica y protección frente a sesgos, de manera que puedan orientar y asesorar a los consumidores cuando intervengan sistemas automatizados en la contratación o prestación de servicios.

El artículo 134 se refiere expresamente a los nuevos modelos económicos emergentes y menciona de forma explícita la IA junto con otras tecnologías disruptivas. Este precepto obliga a la Administración regional a facilitar información, formación y educación para que la transición tecnológica no reduzca el empoderamiento de los consumidores. En aplicación de esta previsión, Castilla-La Mancha puede desarrollar campañas de información claras sobre el uso de algoritmos en la fijación de precios o en la priorización de ofertas en línea, así como acciones de formación básica dirigidas a colectivos con menor alfabetización digital para que reconozcan cuándo una decisión de consumo está mediada por IA y qué derechos de información y reclamación les asisten.

Finalmente, el artículo 135 impulsa la calidad y competitividad empresarial mediante instrumentos de autocontrol y códigos de buenas prácticas. Esto permite promover distintivos para empresas que implementen sistemas de IA transparentes y auditables, que garanticen explicaciones claras de sus decisiones automatizadas y respeten los derechos de las personas consumidoras, favoreciendo así la autorregulación responsable en el uso de algoritmos.

7. Cooperación

La cooperación interadministrativa constituye un elemento esencial para delimitar el papel de Castilla-La Mancha en la protección de los consumidores frente a los riesgos derivados de la IA. El marco normativo estatal y autonómico prevé de manera expresa la necesidad de colaboración entre distintos niveles de gobierno a fin de garantizar una protección uniforme y eficaz.

En el ámbito estatal, el TRLGDCU establece mecanismos de coordinación y colaboración entre las administraciones públicas competentes en materia de consumo, tanto en el plano normativo como en el de la inspección y el control de mercado. Ello habilita a Castilla-La Mancha a integrarse en órganos colegiados como la Conferencia Sectorial de Consumo y el Consejo de Consumidores y Usuarios, espacios en los que la Comunidad puede plantear la adaptación de la normativa y las prácticas de supervisión a los escenarios derivados de la contratación y la publicidad digital mediada por IA. Además, el TRLGDCU prevé la cooperación en actuaciones de inspección y control, lo que permite articular planes conjuntos con las autoridades estatales para detectar y sancionar infracciones vinculadas a sistemas automatizados, como la omisión de información sobre precios personalizados o recomendaciones algorítmicas.

En el plano europeo y nacional, el AI Act configura una gobernanza multinivel que requiere la cooperación de autoridades europeas, estatales y regionales para asegurar una aplicación uniforme de los requisitos armonizados. El APLIA se inserta en este esquema, previendo que las autoridades nacionales competentes cooperen con las autonómicas en los ámbitos sectoriales de su competencia. A partir de esta previsión, Castilla-La Mancha podría integrarse en redes nacionales de vigilancia de mercado, comunicar riesgos detectados en plataformas digitales que operen en su territorio, colaborar en la ejecución de sanciones y participar en programas de apoyo a la innovación, como los espacios controlados de prueba.

Desde la perspectiva autonómica, el Estatuto de Autonomía de Castilla-La Mancha reconoce en su artículo 32.6 la competencia de desarrollo legislativo y ejecución en materia de defensa de los consumidores, lo que se complementa con el artículo 9.2, que habilita expresamente la cooperación con otras administraciones públicas para la mejor protección de los derechos de los ciudadanos. Ello legitima a la Comunidad para integrarse en sistemas de información compartida sobre riesgos de la IA en el consumo,

participar en planes coordinados de inspección y control, y desarrollar programas conjuntos de educación y sensibilización digital junto a autoridades estatales y europeas.

En términos más concretos, Castilla-La Mancha podría participar en la Red de Alerta de Consumo, incorporando incidencias vinculadas a algoritmos de recomendación o precios personalizados. Colaborar con la AESIA en la detección de infracciones relacionadas con la contratación digital. Desarrollar observatorios autonómicos de IA y consumo en coordinación con el Ministerio de Transformación Digital, alimentando bases de datos compartidas. Firmar convenios de cooperación con otras comunidades autónomas para intercambiar buenas prácticas sobre educación digital y arbitraje de consumo en entornos automatizados. Impulsar, en colaboración con la UE y el Estado, campañas conjuntas de información sobre el uso de IA en la publicidad digital dirigida a colectivos vulnerables.

En definitiva, la cooperación interadministrativa permite a Castilla-La Mancha desempeñar un papel activo en la protección de los consumidores frente a la IA, siempre dentro de sus competencias, reforzando los mecanismos de información, transparencia y control y garantizando que la tutela de los consumidores se integre en una estrategia coherente a escala nacional y europea.

V. CUADRO COMPARATIVO COMPETENCIAS: UE, ESTADO, CASTILLA-LA MANCHA

Nivel	Base competencial	Competencias materiales	Límites competenciales
Unión Europea	- Artículos 4.2 f), 12 y 169 TFUE (protección del consumidor). - Artículo 114 TFUE (armonización para el mercado interior). - Artículo 5.3 TUE (subsidiariedad).	- Armoniza la protección de consumidores mediante directivas de armonización plena (p. ej. Dir. 2019/2161 → artículos 20.1 c), 20.3, 97.1 f), 97 bis TRLGDCU). - Aprueba reglamentos directamente aplicables que afectan a riesgos de IA: RGPD, RSD, RMD, AI Act. - El AI Act fija requisitos técnicos y de uso de sistemas de IA y crea la gobernanza europea.	-Principio subsidiariedad (artículo 5.3 TUE).
Estado español	- Artículos 51, 148 y 149 CE. - Títulos del	- Competencia Derecho civil, mercantil y procesal: TRLGDCU, LCCC, LCCI,	- Debe respetar el Derecho de la UE: no puede contradecir ni

Nivel	Base competencial	Competencias materiales	Límites competenciales
	artículo 149.1 CE (1, 6, 8, 11, 13, 16, 18).	Ley 22/2007, Ley 4/2012, Orden EHA/2899/2011. - Desarrollo del AI Act en los aspectos que este remite a los Estados: régimen sancionador, autoridades notificantes y de vigilancia, gobernanza nacional, alfabetización y espacios de prueba (APLIA).	completar la armonización plena de las directivas. -En reglamentos, no existe margen nacional salvo excepciones previstas (p. ej. artículo 8 RGPD). - Su actuación en IA se limita a lo delegado por el AI Act.
Castilla-La Mancha	- Artículo 32.6 EACM. - Ley 3/2019, de 22 de marzo.	- Desarrollo legislativo y ejecución en protección de consumidores dentro del marco estatal. – Alfabetización, formación, inspección, vigilancia, sanciones, mediación, arbitraje y planificación de servicios públicos de consumo.	- No puede modificar obligaciones de información armonizadas (artículos 20.3, 97.1 f), 97 bis TRLGDCU). - No puede regular contratos, proceso, unidad de mercado ni requisitos técnicos de IA (competencias estatales/UE). - Su margen de actuación se limita a información, alfabetización, inspección, cooperación y ejecución de la normativa estatal y europea.

VI. MAPA INSTITUCIONAL DE LA GOBERNANZA EN MATERIA DE IA

Nivel / Órgano	Naturaleza / Base jurídica	Funciones según AI Act / APLIA	Ámbito de actuación
Oficina de IA (UE)	Órgano técnico de la Comisión Europea	Coordinar la aplicación del AI Act; asistencia técnica a Estados; apoyo a vigilancia del mercado; desarrollo de capacidades técnicas;	Unión Europea

Nivel / Órgano	Naturaleza / Base jurídica	Funciones según AI Act / APLIA	Ámbito de actuación
	(artículo 64 AI Act)	cooperación con autoridades nacionales.	
Consejo Europeo de IA	Foro de coordinación (artículos 65–66 AI Act)	Facilitar aplicación coherente del AI Act; coordinar autoridades nacionales; emitir recomendaciones y dictámenes; promover alfabetización; organizar subgrupos permanentes; apoyar vigilancia de mercado.	Unión Europea + Estados miembros
Foro consultivo	Órgano de participación (artículo 67 AI Act)	Representación equilibrada de partes interesadas; asesoramiento al Consejo y a la Comisión; elaboración de informes, dictámenes y subgrupos de trabajo.	Unión Europea
Grupo de expertos científicos independientes	Designado por la Comisión (artículo 68 AI Act)	Identificar riesgos sistémicos de modelos GPAI; desarrollar herramientas de evaluación; apoyar vigilancia de mercado; asistencia técnica transfronteriza; colaboración a petición de Estados (artículo 69 AI Act).	Unión Europea + apoyo a los Estados
Secretaría de Estado de Digitalización e IA (España)	Autoridad notificante (artículo 28.1 AI Act; artículos 4.1–4.4 APLIA)	Establecer y ejecutar procedimientos para evaluar, designar y notificar organismos de evaluación de conformidad; supervisarlos; potestad sancionadora; retirar designaciones; designar representante en el Consejo de IA; comunicar autoridades de vigilancia del mercado (artículo 70.2 AI Act).	Estado miembro – España
ENAC (España)	Organismo nacional de acreditación (artículo 28.2 AI Act; artículo 4.3 APLIA)	Evaluación y supervisión de organismos notificados; retirada de designaciones cuando no cumplan requisitos.	Estado miembro – España
Autoridades de vigilancia del	Autoridades designadas por	Vigilancia, inspección y sanción de sistemas de IA; control de	Ámbito nacional, según

Nivel / Órgano	Naturaleza / Base jurídica	Funciones según AI Act / APLIA	Ámbito de actuación
mercado (generales)	el Estado (artículos 70–82 AI Act; artículos 6–8 APLIA)	proveedores, fabricantes, distribuidores, responsables del despliegue, importadores; actuación según Cap. IX AI Act; coordinación interadministrativa; uso de Safety Gate y sistemas de información.	competencia sectorial
AESIA	Agencia estatal (RD 729/2023; artículos 6.2, 6.7, 6.12, 6.14, 6.15, 9 APLIA)	Punto de contacto único (artículo 70.2 AI Act); autoridad de vigilancia para IA prohibida y alto riesgo en los ámbitos previstos en artículo 6.2 APLIA; supervisión residual cuando falta capacidad técnica de autoridades sectoriales; medidas urgentes ante incidentes; asistencia técnica; coordinación; creación del sandbox (artículo 57.1 AI Act).	Vigilancia del mercado en IA (ámbitos definidos en APLIA)
AEPD y autoridades autonómicas de protección de datos	Autoridades de vigilancia sectorial (artículo 6.3 APLIA)	Supervisión de IA prohibida en ámbitos d), g), h) del artículo 5.1 AI Act; vigilancia de sistemas de alto riesgo de biometría, cumplimiento del derecho, gestión fronteriza, migración y asilo (Anexo III AI Act).	Protección de datos, seguridad pública y fronteras
BdE y CNMV	Autoridades financieras (artículo 6.4 APLIA)	Vigilancia de sistemas de IA de alto riesgo en evaluación de solvencia y calificación crediticia (Anexo III.5 b) AI Act).	Sector financiero
DGSFP	Autoridad aseguradora (artículo 6.5 APLIA)	Vigilancia de sistemas de IA de alto riesgo para evaluación de riesgos y fijación de precios en seguros de vida y salud (Anexo III.5 c) AI Act).	Sector seguros
Dirección de Supervisión y Control de Protección de Datos del CGPJ	Autoridad judicial específica (artículo 6.6 APLIA)	Vigilancia de sistemas de IA en administración de justicia (Anexo III.8.a) AI Act) y prácticas prohibidas en este ámbito.	Administración de justicia
Junta Electoral Central	Autoridad en procesos democráticos	Vigilancia de IA de alto riesgo en procesos democráticos (Anexo	Procesos electorales

Nivel / Órgano	Naturaleza / Base jurídica	Funciones según AI Act / APLIA	Ámbito de actuación
	(artículo 6.6 APLIA)	III.8.b) AI Act) y prácticas prohibidas vinculadas.	
Autoridades sectoriales de vigilancia del mercado (productos armonizados)	Autoridades previstas en actos legislativos de armonización (artículo 74.3 AI Act)	Vigilancia de IA de alto riesgo asociada a productos regulados por la legislación armonizada de la UE.	Sectores armonizados (producto)
AESIA (competencia residual)	Suplencia cuando no hay medios suficientes (artículo 6.7 APLIA)	Asume supervisión, inspección y sanción cuando la autoridad sectorial carece de medios técnicos/financieros/humanos.	Supervisión subsidiaria
Secretaría de Estado de Digitalización e IA	En nuevos ámbitos (artículo 7.8 APLIA)	Puede designar nuevas autoridades de vigilancia del mercado si la Comisión abre nuevos ámbitos de supervisión de IA.	Ámbitos adicionales creados por actos delegados de la Comisión
Comisión mixta de coordinación de autoridades de vigilancia del mercado	Órgano interno de coordinación (artículo 8.5 APLIA)	Asegurar coordinación interadministrativa; intercambio de información; seguimiento de actuaciones; elaboración del informe anual del artículo 5 y 6 AI Act.	España (coordinación estatal)

CAPÍTULO III. RIESGOS REALES DE LA IA PARA CONSUMIDORES Y NORMATIVA APLICABLE

I. LA INTELIGENCIA ARTIFICIAL EN LAS RELACIONES DE CONSUMO

La IA se utiliza en algunos aspectos concretos de la contratación con consumidores, pero su presencia real sigue siendo todavía limitada, aunque se prevé que aumente con el paso del tiempo. Los usos de la IA en la contratación de consumo que se describen a continuación son precisamente aquellos previstos por la normativa europea y española, que ha identificado en ellos riesgos relevantes para los consumidores y, en consecuencia, ha impuesto obligaciones específicas a los comerciantes para prevenir o mitigar dichos riesgos.

El uso más habitual de la IA en la contratación de consumo es la personalización, mediante tratamientos automatizados de datos personales, ya sea de contenidos, publicidad, ofertas o precios. El entorno digital se caracteriza cada vez más por la generación, acumulación y control de enormes cantidades de datos sobre los consumidores, que pueden combinarse con algoritmos e IA para transformarlos en información utilizable con fines comerciales. Entre otros fines, estos datos permiten obtener una visión detallada de características sociodemográficas (como edad, género o situación financiera) y de características personales o psicológicas (como intereses, preferencias, perfil psicológico o estado de ánimo). Esto posibilita que los comerciantes conozcan mejor a los consumidores, incluso sus posibles vulnerabilidades.

Las prácticas de personalización basadas en datos incluyen la publicidad dirigida, los sistemas de recomendación, la fijación personalizada de precios, la clasificación de ofertas en los resultados de búsqueda, entre otras. Esta personalización mediante la combinación de datos personales y algoritmos también influye en la evaluación de la solvencia o el riesgo asegurador y condicionan la celebración de contratos como créditos, pólizas de seguro o líneas de telefonía.

Además de estos procesos de personalización a través del tratamiento automatizado de datos personales, la IA interviene también en la interacción directa con los consumidores durante la relación contractual. Es habitual el uso de chatbots y asistentes conversacionales en la fase precontractual —tanto para obtener información como para configurar la oferta— y, sobre todo, en la fase poscontractual, especialmente en la atención al cliente y la gestión de reclamaciones.

Asimismo, se emplean bots automatizados para acaparar entradas de eventos y otros productos con fines de reventa, así como para generar reseñas falsas de bienes y servicios y sus proveedores.

Por otra parte, algunos bienes de consumo incorporan ya sistemas de IA integrados en su funcionamiento, especialmente en productos con elementos digitales conectados. En

estos casos, la conformidad del bien depende tanto de sus características materiales como del comportamiento del componente digital y del sistema de IA que integra. Fallos en los algoritmos, pérdida de funcionalidades tras una actualización, problemas de interoperabilidad o interrupciones del soporte digital pueden afectar a la conformidad del bien durante su vida útil y activar las garantías previstas para este tipo de productos.

Por último, aunque en rigor no forma parte del Derecho contractual de consumo, pueden surgir problemas específicos de responsabilidad civil extracontractual del fabricante derivados de sistemas de IA defectuosos que causen ciertos daños personales o materiales a los consumidores.

Los apartados siguientes analizan cada uno de estos ámbitos con el fin de identificar los principales riesgos que plantean para los consumidores y examinar la normativa aplicable. El objetivo es ofrecer un marco sistemático que permita comprender cómo se articulan las diferentes obligaciones de los empresarios y los derechos de los consumidores en relación con el uso de sistemas de IA, y valorar en qué medida estas normas resultan adecuadas para abordar los problemas detectados.

II. PERSONALIZACIÓN

1. Contenidos, anuncios, ofertas

1.1. Riesgos

Las plataformas en línea pueden utilizar sistemas de recomendación y publicidad personalizada para mostrar contenidos, información y ofertas priorizadas en función del perfil del consumidor. Esta personalización se basa en tratamientos automatizados de datos personales —historial de navegación o de compras, ubicación, interacciones en línea, características inferidas del comportamiento, etc.— que permiten predecir intereses y decidir qué información, anuncio u oferta se muestra primero. En particular, los modelos de negocio de las plataformas en línea van desde el mero hecho de permitir a los usuarios buscar información facilitada por terceros hasta permitir directamente las transacciones de carácter contractual entre terceros comerciantes y consumidores. Las plataformas también pueden anunciar y vender, en su propio nombre, diferentes tipos de productos.

Estas técnicas pueden facilitar la búsqueda de productos o servicios, reducir el tiempo necesario para decidir y evitar la exposición a anuncios irrelevantes. Para las empresas, incrementan la eficacia del marketing y la probabilidad de que el usuario interactúe con el contenido o realice una compra. Un estudio sobre personalización mostró que los principales beneficios percibidos por los consumidores son ver productos y descuentos relevantes, reducir anuncios irrelevantes y posibilitar la existencia de servicios en línea “gratuitos”. Sin embargo, la personalización también plantea riesgos, pues pueden limitar la diversidad de la información disponible, influir en la decisión de compra mediante

formas de persuasión o manipulación difíciles de detectar, generar tratos desiguales o discriminatorios al mostrar ofertas diferentes a cada usuario y exigir un tratamiento intensivo de datos personales que aumenta el riesgo de recopilación excesiva o de usos no esperados por el consumidor. Las principales preocupaciones se centran en la recopilación, uso y compartición de datos personales y en la imposibilidad de rechazar la personalización. El estudio reveló, además, niveles de concienciación significativamente más bajos entre consumidores vulnerables, como personas mayores, con menor nivel educativo o menor experiencia en compras en línea[32].

Por su parte, en 2024, la Comisión ha confirmado la persistencia de estos riesgos a través de la realización de una encuesta: el 41 % de los consumidores indicó dificultades para comprender cómo se utilizarían sus datos personales debido al diseño o lenguaje del sitio web o aplicación; el 37 % tuvo la impresión de que la empresa conocía sus vulnerabilidades y las utilizaba con fines comerciales; el 34 % declaró no poder rechazar ofertas comerciales personalizadas; el 38 % tuvo dificultades para comprender el "perfil" creado a partir de sus datos y cómo afectaba al contenido mostrado, problema especialmente intenso entre quienes apuestan en línea; y el 37 % encontró dificultades para cambiar sus preferencias de uso de datos personales debido al diseño de la interfaz.[33]

Las prácticas de personalización son empleadas por: redes sociales como Facebook, Instagram, TikTok, que determinan algorítmicamente el contenido del feed y los anuncios; empresas que venden bienes o servicios en su propia web o aplicación, como Zara, Ikea o Iberia, que recomiendan productos según el historial de navegación o compras; plataformas y marketplaces como Amazon, AliExpress, Booking o Expedia, que priorizan y personalizan los resultados de búsqueda; plataformas de contenidos y streaming, como Netflix, HBO Max, Disney+ o Spotify, que sugieren contenidos en función del historial de uso; y buscadores como Google o Bing, que personalizan resultados de búsqueda en función del historial, la ubicación y la interacción previa. Es muchos de estos casos puede afectar a menores, lo que se encuentra prohibido por el artículo 28 DSA.

Como ha señalado la Comisión, la publicidad, la clasificación y las recomendaciones personalizadas están ampliamente extendidas. No obstante, el grado de dependencia de la personalización varía según el tamaño del comerciante. En la encuesta empresarial realizada, integrada principalmente por pymes, el 76 % indicó no recopilar datos personales de consumidores. Entre quienes sí los utilizaban, el 31 % los empleaba para

[32] Danish Competition and Consumer Authority. "Consumers benefit from visually salient standardized commercial disclosures on social media", 2021, pp. 11–13. Disponible en: https://www.kfst.dk/media/z3lmycgw/20210617-consumers-benefit-from-visually-salient-standardized-commercial-disclosures-on-social-media.pdf

[33] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.

decidir qué ofertas destacar, el 30 % para adaptar o personalizar la publicidad y el 18 % para personalizar precios[34].

1.2. Marco normativo

1.2.1. Protección de datos

El RGPD se puede aplicar a la personalización y a los sistemas de recomendación, ya que se basan en el tratamiento automatizado de datos personales y, por lo general, en la elaboración de perfiles, definida en el artículo 4.4 RGPD como el uso de datos personales para evaluar o predecir aspectos relativos a las preferencias, intereses o comportamientos de una persona física. El RGPD no prohíbe estas prácticas, pero impone un marco estricto de licitud, transparencia y control.

Las obligaciones recaen sobre el responsable del tratamiento, que es quien decide para qué y cómo se tratan los datos (artículo 4.7 RGPD). En este ámbito pueden ser responsables tanto los empresarios en línea que venden directamente al consumidor, como Zara, las plataformas y marketplaces, como Amazon o Booking, los servicios de streaming, como Netflix o Spotify, los buscadores como Google o las redes sociales como Instagram o TikTok.

El artículo 22 RGPD reconoce al interesado el derecho a no ser objeto de una decisión basada únicamente en tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, salvo que haya dado su consentimiento explícito. Además, no pueden utilizarse categorías especiales de datos personales para la personalización, salvo que el interesado consienta expresamente o exista habilitación legal y se adopten las debidas garantías.

Aunque es dudoso si la recomendación de contenidos, anuncios u ofertas constituye una "decisión automatizada que produzca efectos jurídicos o afecte significativamente de modo similar", en el sentido del artículo 22, puede sostenerse que lo es cuando el sistema determina de forma autónoma qué información, productos o anuncios se muestran o se ocultan, condicionando así de manera significativa el acceso del usuario a ofertas y contenidos relevantes. En este sentido, el Comité Europeo de Protección de Datos ha considerado que la publicidad dirigida también puede estar sujeta a las normas sobre decisiones automatizadas del artículo 22 del RGPD[35].

Por otro lado, los artículos 13.2.f, 14.2.g y 15.1.h RGPD reconocen al interesado el derecho a ser informado de la existencia de decisiones automatizadas, incluida la

[34] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.
[35] "Directrices 8/2020 sobre la focalización de los usuarios de medios sociales", ejemplo 8 y apartados 85 a 88. Disponible en: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_ en.pdf.

elaboración de perfiles, y a obtener "información significativa sobre la lógica aplicada", así como sobre la importancia y las consecuencias previstas de dicho tratamiento. Esta obligación de transparencia permite al consumidor conocer cómo funcionan los sistemas que personalizan su experiencia y comprender su impacto en la información que recibe. También destaca el artículo 25, referente a la protección de datos desde el diseño.

La STJUE de 27 de febrero de 2025, asunto C-203/22, *Dun & Bradstreet,* que refuerza el derecho a explicaciones claras y accesibles, ha precisado que la información significativa debe describir los procedimientos y principios en los que se basa el tratamiento automatizado de datos, de forma concisa, inteligible y accesible, en lenguaje claro y, preferiblemente, con ejemplos reales y tangibles. No es suficiente ofrecer fórmulas matemáticas o explicaciones técnicas que solo un experto pueda comprender. El objetivo es que el interesado entienda qué datos se han utilizado y cómo se han empleado para recomendarle o priorizar cierto contenido u oferta, de modo que pueda ejercer de manera efectiva los derechos que le reconoce el artículo 22[36].

En conclusión, cuando el consumidor es objeto de un sistema de recomendación de contenidos u ofertas comerciales basado en el tratamiento automatizado de datos personales, el responsable debe informarle de los parámetros generales o la lógica utilizada para generar la recomendación. Esta información debe ser clara, comprensible y fácilmente accesible para que el consumidor pueda comprender que datos se están tratando por el sistema de recomendación.

Ahora bien, el RGPD resulta insuficiente para hacer frente a muchos de los problemas que plantea la recomendación automatizada de contenidos, bienes y servicios, pues no está claro si estas prácticas constituyen decisiones en el sentido del artículo 22. Además, este artículo sólo se aplica a decisiones exclusivamente automatizadas con efectos jurídicos o similares, y no a decisiones parcialmente automatizadas. Por ello, el legislador de la Unión ha aprobado normas que regulan de manera más específica estas cuestiones, como veremos a continuación.

1.2.2. Equidad y transparencia para usuarios profesionales de plataformas

El Reglamento (UE) 2019/1150 impone obligaciones de transparencia sobre la priorización de bienes, servicios y sitios web en favor de los usuarios profesionales que operan en plataformas y motores de búsqueda. Aunque estas obligaciones se dirigen formalmente a usuarios profesionales, los criterios de transparencia que establecen pueden extrapolarse conceptualmente al ámbito del consumo, pues abordan problemas estructurales —como la opacidad en la clasificación o la influencia de pagos en el posicionamiento— que también afectan a los consumidores.

[36] Martín Faba, J. M.ª, "La información sobre la lógica aplicada en el credit scoring automatizado: fácil, concisa y sin tecnicismos" (2025). Revista CESCO De Derecho De Consumo, 54, 3025, 15-30. Es preciso añadir que la aplicabilidad a recomendaciones es discutida, pero reforzada por el Comité Europeo de Protección de Datos.

Los proveedores de servicios de intermediación en línea (*vid*. artículo 2.2), como Amazon o eBay, deben incluir en sus condiciones generales los parámetros principales que determinan la clasificación de los bienes o servicios y explicar por qué unos tienen mayor importancia que otros (artículo 5.1). Si el proveedor permite que los usuarios profesionales influyan en la clasificación mediante remuneración directa (pagos) o indirecta (uso de servicios premium o logísticos), debe indicarlo de forma clara y explicar sus efectos en el posicionamiento (artículo 5.3).

De forma similar, los motores de búsqueda como Google o Bing están obligados a publicar, en un lugar de acceso fácil y público, una descripción sencilla de los parámetros más relevantes para la clasificación de sitios web corporativos y su importancia relativa (artículo 5.2). También deben informar si la apariencia o el diseño del sitio web (por ejemplo, su optimización para móviles) influye en el ranking (artículo 5.5).

En ningún caso se exige revelar el algoritmo ni información que pueda facilitar la manipulación de resultados (artículo 5.6), pero la descripción debe permitir a los usuarios profesionales comprender cómo afectan las características de sus productos o servicios a su posición en el ranking.

La Comisión ha publicado unas directrices sobre la transparencia de la clasificación de conformidad con dicho Reglamento. Estas directrices abordan varias cuestiones relativas a la transparencia de la clasificación, como el concepto de "parámetros principales", "preeminencia relativa" y "remuneración directa e indirecta"[37].

En conclusión, el Reglamento (UE) 2019/1150 obliga a las plataformas y motores de búsqueda a ofrecer información clara, accesible y actualizada sobre los parámetros de priorización utilizados en la clasificación de bienes, servicios y sitios web. Aunque este marco se dirige exclusivamente a las relaciones con usuarios profesionales, los principios de transparencia que incorpora constituyen un referente útil y potencialmente extrapolable al ámbito del consumo, al abordar fenómenos idénticos de opacidad en la ordenación de resultados y en la influencia de pagos sobre el posicionamiento.

1.2.3. Información básica en la oferta de bienes y servicios

De manera complementaria, el artículo 20.3 TRLGDCU, reformado con ocasión de la transposición de la Directiva (UE) 2019/2161, que introduce obligaciones específicas en materia de transparencia en clasificaciones[38] (normas de armonización plena), establece

[37] Comunicación de la Comisión. "Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo" (DO C 424 de 8.12.2020).

[38] A través del Real Decreto-ley 24/2021, de 2 de noviembre, de transposición de directivas de la Unión Europea en las materias de bonos garantizados, distribución transfronteriza de organismos de inversión colectiva, datos abiertos y reutilización de la información del sector público, ejercicio de derechos de autor y derechos afines aplicables a determinadas transmisiones en línea y a las retransmisiones de programas de

que las prácticas comerciales consistentes en ofrecer a los consumidores la posibilidad de buscar bienes y servicios ofertados por distintos empresarios o consumidores sobre la base de una consulta en forma de palabra clave, expresión u otro tipo de dato introducido, independientemente de dónde se realicen las transacciones en último término, deberán contener, en una sección específica de la interfaz en línea que sea fácil y directamente accesible desde la página en la que se presenten los resultados de la búsqueda, la siguiente información: a) Información general relativa a los principales parámetros que determinan la clasificación de los bienes y servicios presentados al consumidor y usuario como resultado de la búsqueda. b) La importancia relativa de dichos parámetros frente a otros. Estos conceptos serán explicados en el epígrafe siguiente, cuando se analice el artículo 97 bis, que contiene una obligación similar.

Lo criticable es que el precepto genera un nivel de transparencia desigual para el consumidor en función del modelo de negocio del comerciante. Mientras que los mercados en línea[39] deben revelar los parámetros que determinan la clasificación de los resultados —lo que permite al usuario comprender por qué ciertos productos aparecen primero—, los comercios que solo muestran productos propios no están sujetos a esta obligación, pese a que también organizan y priorizan los bienes que ofrecen. Además, el requisito de información sólo se aplica a los comerciantes cuando el consumidor realiza una consulta. En cambio, no se aplica a la organización predeterminada de la interfaz en línea que se muestra al consumidor y que no es el resultado de una consulta específica en esa interfaz en línea. Además, la obligación de transparencia no se extiende a los motores de búsqueda en línea, ya cubiertos por una obligación similar en el Reglamento (UE) 2019/1150, adoptado con anterioridad. El resultado es una asimetría regulatoria difícil de justificar desde la perspectiva del consumidor, pues la necesidad de transparencia en la presentación de los productos no depende de que procedan de distintos comerciantes, sino de que la ordenación influye directamente en la decisión de compra.

1.2.4. Contratos a distancia: Requisitos de información específicos adicionales para contratos celebrados en mercados en línea

Los motores de búsqueda permiten buscar información en internet con arreglo a un algoritmo específico. Otros intermediarios, como los mercados en línea y los servicios de comparación de precios, ofrecen también la posibilidad de buscar entre los diferentes productos y proveedores accesibles a través de sus servicios. Los consumidores esperan que los resultados de las búsquedas sean "naturales" u "orgánicos" y se basen en criterios suficientemente imparciales. Sin embargo, los proveedores también incluyen en los

radio y televisión, exenciones temporales a determinadas importaciones y suministros, de personas consumidoras y para la promoción de vehículos de transporte por carretera limpios y energéticamente eficientes.

[39] Según artículo 59 bis 3 TRLCU, se considera "mercado en línea" un servicio que emplea programas (software), incluidos un sitio web, parte de un sitio web o una aplicación, operado por el empresario o por cuenta de éste, que permite a los consumidores o usuarios celebrar contratos a distancia con otros empresarios o consumidores, y se considera "proveedor de un mercado en línea" a todo empresario que pone a disposición de los consumidores o usuarios un mercado en línea".

resultados de las búsquedas publicidad de pago o mejoran la clasificación de los productos debido al pago directo o indirecto que reciben de los terceros comerciantes pertinentes.

El artículo 97 bis. 1 a) TRLGDCU, modificado también con ocasión de la transposición de la Directiva (UE) 2019/2161, introduce obligaciones para los mercados en línea, que, como hemos explicado, son plataformas en línea que permiten a los clientes comprar productos ofrecidos por terceros proveedores (comerciantes o consumidores) directamente en la interfaz del mercado (artículo 59 bis 3 TRLCU). El "mercado en línea" es un concepto neutro desde el punto de vista tecnológico, que también incluye tiendas de aplicaciones que suministran contenidos y servicios digitales[40].

Así, el citado precepto establece que, antes de que el consumidor quede obligado por un contrato a distancia, o cualquier oferta correspondiente, en un mercado en línea, el proveedor del mercado le facilitará la siguiente información de forma clara, comprensible y adecuada a las técnicas de comunicación a distancia: a) Información general, facilitada en la sección específica interfaz en línea que sea fácil y directamente accesible desde la página en la que se presenten las ofertas, relativa a: (i) Principales parámetros que determinan la clasificación, de las ofertas presentadas al consumidor como resultado de la búsqueda y (ii) la importancia relativa de dichos parámetros frente a otros parámetros.

Con esta regla se trata de evitar que, en plataformas como Amazon o Booking, el consumidor crea que los primeros resultados de su búsqueda son los más relevantes o mejores para sus intereses, cuando en realidad aparecen en primer lugar porque, por ejemplo, el vendedor ha pagado una comisión más alta a la plataforma. Así, el consumidor puede saber si lo que está viendo responde a criterios objetivos de calidad o precio, o simplemente a un pago por posicionamiento u otra circunstancia.

Como en el caso anterior, el ámbito de esta disposición no cubre a los comerciantes que permiten a los consumidores buscar únicamente entre sus propias ofertas de distintos productos, ni se aplica a la clasificación dentro de la organización predeterminada de la interfaz en línea que no deriva de una consulta de búsqueda concreta. La obligación de transparencia no se extiende a los motores de búsqueda en línea, ya cubiertos por una obligación similar en el Reglamento (UE) 2019/1150.

Por lo que se refiere al contenido de la información, la plataforma debe proporcionar información "general", facilitada en la sección específica interfaz en línea en la que se presenten las ofertas, sobre los "parámetros principales" que determinan la clasificación de los productos y sobre la "importancia relativa" de dichos parámetros con respecto a otros.

Estas normas sobre la transparencia de la clasificación hacia los consumidores definen la "clasificación" en términos sustancialmente similares a los del Reglamento (UE)

[40] 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).

2019/1150. Dicho Reglamento obliga a las plataformas a informar a los usuarios profesionales a través de la información contenida en las condiciones generales de las relaciones entre empresas de la plataforma, o a facilitar la información en la fase precontractual. Con todo, el artículo 97 bis TRLCU requiere que esta información se encuentre accesible directa y fácilmente en el interfaz donde se presentan las ofertas, para que así el consumidor pueda tener esta información antes de realizar una concreta transacción. La información deberá facilitarse de manera clara, comprensible y adecuada a los medios de comunicación a distancia.

La obligación de información también se aplica cuando un comerciante permite realizar búsquedas en una interfaz en línea mediante comandos por voz (a través de "asistentes digitales"), en lugar de tecleando. También en este caso, la información debe estar disponible para su consulta en el sitio web o la aplicación del comerciante "en una sección específica de la interfaz en línea"[41].

Aunque los requisitos de información de los dos cuerpos normativos (TRLGDCU y Reglamento (UE) 2019/1150) son similares, sus "públicos" son diferentes. Por este motivo, las disposiciones del TRLGDCU solo requieren información "general" sobre los principales parámetros de clasificación y su importancia relativa. La descripción de los parámetros de clasificación por defecto puede mantenerse en un nivel general y no es necesario que se presente de un modo personalizado para cada una de las consultas concretas efectuadas[42]. Esta diferencia con respecto al Reglamento (UE) 2019/1150 refleja las necesidades de información de los consumidores, que necesitan información concisa y fácil de comprender. En efecto, según el considerando 22 de la Directiva (UE) 2019/2161, "[p]or parámetros que determinan la clasificación se entienden los criterios generales, procesos, señales específicas incorporadas en los algoritmos u otros mecanismos de ajuste o degradación que se utilicen en la clasificación". Por la misma razón, las normas del TRLGDCU tampoco requieren una explicación de los "motivos" de la "importancia relativa de los principales parámetros" de clasificación que exige el Reglamento (UE) 2019/1150.

La información sobre la clasificación se entiende sin perjuicio de lo dispuesto en la Directiva (UE) 2016/943 sobre secretos comerciales. Como se explica en la obligación paralela de transparencia de la clasificación para todas las plataformas en línea y los motores de búsqueda en línea establecida en el artículo 5 del Reglamento (UE) 2019/1150, esto significa que la consideración de los intereses comerciales de los proveedores pertinentes nunca debe dar lugar a la negativa a revelar los parámetros principales que determinan la clasificación. Al mismo tiempo, ni la Directiva (UE) 2016/943 ni el Reglamento (UE) 2019/1150 obligan a la divulgación del funcionamiento detallado de los mecanismos de clasificación de los proveedores pertinentes, incluidos

[41] 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).
[42] *Vid*. considerando 23 de la Directiva (UE) 2019/2161.

sus algoritmos[43]. El mismo enfoque se aplica al requisito de información en virtud de la Directiva (UE) 2019/2161[44].

1.2.5. Prácticas desleales

La Directiva 2005/29/CE tiene un ámbito de aplicación amplio, pues cubre la totalidad de las transacciones entre empresas y consumidores, tanto en línea como fuera de ella. Es neutra desde el punto de vista tecnológico y se aplica con independencia del canal, medio o dispositivo utilizado para llevar a cabo la práctica comercial de las empresas en sus relaciones con los consumidores. Se aplica a los intermediarios en línea, incluidos las redes sociales, los mercados en línea y las tiendas de aplicaciones, los motores de búsqueda, las herramientas comparativas y otros comerciantes que operan en el sector digital. La Directiva 2005/29/CE se aplica también a las prácticas y los productos que implican el uso de tecnologías como algoritmos, decisiones automatizadas e IA. Esto incluye todas las prácticas de las empresas en sus relaciones con los consumidores adoptadas por los comerciantes en relación con los consumidores en las fases publicitaria, de venta y posventa, como el uso de tecnologías de seguimiento y selección, personalización algorítmica, optimización dinámica y tecnologías de registro descentralizado[45].

Según el artículo 26.2 LCD, introducido con ocasión de la transposición de la Directiva (UE) 2019/2161, que modifica a su vez la Directiva 2005/29/CE, se consideran desleales por engañosas las prácticas que: Faciliten resultados de búsquedas en respuesta a las consultas en línea efectuadas por un consumidor o usuario sin revelar claramente cualquier publicidad retribuida o pago dirigidos específicamente a que los bienes o servicios obtengan una clasificación superior en los resultados de las búsqueda, entendiendo por clasificación la preeminencia relativa atribuida a los bienes o servicios, en su presentación, organización o comunicación por parte del empresario, independientemente de los medios tecnológicos empleados para dicha presentación, organización o comunicación.

Se trata de evitar prácticas como las analizadas en el caso Google Shopping[46], en las que el buscador otorgaba sistemáticamente una posición de ventaja a sus propios servicios de comparación de precios respecto de los de terceros, presentándolos como si se tratara de resultados de búsqueda no promocionados. Para el consumidor medio, esto implicaba que los primeros productos que visualizaba no respondían necesariamente a criterios de

[43] *Vid*. considerandos 23 Directiva (UE) 2019/2161 y 27 Reglamento (UE) 2019/1150.
[44] Comunicación de la comisión. Directrices sobre la interpretación y la aplicación de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo sobre los derechos de los consumidores (2021/C 525/01, 29.12.2021).
[45] 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).
[46] En este sentido, es destacable la Decisión de la Comisión Europea de 27 junio 2017 (AT.39740), respecto a la imposición de una multa de 2.420 millones de euros.

relevancia, calidad o precio, sino a un tratamiento preferencial vinculado a intereses comerciales del propio operador[47]. Asimismo, se trata de evitar prácticas engañosas como la de un sitio web de comparación de precios que ofrecía colocar en el nivel superior de una clasificación los productos de los comerciantes que pagaban una tasa adicional, pero sin indicar claramente que esta clasificación en el nivel superior obedecía a un pago, de forma que la herramienta comparativa podía distorsionar de manera sustancial el comportamiento económico de los consumidores[48]. También trata de evitar prácticas como las llevadas a cabo por un importante proveedor de servicios de comparación y reserva, que permite a los hoteles manipular la clasificación pagando comisiones más elevadas, sin informar a los consumidores.[49].

Nótese que el artículo 26.2 LCD, aplica a cualquier comerciante que ofrezca la posibilidad de buscar "productos", incluidos los motores de búsqueda. No prohíbe la inclusión de publicidad o una clasificación superior debido a los pagos recibidos de los comerciantes de que se trate, pero exige que el proveedor del servicio de búsqueda informe claramente al consumidor cuando los resultados de la búsqueda incluyan productos o sitios web o URL de comerciantes que hayan pagado para ser incluidos en los resultados de la búsqueda (publicidad) o cuando la clasificación esté influida por pagos directos o indirectos.

Por "publicidad" se entiende la inserción, en la parte superior o entre los resultados "naturales", de entradas que, de otro modo, no se habrían presentado al consumidor con arreglo a los criterios de búsqueda objetivos aplicables. Por "clasificación superior" se entiende las situaciones en las que la posición de una o más entradas de la clasificación ha mejorado debido a los pagos directos o indirectos[50].

El considerando 20 de la Directiva (UE) 2019/2161 ofrece ejemplos no exhaustivos de pagos indirectos a efectos de la clasificación superior: aceptación por parte de un comerciante de obligaciones adicionales de cualquier tipo respecto del proveedor; comisión mayor por transacción; distintos sistemas de compensación que den lugar en concreto a una clasificación superior. Por el contrario, los pagos indirectos no incluyen los pagos por servicios generales, como comisiones de venta o suscripciones de miembros, que hacen referencia a una amplia gama de funcionalidades, siempre y cuando tales pagos no estén destinados a obtener una clasificación superior.

Los anuncios en los resultados de las búsquedas y los resultados de las búsquedas que sean objeto de pago específicamente para obtener una clasificación superior deben

[47] European Commission. "Commission Decision of 27 June 2017 in Case AT.39740 – Google Search (Shopping)". C (2017) 4444 final. Brussels, 27 June 2017. Disponible en: https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf
[48] Cass. Com. 4 décembre 2012, 11-27729, Publicité Sté Pewterpassion.com c/Sté Leguide.com.
[49] LG Berlin, 25.8.2011, Az.16 O 418/11.
[50] 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).

destacarse de forma clara y prominente como tales. La información sobre el anuncio o el pago específico para obtener una clasificación superior debe presentarse de forma directamente asociada al resultado de la búsqueda pertinente de una forma visualmente destacada, que destaque del resto de la interfaz en línea general, de manera que el consumidor no pueda evitar advertirla al ver el resultado de la búsqueda. No obstante, cuando los pagos efectuados específicamente para lograr una clasificación superior formen parte de los parámetros de clasificación e influyan en la clasificación de todos los resultados mostrados, la información sobre dichos pagos también podrá facilitarse mediante una única declaración clara y visible en la página de resultados de las búsquedas. Dicha declaración debe ser independiente y ha de ofrecerse además de la información general sobre los parámetros de clasificación que los comerciantes deben facilitar de conformidad con la Directiva (UE) 2019/2161 anteriormente mencionada[51].

1.2.6. Publicidad de las plataformas en línea

En el ecosistema digital contemporáneo, la publicidad segmentada constituye una de las principales fuentes de ingresos de las plataformas en línea. Redes sociales como Instagram o TikTok, motores de búsqueda como Google y marketplaces como Amazon o Booking muestran anuncios integrados en la interfaz que se mimetizan con el contenido orgánico, hasta el punto de que el usuario a menudo no distingue entre resultados naturales y patrocinados.

Sobre todo, algunas plataformas de redes sociales se han convertido en entornos para la publicidad. Por tanto, pueden presentar un riesgo creciente de publicidad encubierta, dado que mezclan elementos comerciales con contenido social y cultural generado por los usuarios. Además, es posible que los consumidores no siempre sean conscientes de que los comerciantes utilizan los medios sociales para fines de comercialización.

Las plataformas de redes sociales presentan diferentes tipos de publicidad, como la publicidad nativa, que consiste en mezclar contenidos comerciales con contenidos no comerciales y a menudo se muestra con el mismo formato y en la misma posición que el contenido generado por los usuarios (por ejemplo, noticias personales de un usuario). También es más visible en entornos móviles, ya que el contenido puede ocupar todo el espacio en una pantalla más pequeña. El contenido suele ser desarrollado por anunciantes utilizando las opciones de publicación disponibles en la plataforma publicitaria[52].

Además, la segmentación se realiza mediante sistemas de *adtargeting* que combinan datos de navegación, historial de compras y perfiles demográficos para personalizar el anuncio a cada usuario, lo que aumenta su efectividad, pero también plantea riesgos de opacidad

[51] 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).
[52] 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).

y de discriminación. En muchas ocasiones, el consumidor desconoce quién está detrás del anuncio, por qué se le muestra a él y no a otro usuario y cómo puede modificar esos parámetros de segmentación. Esta falta de transparencia mina la confianza en el entorno digital y dificulta la formación de una decisión de consumo informada. Como ha expuesto una reciente encuesta de la Comisión, al 93 % de los compradores en internet le preocupa la publicidad personalizada en línea, incluida la recogida de datos personales, la publicidad excesiva y la personalización[53].
Pues bien, en primer lugar, en España, las prácticas publicitarias se rigen por la Ley 34/1988, de 11 de noviembre, General de Publicidad. Su artículo 3 c) establece que es ilícita la publicidad subliminal. El artículo 4 define la publicidad subliminal como la "que mediante técnicas de producción de estímulos de intensidades fronterizas con los umbrales de los sentidos o análogas, pueda actuar sobre el público destinatario sin ser conscientemente percibida".

Además, puesto que en estos casos se hace uso de sistemas de I para dirigir publicidad, hemos de atender a lo recogido en el AI Act. Recordemos que, entre las prácticas prohibidas, se encuentran aquellas destinadas a manipular y perjudicar a individuos o grupos, prestando especial atención a las personas vulnerables. En el artículo 5 apartado 1 se prohíbe lo siguiente: "la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas (…)".

Por su parte, el artículo 26 DSA introduce un marco normativo destinado a garantizar la transparencia publicitaria en las plataformas en línea[54]. Obliga a que, por cada anuncio mostrado, el usuario pueda identificar de forma clara e inequívoca: (i) que se trata de un anuncio, mediante indicaciones destacadas; (ii) la persona física o jurídica en cuyo nombre se presenta el anuncio; (iii) el pagador de la publicidad, si es distinto del anunciante; y (iv) los principales parámetros utilizados para determinar que el anuncio se muestre a ese usuario en concreto, con información fácilmente accesible para modificarlos. Asimismo, las plataformas deben proporcionar mecanismos para que los propios usuarios declaren si el contenido que publican es comunicación comercial y asegurarse de que el resto de usuarios pueda identificarlo en tiempo real de forma clara y visible.
No podemos dejar de mencionar el riesgo de discriminación publicitaria. En 2019, trascendió que ciertas plataformas permitían a los anunciantes segmentar anuncios de vivienda o empleo excluyendo a colectivos protegidos (por ejemplo, mostrar ofertas de empleo solo a varones jóvenes, o anuncios de vivienda solo a usuarios de cierta etnia o

[53] Comisión Europea - Comunicado de prensa. Nuevos datos indican un alto grado de confianza de los consumidores, pero persisten las amenazas en línea, Brussels, 14 de marzo de 2025, https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_25_762/IP_25_762_ES.pdf
[54] Un requisito de divulgación similar se encuentra en los artículos 9, 10 y 28 ter de la Directiva de servicios de comunicación audiovisual.

código postal). Facebook (Meta) fue investigada por ello y debió ajustar sus algoritmos para evitar tratos discriminatorios.

Este tipo de publicidad se considera ilícita en virtud del artículo 3 a) Ley 34/1988, de 11 de noviembre, General de Publicidad, que considera ilícita "la publicidad que atente contra la dignidad de la persona o vulnere los valores y derechos reconocidos en la Constitución Española, especialmente a los que se refieren sus artículos 14, 18 y 20, apartado 4. Se entenderán incluidos en la previsión anterior los anuncios que presenten a las mujeres de forma vejatoria, bien utilizando particular y directamente su cuerpo o partes del mismo como mero objeto desvinculado del producto que se pretende promocionar, bien su imagen asociada a comportamientos estereotipados que vulneren los fundamentos de nuestro ordenamiento, coadyuvando a generar las violencias a que se refieren la Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género y la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual".

El artículo 26.2 DSA aborda en cierta medida la cuestión, ya que prohíbe de forma expresa la presentación de anuncios basados en la elaboración de perfiles que utilicen las categorías especiales de datos personales a que se refiere el artículo 9.1 RGPD. Esta prohibición supone un estándar más estricto que el previsto en el propio RGPD, que sí permite el tratamiento de estas categorías de datos con el consentimiento explícito del interesado (artículo 9.2.a RGPD). El DSA, en cambio, cierra esta posibilidad incluso en caso de consentimiento, evitando que la microsegmentación publicitaria pueda realizarse sobre la base de datos sensibles y reforzando así la protección frente a prácticas de segmentación potencialmente discriminatorias o intrusivas. La prohibición relativa a los datos sensibles se limita a las categorías especiales de datos contempladas en el artículo 9(1) del RGPD (esto es, datos sobre origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos con fines de identificación única, salud u orientación sexual). Las categorías especiales de datos incluyen cualquier información —incluidos los resultados inferidos— que revele una de las categorías enumeradas en dicho precepto. El TJUE interpreta "datos sensibles" de forma amplia, pero la jurisprudencia actual no aclara si dicho concepto abarca, por ejemplo, datos relativos a comportamientos o estados mentales (emociones, estados de ánimo o pensamientos) o datos relativos a eventos negativos (problemas de pareja, fallecimiento de familiares, dificultades económicas o problemas de juego)[55]. Como ejemplo en la jurisprudencia nacional, destaca la STS (1ª) de lo Civil núm. 272/2019, de 17 de mayo de 1019, rec. 3899/2016.

Otro problema recurrente es la publicidad dirigida a menores[56]. Así, en primer lugar, es preciso mencionar el artículo 20.4 Ley 34/1988, de 11 de noviembre, General de Publicidad, referente a la protección de la juventud y la infancia. Este precepto establece

[55] STJUE de 4 de septiembre de 2025, asunto C-413/23.
[56] Véase Cap. V, casos de uso en menores.

que se considera ilícita la publicidad "dirigida a menores que les incite a la compra de un bien o servicio, explotando su inexperiencia o credulidad".

En segundo lugar, el artículo 28.1 DSA establece que "los prestadores de plataformas en línea accesibles a los menores establecerán medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en su servicio". Por su parte, el artículo 28.4 DSA establece que "la Comisión, previa consulta a la Junta, podrá proporcionar directrices para guiar a los prestadores de plataformas en línea en la aplicación del apartado 1". En virtud de este precepto, la Comisión, mediante comunicación de 10 octubre 2025, ha dictado las Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28.4 DSA[57].

En particular, el artículo 28.3 DSA establece que prestadores de plataformas en línea no presentarán anuncios en su interfaz basados en la elaboración de perfiles, tal como se define en el artículo 4.4 RGPD, mediante la utilización de datos personales del destinatario del servicio cuando sean conscientes con una seguridad razonable de que el destinatario del servicio es un menor[58]. El ámbito de estas disposiciones de la DSA se limita a las plataformas en línea, por lo que quedan excluidos otros tipos de comerciantes que también pueden recurrir a la publicidad personalizada.

La relevancia de estos riesgos ha llevado a la Comisión a intensificar el control sobre las plataformas de muy gran tamaño. Un ejemplo reciente es la incoación, el 16 de mayo de 2024, de un procedimiento formal contra Meta por posibles infracciones de la DSA en relación con la protección de los menores en Facebook e Instagram. La Comisión investiga si el diseño de las interfaces y los algoritmos de ambas plataformas fomentan comportamientos adictivos y los denominados "efectos de agujero de conejo", así como la adecuación y eficacia de sus mecanismos de verificación de edad y de las configuraciones de privacidad por defecto. También analiza si Meta cumple las obligaciones de evaluación y mitigación de riesgos (artículos 34 y 35 DSA) y de protección reforzada de los menores (artículo 28 DSA). La apertura del procedimiento no prejuzga su resultado, pero confirma que la aplicación del DSA en materia de menores constituye una prioridad de supervisión para la Comisión[59].

1.2.7. Información sobre sistemas de recomendación

[57] «DOUE» núm. 5519, de 10 de octubre de 2025.
[58] A mayor abundamiento, el punto 28 del anexo I de la Directiva 2005/29/CE prohíbe las exhortaciones directas a los niños en las comunicaciones comerciales. Por lo tanto, las prácticas de publicidad dirigida centradas en los niños como grupo destinatario no pueden contener ninguna exhortación directa a comprar los productos anunciados.
[59] Comisión Europea-Comunicado de Prensa. La Comisión incoa un procedimiento formal contra Meta en virtud de la Ley de Servicios Digitales en relación con la protección de los menores en Facebook e Instagram, 16 de mayo de 2024, https://ec.europa.eu/commission/presscorner/detail/es/ip_24_2664.

Parte fundamental negocio plataforma en línea forma en que prioriza y presenta la información en su interfaz para facilitar y optimizar el acceso a ella destinatarios. Ello se hace a través de sistemas de recomendación, definidos en el artículo 3 s) DSA como un "sistema total/parcialmente automatizado y utilizado por una plataforma en línea para proponer en su interfaz en línea información específica para los destinatarios del servicio o priorizar dicha información, también como consecuencia de una búsqueda iniciada por el destinatario del servicio, o que determine de otro modo el orden relativo o la relevancia de la información presentada".

Los sistemas de recomendación facilitan búsqueda información pertinente para destinatarios del servicio y contribuyen a mejorar su experiencia. También desempeñan papel importante en amplificación de determinados mensajes, la difusión viral de información y la promoción de comportamientos en línea. Un ejemplo es el algoritmo de YouTube, que sugiere vídeos en función del historial de visionado: si un usuario busca recetas de cocina, el sistema le recomendará vídeos similares, facilitando la experiencia. Sin embargo, el mismo mecanismo puede amplificar contenidos engañosos o nocivos, favoreciendo su difusión masiva. Algo parecido ocurre en TikTok o Instagram, donde las recomendaciones pueden dirigir al consumidor hacia tendencias de compra muy concretas, incentivando determinados hábitos de consumo sin que este perciba plenamente la influencia algorítmica.

Pues bien, las plataformas deben informar de modo coherente a los destinatarios del servicio sobre cómo los sistemas de recomendación afectan a la forma en que se muestra la información y pueden influir en la manera en que se les presenta. Deben presentar con claridad los parámetros de dichos sistemas de recomendación de manera fácilmente comprensible para que los destinatarios del servicio entiendan cómo se prioriza la información para ellos.

Así, las plataformas que utilicen sistemas de recomendación establecerán en sus condiciones generales, utilizando lenguaje claro y comprensible, los parámetros principales utilizados en sus sistemas de recomendación, así como cualquier opción a disposición de los destinatarios del servicio para modificar o influir en dichos parámetros principales (artículo 27.1). Dichos parámetros explicarán por qué se sugiere determinada información al destinatario del servicio. Incluirán, como mínimo (artículo 27.2): a) los criterios más significativos a la hora de determinar la información sugerida al destinatario del servicio, y b) las razones de la importancia relativa de dichos parámetros.

Además, si hay varias opciones disponibles para sistemas de recomendación que determinen el orden relativo de información, plataformas también pondrán a su disposición una funcionalidad que permita al destinatario del servicio seleccionar y modificar en cualquier momento su opción preferida. Dicha funcionalidad será accesible directa y fácilmente desde la sección específica de la interfaz de la plataforma (artículo 27.3).

Finalmente, las plataformas y motores de búsqueda de muy gran tamaño deben garantizar sistemáticamente que los destinatarios servicio disfruten de alternativas que no se basen en la elaboración de perfiles, en el sentido del RGPD, para los parámetros principales de sus sistemas de recomendación. Estas opciones deben ser directamente accesibles desde la interfaz en línea en la que se presentan las recomendaciones (considerando 94). Así, ofrecerán al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles tal como se define en el artículo 4.4 RGPD (artículo 38 RSD).

Nótese que estas reglas no cubren, sin embargo, la mayoría de las situaciones B2C fuera de plataformas centralizadas. Es decir, el DSA regula a intermediarios (redes sociales, marketplaces) pero no a la tienda online individual que usa su propio algoritmo de recomendación. Ello deja entrever que la UE ha ido actuando sectorialmente o por niveles, más que ofrecer un régimen integral.

1.2.8. Mercados digitales

El DMA no es una norma de protección directa de los usuarios finales, sino un instrumento de política de competencia que persigue garantizar la disputabilidad de los mercados digitales y limitar el poder de mercado de los denominados guardianes de acceso. Sin embargo, varias de las obligaciones que impone a estos operadores tienen efectos indirectamente beneficiosos para los usuarios, al reforzar su capacidad de elección y reducir el grado de dependencia respecto de las grandes plataformas.

Entre estas obligaciones destacan las contenidas en el artículo 5.2, que prohíben al guardián de acceso: tratar datos personales de los usuarios de servicios de terceros para prestar servicios de publicidad en línea; combinar datos personales procedentes de distintos servicios básicos de plataforma o de otros servicios que preste; cruzar datos personales entre sus diferentes servicios; o iniciar sesión de forma automática en otros servicios con el fin de combinar datos, salvo que el usuario haya otorgado un consentimiento válido conforme a los artículos 4.11 y 7 RGPD. Con ello se busca limitar el poder de mercado derivado de la acumulación masiva de datos, reduciendo las posibilidades de crear perfiles sin conocimiento del usuario.

Además, el DMA exige que el guardián de acceso ofrezca a los usuarios una alternativa menos personalizada pero equivalente, que no puede tener una calidad degradada en comparación con el servicio para quienes han consentido el tratamiento de sus datos, salvo en la medida en que la personalización sea técnicamente necesaria para la prestación. El considerando 37 aclara que, en el momento de solicitar el consentimiento, debe informarse al usuario de que la negativa puede dar lugar a una experiencia menos personalizada (por ejemplo, resultados de búsqueda menos adaptados a sus preferencias), pero que el servicio básico de plataforma seguirá plenamente disponible y no se eliminará ninguna funcionalidad. Este régimen favorece que los consumidores puedan utilizar los servicios de los guardianes de acceso sin tener que aceptar prácticas de recopilación extensiva de datos como condición para acceder a ellos, equilibrando así el poder de

negociación en el mercado digital y mitigando la ventaja competitiva derivada de la explotación masiva de datos personales.

1.2.9. Plataformas de intercambio de videos: Publicidad personalizada y menores

La protección de los menores frente a la publicidad personalizada y al uso de sus datos con fines comerciales se aborda en el ordenamiento europeo y nacional mediante normas complementarias.

El artículo 90 LGCA, introducido con ocasión de la transposición de la Directiva (UE) 2018/1808, establece una prohibición general para los prestadores de servicios de intercambio de vídeos, impidiéndoles tratar datos personales de menores para mercadotecnia directa, elaboración de perfiles o publicidad personalizada basada en el comportamiento, sin excepciones incluso en caso de consentimiento.

Por su parte, el artículo 28 RSD amplía el ámbito subjetivo de la protección, al aplicarse a todas las plataformas en línea accesibles a menores, pero limita la prohibición a la presentación de anuncios basados en elaboración de perfiles cuando el prestador sabe con seguridad razonable que el usuario es menor.[60] De este modo, la LGCA ofrece una protección más intensa pero sectorial, mientras que el DSA proporciona un marco horizontal de salvaguardas que refuerza la privacidad y seguridad de los menores en todo el entorno digital.

1.2.10. Reglamento de Inteligencia Artificial

El AI Act prohíbe determinados casos de uso de sistemas de IA que impliquen técnicas subliminales, técnicas deliberadamente manipuladoras o engañosas, o la explotación de vulnerabilidades relacionadas con la edad, discapacidad o situación social o económica, cuando ello produzca, o sea razonablemente probable que produzca, un perjuicio significativo (artículo 5.1 a) AI Act). La aplicación de estas prohibiciones depende de la interpretación de términos como "técnica subliminal" o "deliberadamente manipuladora o engañosa", y exige que el perjuicio sea significativo[61].

Nótese que el AI Act, bajo un enfoque de gestión de riesgos, clasifica los sistemas de IA en prohibidos (los pocos casos intolerables, como sistemas de puntuación social generalizados por gobiernos, o manipulación subliminal que cause daño físico/psicológico, etc.), alto riesgo, riesgo limitado, y mínimo riesgo. Los sistemas de "alto riesgo" incluyen los utilizados en: educación (ej. decidir admisión), empleo (filtrar CVs), servicios esenciales privados o públicos (agua, electricidad, policía),

[60] *Vid*. Comisión Europea, Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065, C/2025/5519, 2025.
[61] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.

administración de justicia, identificación biométrica en vivo, y determinación de acceso a crédito o servicios financieros esenciales, entre otros (Anexo III). Para estos sistemas se exige una serie de obligaciones ex ante: evaluación de conformidad, requisitos de datos de entrenamiento libres de sesgos en la medida de lo posible, documentación técnica exhaustiva, supervisión humana, robustez, ciberseguridad, etc.

Ahora bien, el AI Act no cubre todos los supuestos de impacto algorítmico en consumo. Por ejemplo, un algoritmo de fijación de precios en una tienda de ropa puede no ser "alto riesgo" según el reglamento, l no encajar en las áreas listadas, a pesar de su relevancia para consumidores. Los sistemas de recomendación de productos, los chatbots comerciales, los algoritmos de personalización de anuncios online (salvo que afecten derechos fundamentales) quedarían como "riesgo limitado", sujetos solo a ciertas obligaciones de transparencia básicas: p. ej., el AI Act obligará a etiquetar contenidos generados por IA (para que el consumidor sepa si interactúa con una IA o con un humano, artículo 52), y pocas cosas más para esos casos. En definitiva, aunque el AI Act es un hito importante hacia la transparencia, su alcance en consumo es parcial.

1.3. Conclusión

Las normas europeas y españolas analizadas articulan un conjunto de derechos que giran en torno a un eje común: la transparencia algorítmica. El consumidor tiene derecho a saber por qué ve determinados productos, ofertas, contenidos o anuncios y a conocer los criterios principales que determinan su posición en los resultados. Esto incluye saber si un producto aparece primero por relevancia, por un pago por posicionamiento o porque se han tenido en cuenta las preferencias del consumidor a través del tratamiento automatizado de datos, y entender qué factores pesan más en las recomendaciones[62].

Sobre este núcleo de transparencia se superponen diversos derechos sectoriales que refuerzan la posición del consumidor frente al uso de sistemas de IA. Entre ellos destacan: la posibilidad de optar, en ciertos servicios de plataforma, por una experiencia menos personalizada sin que ello implique una degradación injustificada del servicio; el derecho, en determinados supuestos, a solicitar intervención humana cuando las decisiones automatizadas producen efectos relevantes sobre su situación; y la protección reforzada de los menores, basada en la prohibición de utilizar sus datos para mercadotecnia directa, elaboración de perfiles o publicidad personalizada basada en el comportamiento. A ello se añaden límites específicos a la combinación y reutilización de datos por parte de los guardianes de acceso, así como prohibiciones dirigidas contra técnicas especialmente manipuladoras o explotadoras de vulnerabilidades.

Todo ello conforma un marco aún fragmentado, en el que las obligaciones se reparten entre responsables del tratamiento, plataformas, marketplaces, motores de búsqueda, guardianes de acceso y prestadores audiovisuales, y donde persisten lagunas y asimetrías. Sin embargo, más allá de esa dispersión normativa, se vislumbra una tendencia común:

[62] Véase capítulo IV sobre derechos de transparencia y explicabilidad.

la consolidación progresiva de un auténtico derecho del consumidor a la transparencia algorítmica, complementado por garantías sectoriales frente a los riesgos más intensos de la personalización y de la toma de decisiones automatizada.

2. Dark patterns

2.1. Riesgos

En el mercado digital actual, los sistemas de recomendación constituyen el principal mecanismo de exposición de contenidos, productos y ofertas, condicionando de forma decisiva la experiencia del usuario. Plataformas de comercio electrónico como Amazon priorizan productos que maximizan su margen de beneficio; servicios de streaming como Netflix organizan el catálogo para aumentar el tiempo de permanencia; y redes sociales como TikTok destacan los contenidos que generan mayor interacción, no necesariamente los más relevantes o veraces.

En este contexto surge el concepto de *dark patterns*: estrategias de diseño que manipulan la conducta del usuario mediante la arquitectura de la interfaz. Se trata de patrones visuales, mensajes o flujos de interacción diseñados para influir en la decisión del consumidor en beneficio del comerciante. El término describe configuraciones o procesos engañosos integrados en la interfaz que orientan al usuario hacia elecciones que no adoptaría libremente.

Esta arquitectura de elección puede inducir decisiones que limitan la autonomía del consumidor. Entre las prácticas habituales se encuentran presentar productos patrocinados como si fueran resultados naturales, inducir a aceptar condiciones de tratamiento de datos mediante mensajes emergentes reiterados o dificultar la cancelación de un servicio imponiendo procedimientos significativamente más complejos que los de suscripción. Estas técnicas erosionan la capacidad del usuario para formarse una decisión informada y favorecen comportamientos impulsivos o no deseados.

La irrupción de la IA amplifica la eficacia de los patrones oscuros al permitir su personalización dinámica según las características individuales del consumidor. Un algoritmo puede detectar vulnerabilidades o sesgos cognitivos —como propensión a compras nocturnas, dificultades para localizar determinadas opciones o tendencia a aceptar mensajes repetitivos— y adaptar la interfaz para obtener el resultado deseado, ya sea una venta adicional, la renovación de una suscripción o la aceptación de cookies.

Esta explotación algorítmica de vulnerabilidades se intensifica cuando los sistemas monitorizan el comportamiento en tiempo real. Si el algoritmo identifica indecisión o abandono del carrito, puede mostrar ofertas en el momento de mayor debilidad, o desplegar mensajes confusos cuando el usuario intenta rechazar cookies. Un ejemplo especialmente ilustrativo se observa en los videojuegos en línea, donde los algoritmos calculan la “puntuación de asunción de riesgo” del jugador y ajustan dinámicamente la

oferta de cajas de recompensas, las probabilidades de obtener objetos valiosos o el nivel de dificultad para maximizar el gasto dentro del juego.

La explotación personalizada de vulnerabilidades no se limita al ámbito lúdico. Un comerciante puede detectar que un adolescente atraviesa un momento emocional delicado y utilizar esa información para mostrar anuncios basados en emociones en los momentos de mayor impacto. De forma similar, conocer el historial financiero de un consumidor —como una denegación previa de crédito— puede servir para dirigirle ofertas que se aprovechan de su situación económica. En otros casos, comerciantes analizan patrones de gasto vinculados a juegos de azar o a compras relacionadas con contenido aleatorio y envían comunicaciones comerciales con elementos similares, incrementando la probabilidad de que el usuario contrate productos especialmente sensibles a sus hábitos previos.

2.2. Marco normativo

2.2.1. Prácticas desleales

Persuadir a los consumidores para que interactúen con contenidos y ofertas forma parte esencial de las prácticas comerciales, tanto en línea como fuera de línea. Sin embargo, el entorno digital permite a los comerciantes desplegar estas técnicas con una eficacia muy superior, apoyándose en datos de los usuarios, aplicándolas a gran escala y, en muchos casos, ajustándolas dinámicamente en tiempo real. Los comerciantes pueden desarrollar prácticas de persuasión altamente personalizadas gracias al conocimiento acumulado que obtienen mediante el tratamiento de datos agregados sobre comportamientos y preferencias, incluidos aquellos procedentes de distintas fuentes. Este conocimiento les permite realizar ajustes continuos para maximizar la eficacia de sus prácticas y aprender progresivamente más sobre el comportamiento de los consumidores. A menudo, estas prácticas se aplican sin que el consumidor sea plenamente consciente de su existencia o de su grado de personalización. La combinación de estos elementos (volumen de datos, capacidad de ajuste dinámico y opacidad) es lo que diferencia las técnicas de publicidad o venta altamente persuasivas de las prácticas comerciales que pueden considerarse manipuladoras y, por tanto, potencialmente desleales desde la perspectiva del Derecho de consumo.

Cualquier práctica empresarial que distorsione, o pueda distorsionar, de manera sustancial el comportamiento económico de un consumidor medio o vulnerable puede infringir la Directiva 2005/29/CE. Dependiendo de las circunstancias, la conducta puede vulnerar la exigencia general de diligencia profesional del artículo 5, constituir una práctica engañosa conforme a los artículos 6 y 7, o bien ser calificada como práctica agresiva con arreglo a los artículos 8 y 9. A efectos de esta evaluación, la referencia al "consumidor medio" puede modularse en función del grupo destinatario y, cuando la práctica sea altamente

personalizada, incluso valorarse desde la perspectiva de la persona concreta a la que se dirige[63].

Estas prácticas pueden tener un impacto especialmente intenso en los consumidores vulnerables. Las características que definen la vulnerabilidad en el artículo 5.3 de la Directiva 2005/29/CE son meramente indicativas y no exhaustivas. El concepto es dinámico y contextual: un consumidor puede ser vulnerable en ciertos contextos y no en otros. Así, un usuario puede mostrarse particularmente sensible ante prácticas de persuasión personalizadas en el entorno digital, pero no en una tienda física. El uso comercial de información relativa a vulnerabilidades específicas (ya sean emocionales, económicas, cognitivas o derivadas de otra circunstancia personal) puede influir de manera decisiva en las decisiones de transacción. En función del caso, ello podría constituir una forma de manipulación basada en la "influencia indebida" del comerciante sobre el consumidor, dando lugar a una práctica agresiva prohibida por los artículos 8 y 9 de la Directiva. Al evaluar la existencia de influencia indebida, el artículo 9, letra c), exige considerar la explotación de cualquier infortunio o circunstancia grave que menoscabe la capacidad de discernimiento del consumidor y que sea conocida por el comerciante[64].

2.2.2. *Servicios digitales*

El artículo 25 DSA aborda este fenómeno prohibiendo que las interfaces se diseñen, organicen o gestionen de forma que engañen o manipulen a los destinatarios del servicio o que distorsionen u obstaculicen sustancialmente su capacidad para tomar decisiones libres e informadas. Esta prohibición se traduce en la obligación de presentar la información de manera clara y equilibrada, evitando prácticas como: resaltar de forma engañosa ciertas opciones —por ejemplo, destacar la suscripción de pago y ocultar la gratuita—;bombardear al usuario con ventanas emergentes hasta que acepte una opción (*nagging*); dificultar injustificadamente la cancelación de un servicio mediante procedimientos complejos y laberínticos; o (iv) priorizar productos patrocinados sin indicarlo claramente, induciendo a pensar que son la mejor opción.

2.2.3. Servicios financieros a distancia

Por su parte, el considerando 41 de la Directiva (UE) 2023/2673 establece que los *dark patterns* en las interfaces en línea de los comerciantes son prácticas que distorsionan o merman sustancialmente, bien de forma deliberada, bien de forma efectiva, la capacidad de los consumidores destinatarios del servicio financiero de tomar decisiones autónomas

[63] 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).
[64] 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).

e informadas. Esto sucede especialmente en el caso de los contratos de servicios financieros celebrados a distancia. Los comerciantes pueden utilizar esas prácticas para persuadir a los consumidores destinatarios de su servicio de que adopten comportamientos o tomen decisiones que estos no desean y que pueden provocarles consecuencias negativas. Por esta razón, debe prohibirse a los comerciantes engañar o predisponer a los consumidores destinatarios de su servicio y distorsionar o mermar su autonomía, su toma de decisiones o su capacidad de elección por medio de la estructura, el diseño o las funcionalidades de una interfaz en línea o de parte de esta.

Entre esas prácticas se pueden incluir, aunque no únicamente, las opciones de diseño abusivas que dirigen al consumidor hacia elecciones o acciones que benefician al comerciante, pero pueden no favorecer los intereses del consumidor al presentarse de una manera que no es neutra (por ejemplo, dando mayor protagonismo a determinadas opciones mediante componentes visuales, auditivos o de otro tipo) cuando se pide al consumidor que tome una decisión. Si bien el DSA prohíbe a los prestadores de servicios intermediarios que explotan plataformas en línea utilizar elementos engañosos en el diseño y la organización de sus interfaces en línea, la Directiva (UE) 2023/2673 obliga a los Estados miembros a impedir que los comerciantes que ofrezcan servicios financieros a distancia utilicen estos elementos al celebrar contratos para dichos servicios.

En este sentido, el artículo 16 sexies Directiva 2011/83/UE, modificado por la Directiva (UE) 2023/2673, establece que, sin perjuicio de lo dispuesto en la Directiva 2005/29/CE y el RGPD, los Estados miembros garantizarán que los comerciantes, cuando celebren contratos de servicios financieros a distancia, no diseñen, organicen ni gestionen sus interfaces en línea —tal como se las define en el artículo 3, letra m), DSA— de manera que induzcan a error o manipulen a los consumidores destinatarios de sus servicios o de otro modo distorsionen o mermen de manera sustancial su capacidad de tomar decisiones libres e informadas. En particular, los Estados miembros adoptarán medidas que, de conformidad con el Derecho de la Unión, aborden al menos una de las siguientes prácticas de los comerciantes: a) dar mayor relevancia a determinadas opciones cuando soliciten a los consumidores destinatarios de su servicio que tomen una decisión; b) solicitar reiteradamente que los consumidores destinatarios de su servicio elijan una opción cuando ya hayan hecho esa elección, especialmente mediante la presentación de ventanas emergentes que interfieran en la experiencia del usuario, o c) hacer que el procedimiento para poner fin a un servicio sea más difícil que suscribirse a él.

2.2.4. Propuesta de Digital Fairness Act

En la UE, la futura Digital Fairness Act buscaría combatir expresamente estos diseños engañosos de manera horizontal. De hecho, se prevé que se consideren prácticas prohibidas los *dark patterns* como opciones de exclusión ocultas o flujos de consentimiento confusos[65].

[65] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.

2.3. Conclusión

Las normas europeas aplicables a los *dark patterns* configuran un conjunto de derechos que, aun distribuidos entre distintos instrumentos, convergen en una misma finalidad: asegurar que las decisiones de consumo se adopten en un entorno de diseño neutral y no manipulador. De la Directiva 2005/29/CE derivan los derechos básicos frente a prácticas engañosas y agresivas, que permiten impugnar configuraciones de interfaz que distorsionen el comportamiento económico del consumidor, especialmente cuando explotan vulnerabilidades individuales. El DSA añade un nivel específico de protección en el ámbito de las plataformas en línea, prohibiendo expresamente los diseños que engañen, manipulen u obstaculicen de forma sustancial la capacidad de tomar decisiones libres e informadas. En el sector financiero a distancia, la Directiva (UE) 2023/2673 refuerza este enfoque al exigir que las interfaces de los proveedores de servicios financieros a distancia se estructuren de modo que no induzcan ni predispongan al consumidor mediante opciones de diseño no neutrales.

A pesar de la fragmentación normativa, se perfila un principio transversal de protección frente al diseño manipulador de las interfaces, según el cual el consumidor tiene derecho a interactuar en entornos digitales configurados de forma transparente, equilibrada y respetuosa con su autonomía. Este principio no se formula explícitamente como tal en una única norma, pero se desprende de la lógica combinada de todas ellas: impedir que el comerciante utilice la arquitectura de elección para orientar al usuario hacia decisiones que no adoptaría libremente. En conjunto, el ordenamiento avanza hacia el reconocimiento de un verdadero derecho a un diseño digital no manipulativo, que completa y amplía los tradicionales derechos de información, consentimiento y libre elección en el entorno digital.

3. Personalización de precios

3.1. Riesgos

La fijación de precios en el comercio electrónico puede adoptar dos formas principales. En primer lugar, los precios dinámicos o en tiempo real, en los que el precio se ajusta de forma flexible en función de factores generales de mercado —como la oferta y la demanda, la disponibilidad, la hora del día o la temporada— y que se aplican por igual a todos los consumidores que acceden en el mismo momento. Ejemplos típicos son las tarifas de Uber o Bolt en horas punta, los precios de hoteles y vuelos ajustados por plataformas como Booking o Expedia cuando aumenta la ocupación, o las variaciones de precios en supermercados en línea en función de la demanda.

Actualmente, la fijación dinámica de precios no está prohibida por el Derecho de la UE. Los comerciantes pueden determinar libremente los precios siempre que informen

adecuadamente al consumidor del precio total. No obstante, ciertas prácticas vinculadas a la fijación dinámica pueden infringir la Directiva 2005/29/CE, por ejemplo, si el precio aumenta durante el proceso de reserva después de que el consumidor haya iniciado la fase de pago. Subir el precio cuando el consumidor ya ha colocado el producto en su carrito o está a punto de pagar, sin concederle un plazo razonable para completar la transacción, puede considerarse contrario a la diligencia profesional o incluso una práctica agresiva conforme a los artículos 8 y 9.

Los precios dinámicos deben distinguirse de los precios personalizados. Mientras que los primeros se basan en variables ajenas al cliente (demanda, hora, disponibilidad, competencia), la personalización implica la individualización del precio en función de datos personales o del comportamiento del usuario. En consecuencia, si no existe personalización, diferentes consumidores deberían ver el mismo precio para un mismo producto adquirido simultáneamente. Diferencias derivadas de impuestos, gastos aplicables o descuentos generales no constituyen precios personalizados[66].

La personalización de precios se basa en la elaboración de perfiles mediante tratamientos automatizados de datos personales. Los comerciantes pueden utilizar información como el historial de navegación, las compras previas, la ubicación o el dispositivo empleado para inferir la disposición a pagar de cada consumidor y ajustar el precio en consecuencia. Así, dos usuarios pueden ver precios distintos para un mismo bien o servicio en el mismo momento. Esta práctica no es ilegal, pero exige un alto nivel de transparencia hacia el consumidor. La falta de referencias comparativas dificulta que este pueda saber si el precio mostrado está personalizado y, en su caso, qué datos lo han motivado.

El principal riesgo jurídico es la discriminación económica injustificada. Si la segmentación conduce a que ciertos consumidores paguen sistemáticamente más por indicadores que funcionan como marcadores indirectos de su nivel socioeconómico —como la zona de residencia, el dispositivo utilizado o el historial de compras— se vulnera la expectativa legítima de trato equitativo y transparente. Un algoritmo que ofrece precios más altos a consumidores con "perfil más pudiente", sin informarles de ello, puede resultar contrario a la buena fe y al principio de transparencia.

Aunque la evidencia empírica sobre precios personalizados aún es limitada, se ha documentado la existencia de diferencias de precio no explicadas en sectores como las citas en línea, el alojamiento y las aerolíneas. El estudio del Parlamento Europeo de 2022 ya anticipó que, aunque su uso todavía era reducido, es probable que estas prácticas se generalicen con la expansión de la IA[67]. En 2024, la Comisión identificó diferencias de precio en 10 de 85 sitios analizados, sin información clara sobre su origen. La

[66] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.
[67] Rott, P., Strycharz, J. & Alleweldt, F. (2022). *Personalised Pricing*. Publication for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

personalización resulta difícil de detectar incluso para expertos y autoridades, especialmente al reconstruir lo que se mostró a un consumidor concreto[68].

3.2. Marco normativo

3.2.1. Discriminación de precios basada en la nacionalidad o el lugar de residencia

La Directiva 2006/123/CE, de 12 de diciembre de 2006, relativa a los servicios del mercado interior, incluye una prohibición general de discriminación de precios basada en la nacionalidad o el lugar de residencia. El artículo 20 de dicha Directiva establece que "las condiciones generales de acceso a un servicio que el prestador ponga a disposición del público" no pueden contener "condiciones discriminatorias basadas en la nacionalidad o el lugar de residencia del destinatario". Sin embargo, según el artículo 20, esto no menoscaba "la posibilidad de establecer diferencias en las condiciones de acceso directamente justificadas por criterios objetivos".

Además, la discriminación de precios, directa o indirecta, basada en la nacionalidad del cliente final o su residencia o en el lugar de establecimiento de los transportistas o de los proveedores de billetes en la Unión está prohibida expresamente por varias normativas sectoriales de la UE. Esto se aplica al transporte aéreo[69], al transporte marítimo[70], al transporte ferroviario[71] y al transporte en autobús y autocar[72].

Es importante traer a colación el Reglamento (UE) 2018/302, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.º 2006/2004 y (UE) 2017/2394.

Su artículo 4 prohíbe que una misma interfaz en línea o aplicación web cambie automáticamente los precios u ofertas tras detectar el lugar de residencia, el lugar de establecimiento o la nacionalidad del cliente (mediante su dirección de IP u otros mecanismos como, por ejemplo, el lugar de emisión del instrumento de pago —tarjeta de crédito, cuenta bancaria desde la que se lleva a cabo la orden de pago, etcétera—).

---

[68] European Commission. "Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness", SWD (2024) 230 final, Brussels, 3 October 2024.
[69] Véase el artículo 23, apartado 2, del Reglamento (CE) n. o 1008/2008 sobre normas comunes para la explotación de servicios aéreos en la Comunidad.
[70] Véase el artículo 4, apartado 2, del Reglamento (UE) n. o 1177/2010 sobre los derechos de los pasajeros que viajan por mar y por vías navegables.
[71] Véase el artículo 5 del Reglamento (UE) 2021/782 sobre los derechos y las obligaciones de los viajeros de ferrocarril
[72] Véase el artículo 4, apartado 2, del Reglamento (UE) n. o 181/2011 sobre los derechos de los viajeros de autobús y autocar.

Un ejemplo de práctica prohibida sería que un consumidor acceda a monarca.co.uk (atraído por los precios más competitivos de esta última en comparación con su versión española) y se da cuenta de que, al incluir un producto en su cesta de compra, el precio cambia automáticamente al aplicado en monarca.co.es. No obstante, algunas diferencias de precio están justificadas si se basan en criterios objetivos y no solo en la nacionalidad. Por ejemplo, en función de los gastos postales, el consumidor puede tener que pagar más por un envío a un país o a otro.[73].

Además, no está prohibido que el comerciante pueda aplicar precios distintos en cada una de las diferentes tiendas en línea que tenga para diversos Estados miembros, o que pueda dirigir ofertas específicas solo a un determinado territorio de un Estado miembro. Un ejemplo de práctica permitida sería que Monarca pueda tener precios diferentes para el mismo producto en monarca.co.uk y en monarca.es. Pero el cliente que entre en monarca.co.uk disfrutará del precio de la web inglesa (sin que se le cambie al precio de la web española) y el cliente que entre en monarca.es disfrutará, siempre, del precio de la web española[74].

No obstante, no existe justificación posible para las diferencias de acceso a los bienes o servicios para los clientes de distintos países de la UE en las tres situaciones siguientes: venta de bienes sin entrega física, por ejemplo cuando compras un producto online que vas a recoger personalmente en una tienda, en lugar de recibirlo en tu casa; venta de servicios prestados por vía electrónica (con exclusión de los contenidos protegidos por derechos de autor), como los servicios de computación en nube o el alojamiento de sitios web; venta de servicios prestados en un lugar específico, por ejemplo reservas de hotel, alquiler de coches, entradas para parques de atracciones, etc.[75]

3.2.2. Contratos a distancia

Según el artículo 97.1 f) TRLGDCU, introducido con ocasión de la transposición de la Directiva (UE) 2019/2161, antes de que el consumidor quede vinculado por cualquier contrato a distancia o cualquier oferta correspondiente, el empresario le facilitará de forma clara y comprensible, la siguiente información: "f) Cuando corresponda, que el precio ha sido personalizado basándose en la toma de decisiones automatizada". Asimismo, el artículo 20.1 TRLCU establece que en los contratos celebrados a distancia o fuera del establecimiento mercantil, el comerciante facilitará de forma clara y comprensible información sobre el precio cuando este haya sido personalizado sobre la base de una toma de decisiones automatizada.

---

[73] Your Europe. Consultado en: https://europa.eu/youreurope/citizens/consumers/unfair-treatment/unfair-pricing/index_es.htm . Última fecha de consulta: 1 de septiembre de 2025.
[74] Área de Competencia de Gómez-Acebo & Pombo, "El nuevo reglamento europeo sobre geobloqueo y geodiscriminación", https://ga-p.com/wp-content/uploads/2019/01/Reglamento-sobre-el-geobloqueo-y-la-geodiscriminaci%C3%B3n.pdf
[75] Your Europe. Consultado en: https://europa.eu/youreurope/citizens/consumers/unfair-treatment/unfair-pricing/index_es.htm- Última fecha de consulta: 1 de septiembre de 2025.

El suministro de información sobre la toma de decisiones automatizada en la política de privacidad del comerciante no será suficiente para cumplir los requisitos de información precontractual sobre la personalización de los precios con arreglo a la Directiva (UE) 2019/2161. Antes de cada transacción, debe facilitarse información sobre la personalización de los precios, y no simplemente como parte de la información general sobre el tratamiento de datos personales facilitada por el comerciante.

Imaginemos que una consumidora navega con frecuencia por sus tiendas en línea favoritas y revisa los precios de diversos artículos, independientemente de si los va a comprar o no, y se da cuenta de que los precios varían dependiendo del dispositivo que utilice y de que sus amigos ven precios diferentes al consultar el mismo sitio web al mismo tiempo. A tenor de la norma aludida, antes de hacer una compra la consumidora tiene derecho a saber si un comerciante utiliza un algoritmo para modificar el precio del producto que te interesa.

Según el considerando 45 de la Directiva (UE) 2019/2161, este requisito de información no debe aplicarse a técnicas como la fijación de precios "dinámica" o "en tiempo real" que implican la alteración del precio de forma extremadamente flexible y rápida en respuesta a la demanda del mercado cuando dichas técnicas no impliquen una personalización basada en la toma de decisiones automatizada. Además, dicho requisito de información se entiende sin perjuicio RGPD, que prevé, entre otros, el derecho del individuo a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles. Como hemos explicado, la fijación de precios dinámica se refiere a cambios en los precios debidos a variables que no están relacionadas con el cliente, como la hora del día, la oferta disponible o los precios de los competidores. Cuando la fijación de precios dinámica se utilice sin personalizar los precios, distintos consumidores o grupos de consumidores deberán ver el mismo precio si compran el mismo producto al mismo tiempo, independientemente de su perfil y sus características individuales[76].

Ahora bien, esta regulación resulta claramente insuficiente. Los artículos 20.1 y 97.1 f) TRLGDCU se limitan a imponer al empresario un deber de advertir al consumidor de que el precio ha sido personalizado, pero no obliga a explicar cómo se ha obtenido ese precio, qué datos se han utilizado para calcularlo, o si el precio ofrecido es más alto o bajo que el que ven otros consumidores. En consecuencia, aunque formalmente se cumpla con el deber de información, la transparencia real para el consumidor sigue siendo muy limitada, lo que dificulta que pueda ejercer de manera efectiva su derecho a una elección libre e informada.

La obligación informativa sobre precios personalizados es bienvenida, pero resulta a todas luces insuficiente para proteger al consumidor de abusos en este terreno. Decirle al comprador "este precio ha sido ajustado mediante algoritmos según sus datos" apenas le

[76] Comunicación de la Comisión. Directrices sobre la interpretación y la aplicación de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo sobre los derechos de los consumidores (2021/C 525/01).

alerta y no le otorga herramientas efectivas, pues la mayoría de los consumidores difícilmente podrán evaluar si ese precio personalizado es razonable o si está inflado.

3.2.3. Proyecto de ley de atención a la clientela

Hemos dicho que actualmente el TRLGDC impone una obligación de informar al consumidor —antes de la perfección del contrato a distancia— cuando el precio ofrecido había sido personalizado mediante una toma de decisiones automatizada. Sin embargo, la norma no exige revelar qué datos, parámetros o criterios se habían utilizado para generar esa personalización. La obligación se limita a advertir que el precio era personalizado, sin detallar cómo ni sobre qué bases se había construido el perfil utilizado.

El PLAC, introduce, por primera vez en el Derecho español, un deber reforzado de transparencia algorítmica en materia de precios personalizados. En su Disposición final segunda —que modifica diversos preceptos del TRLGDCU— incorpora dos novedades de especial alcance.

En primer lugar, se modifica el artículo 20.1.c, relativo a la información obligatoria en la oferta comercial. Además de exigir que se comunique que el precio ha sido personalizado mediante una toma de decisiones automatizada en los contratos a distancia o fuera del establecimiento, la nueva redacción añade que la oferta deberá incluir los parámetros utilizados para la fijación del precio final. De este modo, la transparencia deja de limitarse a informar de la existencia de la personalización y pasa a incorporar la obligación de mencionar los criterios concretos que han influido en el cálculo del precio.

En segundo lugar, el PLAC modifica el artículo 97.1.f, relativo a la información precontractual en contratos a distancia. A partir de la reforma, el empresario deberá informar no solo de que el precio ha sido personalizado mediante una decisión automatizada, sino también de los parámetros utilizados para realizar esa personalización. Además, se establece de forma expresa que estos parámetros no podrán ser discriminatorios ni explotar situaciones de urgencia o necesidad.

En conjunto, las modificaciones de los artículos 20 y 97 introducen por primera vez en el TRLGDCU un deber explícito de transparencia algorítmica en la personalización del precio, obligando al empresario a desvelar los factores concretos empleados para individualizar la oferta económica hecha al consumidor.

3.2.4. Personalización precios casos de urgencia

La DF 1 Real Decreto-ley 8/2024, de 28 de noviembre, introduce nueva medida para garantizar el acceso a bienes o servicios esenciales en situación de emergencia (provocada por la DANA).

Así, la norma modificó el vigente artículo 20.1 c) TRLGDCU, que actualmente establece que, en los contratos celebrados a distancia, el comerciante informará si el precio ha sido personalizado sobre la base de una toma de decisiones automatizada. Ahora bien "esta personalización no podrá derivar en incrementos del precio final de venta cuando se produzca un incremento de la demanda en contextos de urgencia, riesgo o necesidad de la persona consumidora"[77].

Por tanto, si un supermercado en línea utiliza un algoritmo que combina datos de ubicación e historial de compras para detectar que un consumidor vive en una zona afectada por una DANA y está buscando agua embotellada, no puede personalizar al alza el precio en función de esa información, aunque exista un aumento de la demanda en el área. La norma pretende evitar que la fijación individualizada de precios aproveche situaciones de necesidad para incrementar el precio a consumidores concretos en función de sus datos personales.

3.2.5. *Protección de Datos*

Hemos dicho que el TRLGDCU no exige ninguna explicación adicional sobre los precios personalizados en el punto de venta, como los datos o parámetros principales utilizados para determinarlos. En la medida en que la personalización de precios constituya una toma de decisiones automatizada con efectos jurídicos o significativamente similares del artículo 22 RGPD, pueden proporcionarse explicaciones adicionales conforme a los artículos 13, 14 y 15 RGPD, que exigen proporcionar información significativa sobre la lógica aplicada a la decisión automatizada

3.2.6. Crédito al consumo

En el ámbito del crédito al consumo, los prestamistas y los intermediarios de crédito pueden personalizar no solo el tipo de interés ofrecido al consumidor, que constituye el precio del crédito, sino también otras condiciones contractuales como la duración, el importe del préstamo o las condiciones adicionales, para consumidores específicos o categorías de consumidores sobre la base de una toma de decisiones automatizada que incluye la elaboración de perfiles.

La Directiva (UE) 2023/2225 exige que los prestamistas y los intermediarios informen de manera clara y comprensible cuando una oferta se haya personalizado sobre la base de un tratamiento automatizado de datos personales, a fin de que el consumidor pueda tener en cuenta los posibles riesgos derivados de dicha personalización en su decisión de contratar. Esta obligación de información se articula en varios preceptos.

[77] Un contexto de urgencia, riesgo o necesidad es el derivado de cualquier situación que pueda ser calificada como emergencia de protección civil, en los términos regulados en la Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.

El artículo 10 se refiere de forma específica al precio, exigiendo que en la fase de información precontractual se indique expresamente si el tipo de interés ha sido personalizado sobre la base de un tratamiento automatizado de datos personales, incluida la elaboración de perfiles. El artículo 13 amplía el alcance de esta obligación a cualquier elemento de la oferta personalizada sobre la base de un tratamiento automatizado de datos personales, de modo que el prestamista o intermediario debe informar no solo si se ha personalizado el tipo de interés, sino también si se han personalizado el importe, la duración u otras condiciones del contrato. El considerando 46 precisa que, en aplicación del artículo 14.2 f) del RGPD, los prestamistas y los intermediarios deben informar a los consumidores sobre las fuentes de datos utilizadas para la personalización de la oferta, incluidas las inferencias que se hayan realizado.

De este modo, la Directiva no solo garantiza la transparencia en el precio personalizado, sino también en cualquier otro elemento de la oferta de crédito que se haya ajustado en función de un tratamiento automatizado de datos personales. Además, a diferencia del régimen del TRLGDCU para los contratos a distancia, impone expresamente el deber de informar al consumidor sobre las fuentes de datos utilizadas para dicha personalización, incluidas las inferencias realizadas.

3.2.7. Servicios financieros a distancia

En el ámbito de los servicios financieros a distancia, los proveedores pueden utilizar decisiones automatizadas para diferenciar los precios entre distintos grupos de consumidores e incluso, en algunos casos, para adaptar los precios a la sensibilidad concreta que cada consumidor demuestre frente al precio.

De acuerdo con la Directiva (UE) 2023/2673, el consumidor debe ser informado antes de quedar vinculado por el contrato de que el precio del servicio financiero ha sido personalizado sobre la base de una toma de decisiones automatizada. El considerando 27 subraya que esta información debe proporcionarse para que el consumidor pueda comprender que el precio que se le ofrece se ha determinado individualmente mediante un tratamiento automatizado de datos personales.

En el plano normativo, el artículo 16.1 bis de la Directiva 2011/83/UE, introducido por la Directiva 2023/2673, dispone que, con suficiente antelación al momento en que el consumidor quede vinculado por un contrato a distancia o por cualquier otra oferta correspondiente, el comerciante debe proporcionarle de forma clara y comprensible la información de que el precio ha sido personalizado basándose en una toma de decisiones automatizada, cuando proceda.

De este modo, la normativa de contratos de servicios financieros a distancia se alinea tanto con el régimen del crédito al consumo como con el de los contratos a distancia de bienes y servicios no financieros, garantizando un enfoque coherente en la obligación de informar al consumidor cuando el precio que se le ofrece ha sido determinado mediante una decisión automatizada.

3.2.8. Legislación comparada

Ejemplos recientes de legislación nacional en esta área incluyen una ley italiana de 2023 sobre la fijación de precios de billetes aéreos, que incorporó restricciones al uso de algoritmos de fijación automatizada de precios basados en perfiles de usuario cuando ello "afecte negativamente al comportamiento económico del usuario"[78].

3.3. Conclusión

En materia de precios personalizados, los distintos instrumentos normativos reconocen al consumidor un conjunto de derechos de transparencia cuyo alcance varía según el sector, pero que presentan un núcleo común. La garantía compartida en todos los regímenes es el derecho a ser informado, antes de contratar, de que el precio ofrecido ha sido personalizado mediante una toma de decisiones automatizada. Este deber se aplica tanto en los contratos a distancia de bienes y servicios como en los servicios financieros a distancia y en la contratación de crédito al consumo.

En algunos ámbitos, esta exigencia se refuerza. En particular, el régimen del crédito al consumo y —tras la reforma proyectada— los contratos a distancia de bienes y servicios imponen la obligación de informar no solo de la existencia de la personalización, sino también de los parámetros utilizados para determinar el precio individualizado. Ello supone un avance hacia una transparencia algorítmica más sustantiva, al permitir al consumidor conocer los factores que influyen en el precio que se le presenta.

Este movimiento hacia una transparencia reforzada se ve complementado por el carácter transversal del RGPD. Siempre que la personalización de precios constituya una decisión individual automatizada que produzca efectos jurídicos o afecte significativamente al consumidor (artículo 22 RGPD), surge además la obligación de proporcionar "información significativa sobre la lógica aplicada", incluidas las fuentes de datos y las inferencias relevantes. Aunque este régimen no se dirige específicamente a la transparencia en materia de consumo, opera como garantía horizontal que refuerza el control sobre la personalización algorítmica del precio.

El ordenamiento incorpora asimismo límites materiales. En situaciones de urgencia, riesgo o necesidad, la personalización al alza del precio está expresamente prohibida; y, en todo caso, los parámetros empleados no pueden ser discriminatorios ni explotar vulnerabilidades del consumidor. Estas restricciones complementan los deberes de información, introduciendo garantías sustantivas frente a prácticas potencialmente abusivas.

[78] Decreto-Ley n.º 104, 10 agosto 2023 (convertido en la Ley n.º 136/2023), Italia, artículo 1 y ss. (sector transporte aéreo) — prohíbe la fijación de tarifas mediante procedimientos automatizados basados en el perfilado web del usuario o en el dispositivo electrónico utilizado, cuando ello implique perjuicio económico al usuario.

En conjunto, el sistema reconoce al consumidor el derecho a saber que el precio ha sido individualizado, a conocer —en determinados sectores— los parámetros utilizados y a no sufrir personalizaciones abusivas en situaciones de vulnerabilidad. Aunque la intensidad de estas garantías difiere según el tipo de contrato, se advierte una tendencia común hacia un principio de transparencia y equidad en la personalización del precio, reforzado por la interacción entre la normativa sectorial y el régimen general de protección de datos.

4. Evaluación de la solvencia

4.1. Riesgos

La utilización de IA para la evaluación de la solvencia se ha convertido en una práctica creciente en el mercado. Los prestamistas u operadores de telecomunicaciones emplean sistemas automatizados que analizan grandes volúmenes de datos —historial crediticio, ingresos, patrones de pago, datos de consumo, datos sociodemográficos o incluso información inferida— para valorar el riesgo de impago. Estos modelos generan puntuaciones o perfiles de riesgo que se utilizan para decidir la concesión o denegación de un préstamo o la celebración de un contrato de telefonía. Esta práctica permite agilizar decisiones y reducir costes, pero plantea cuestiones de transparencia y posibles riesgos de discriminación algorítmica. Si el sistema de IA trata de modo sistemáticamente desfavorable a un colectivo (por ejemplo, ofreciendo peores condiciones de crédito a personas de cierto barrio, o mostrando publicidad de menor calidad a un grupo étnico), podría constituir una discriminación.

Si un algoritmo considera como variable el código postal del solicitante, puede estar negando créditos sistemáticamente a residentes de barrios humildes, donde quizá predominan minorías étnicas, reproduciendo así la discriminación socioeconómica previa. Algo similar ocurrió con la ya mencionada tarjeta de crédito Apple Card en EE. UU. Varias denuncias reportaron que el algoritmo de Apple/Goldman Sachs asignaba límites de crédito mucho menores a las mujeres que a los hombres con perfiles financieros similares (en un caso, a una mujer le dieron 1/10 del crédito de su marido a pesar de compartir bienes). Aunque la empresa negó discriminar intencionalmente, el caso ejemplificó cómo un scoring opaco podía arrojar resultados sesgados de modo sexista.

Un caso judicializado es el resuelto por la STJUE de 27 de febrero de 2025 (asunto C-203/22, Dun & Bradstreet). Aquí un operador de telefonía móvil denegó a un consumidor la prórroga de su contrato de 10 euros al mes basándose exclusivamente en un score de solvencia generado de forma automatizada. Aunque los datos financieros individuales del interesado acreditaban que podía hacer frente al pago, el sistema tomó en consideración factores sociodemográficos, como su lugar de residencia, que condujeron a un resultado negativo. Además, el consumidor no recibió una explicación clara de los motivos concretos de la denegación, lo que evidenció cómo el uso de sistemas automatizados puede afectar al acceso a servicios esenciales sin que el interesado comprenda por qué ha

sido rechazado. Este supuesto muestra de manera clara cómo el uso de la IA en la evaluación de la solvencia puede afectar directamente al acceso a servicios básicos, planteando riesgos de falta de transparencia e incluso de discriminación indirecta.[79]

4.2. Marco normativo

4.2.1. Protección de datos

La utilización de modelos automatizados para calcular una puntuación de solvencia constituye, cuando determina la concesión o denegación del contrato, una decisión basada únicamente en tratamiento automatizado en el sentido del artículo 22.1 RGPD. Estas puntuaciones son valores numéricos o categorías de riesgo que se generan a partir de datos personales (historial crediticio, deudas vigentes, ingresos, variables sociodemográficas o incluso datos inferidos) para estimar la probabilidad de impago y servir de base a la decisión del empresario. La STJUE de 7 de diciembre de 2023, C-634/21, Schufa, ha precisado que un score que condiciona de forma determinante la concesión de crédito es, en sí mismo, una decisión automatizada en el sentido del artículo 22, por lo que deben aplicarse estas garantías[80].

El artículo 22.1 reconoce al interesado el derecho a no ser objeto de decisiones exclusivamente automatizadas que produzcan efectos jurídicos o le afecten significativamente, salvo en los supuestos del artículo 22.2: consentimiento explícito, necesidad para la ejecución de un contrato o habilitación legal. En todos estos casos, el artículo 22.3 impone garantías adicionales, esto es, el derecho a solicitar intervención humana, expresar su punto de vista e impugnar la decisión.

Una vez reconocido que un score de solvencia se trata de una decisión automatizada, entran en juego los derechos de información y transparencia previstos en los artículos 13.2.f, 14.2.g y 15.1.h RGPD. El responsable debe informar de la existencia de la decisión automatizada, de la lógica aplicada, su importancia y las consecuencias previstas para el interesado. Esta explicación debe ser clara, inteligible y accesible, no limitada a fórmulas técnicas incomprensibles. La STJUE de 27 de febrero de 2025, asunto C-203/22, Dun & Bradstreet, subraya que la información significativa debe describir los procedimientos y principios en que se basa el tratamiento y, cuando sea posible, ofrecer ejemplos concretos que permitan al interesado entender cómo sus datos influyen en el resultado. Tanto la agencia que genera la puntuación como la entidad que toma la decisión final tienen obligaciones de información y deben ser capaces de explicar la lógica aplicada cuando el consumidor lo solicite.

Un ejemplo de información significativa sobre la lógica aplicada a un score generado de manera automatizada sería el siguiente. “Con tus datos actuales, esto es, un historial de

[79] MARTÍN FABA, M.ª. “La información sobre la lógica aplicada en el credit scoring automatizado: fácil, concisa y sin tecnicismos”. *Revista CESCO de Derecho de Consumo*, núm. 54, 2025, pp. 15-30.
[80] ARROYO AMAYUELAS, E., “El scoring de Shufa”, Indret, núm. 3, 2024, pp. 134-160.

crédito adecuado (apenas un 10% de tu capacidad de crédito utilizada) y unos ingresos mensuales estables (de 1.200 euros), el sistema considera, sin embargo, que tu perfil presenta riesgos para prorrogar el contrato, debido a factores relacionados con tu lugar de residencia (actualmente vives en una zona con alta morosidad generalizada y un nivel socioeconómico más bajo según estadísticas disponibles). Si residieras en una zona diferente, por ejemplo, en un área con menores tasas de morosidad y mejores indicadores socioeconómicos, el sistema habría valorado tu perfil como más seguro, y se te habría concedido la renovación del contrato. La decisión en este caso no se debe directamente a tus propios datos financieros, que son positivos, sino al impacto estadístico negativo derivado de factores sociodemográficos relacionados con el lugar donde vives". Ahora bien, que esta declaración podría acreditar una conducta discriminatoria del responsable del tratamiento.

Además, si un algoritmo usa datos personales a gran escala y puede afectar derechos (por ej., un sistema que detecta "riesgo de impago" analizando redes sociales), probablemente requiera una Evaluación de Impacto en Protección de Datos (artículo 35 RGPD) antes de ponerse en marcha, para identificar y mitigar riesgos de discriminación o vulneración de derechos.

4.2.2. Reglamento de Inteligencia artificial

Este marco se ve reforzado por el artículo 86 AI Act, que reconoce a toda persona afectada por una decisión basada en la salida de un sistema de IA de alto riesgo (como los sistemas de evaluación de crédito previstos en el anexo III), el derecho a obtener explicaciones claras y significativas sobre el papel del sistema en el proceso y sobre los principales elementos de la decisión. Este derecho complementa el del RGPD, asegurando que la explicación incluya no solo la lógica general del tratamiento de datos, sino también la contribución específica del sistema de IA a la decisión final.

La evaluación automatizada de solvencia se encuadra en los sistemas de IA de alto riesgo en el sentido del AI Act [Anexo III.5(b)], con todas las consecuencias jurídicas que ello implica. Estos sistemas pueden dar lugar a discriminaciones directas o indirectas y perpetuar patrones históricos asociados a factores como origen racial o étnico, género, discapacidad, edad u orientación sexual, o incluso generar nuevas formas de discriminación (considerando 58 AI Act). La sujeción del *credit scoring* automatizado al régimen de alto riesgo activa obligaciones reforzadas. Así, y sin ánimo de exhaustividad, los conjuntos de datos empleados para el desarrollo y funcionamiento del sistema deben configurarse de modo que se eviten resultados discriminatorios indebidos [artículo 10.2(f) AI Act]. Por ello, si el sistema utiliza, por ejemplo, el código postal del interesado como variable predictiva, dicho dato debe tener un valor explicativo real y, además, no producir efectos indirectamente discriminatorios.

4.2.3. Crédito al consumo

La Directiva (UE) 2023/2225 introduce un marco reforzado para la evaluación de solvencia mediante tratamiento automatizado de datos personales. El artículo 18.8 exige que, cuando el prestamista utilice procesamiento automatizado para decidir sobre la concesión del crédito, el consumidor tenga garantizados tres derechos: (i) obtener una explicación clara y comprensible de la evaluación, que incluya la lógica del modelo, los riesgos que implica el tratamiento automatizado y las consecuencias de la decisión; (ii) expresar su punto de vista y aportar información adicional; y (iii) solicitar una revisión humana de la evaluación y de la decisión final.

Estos derechos deben ser comunicados al consumidor antes de contratar, lo que convierte la transparencia en un presupuesto de validez de la decisión automatizada. Además, el artículo 18.9 impone al prestamista la obligación de informar sin demora de la denegación del crédito, indicando expresamente si se ha basado en una evaluación automatizada y recordando el derecho a revisión humana, así como la posibilidad de acudir a servicios de asesoramiento en materia de deudas accesibles.

Un aspecto esencial del régimen de la Directiva (UE) 2023/2225 es la delimitación de las fuentes de datos que pueden utilizarse en la evaluación de solvencia. El artículo 18.3 obliga a que la información utilizada sea pertinente, exacta y proporcionada a la naturaleza y riesgos del crédito, y prohíbe expresamente el uso de las categorías especiales de datos del artículo 9.1 RGPD (origen racial, datos de salud, orientación sexual, etc.), lo que evita que el modelo de IA incorpore variables que puedan conducir a discriminaciones directas o indirectas. Además, aclara que las redes sociales no constituyen una fuente externa válida para la evaluación de solvencia, cerrando la puerta al uso de datos comportamentales obtenidos de plataformas digitales como proxy de la capacidad de pago del consumidor. Esta restricción es coherente con la finalidad de proteger al consumidor frente a prácticas intrusivas y con la obligación de limitar el tratamiento de datos a lo estrictamente necesario.

La Directiva (UE) 2023/2225 representa un avance respecto del artículo 22 RGPD, pues reconoce el derecho a explicación y revisión aun en los casos en que el tratamiento no sea "únicamente automatizado", reforzando así la tutela frente a decisiones en las que interviene un sistema de IA de forma significativa. Esta exigencia también se alinea con el artículo 86 del AI Act, que garantiza a los afectados por decisiones basadas en sistemas de IA de alto riesgo —como los de evaluación de crédito— el derecho a obtener explicaciones claras sobre el papel del sistema en la decisión y sobre sus elementos principales.

En suma, la Directiva (UE) 2023/2225 construye un estatuto garantista de la evaluación de solvencia automatizada, que no se limita a exigir intervención humana, sino que incorpora obligaciones de transparencia y de selección de fuentes de datos, con el fin de prevenir sesgos algorítmicos, decisiones opacas y prácticas de scoring excesivamente intrusivas.

4.2.4. Normativa antidiscriminación

El artículo 14 CE proclama la igualdad ante la ley y prohíbe toda discriminación por razón, entre otras, de sexo, raza, origen, convicciones u otra condición o circunstancia personal o social. Si bien el artículo 14 CE vincula principalmente a los poderes públicos, su espíritu impregna también las relaciones entre particulares, habiendo desarrollado el legislador ordinario instrumentos para prevenir y sancionar la discriminación en campos como el empleo, la vivienda o la prestación de servicios privados.

Toda persona tiene derecho a la igualdad de trato y no discriminación en el acceso, oferta y suministro de bienes y servicios, incluidos los financieros, que se ofrezcan al público. No podrá denegarse el acceso a la contratación de seguros o servicios financieros afines por razón de nacimiento, raza, sexo, religión o cualquier otra condición o circunstancia personal o social, salvo cuando los criterios para tal diferenciación sean razonables y objetivos y lo que se persiga es lograr un propósito legítimo o así venga autorizado por norma con rango de ley (artículos 2. II y 17 Ley 15/2022) Esto adquiere relevancia en contextos algorítmicos: si un sistema de IA trata de modo sistemáticamente desfavorable a un colectivo (por ejemplo, ofreciendo peores condiciones de crédito a personas de cierto barrio, o mostrando publicidad de menor calidad a un grupo étnico), podría constituir una discriminación indirecta prohibida por la ley.

Volviendo a la STJUE de 27 de febrero de 2025, asunto C-203/22, Dun & Bradstreet, si una persona tenía capacidad económica para cumplir el contrato, pero se le denegó porque el sistema automatizado determinó que en su lugar de residencia estadísticamente hay más impagos, puede existir discriminación. Es decir, si dos personas tienen ex ante capacidad financiera para cumplir un contrato, y a una de ellas se le concede porque vive en Chamberí y a otra se le deniega porque vive en Orcasitas, esta última sufre discriminación, porque ante la misma situación (capacidad económica individual para cumplir un contrato) sufre un trato diferente que le perjudica. En realidad, se trata de una discriminación indirecta, pues un criterio aparentemente "neutral" (como el domicilio) produce un perjuicio específico para determinados grupos sociales, sin una justificación objetiva [artículo 6.1 b) 15/2022, en relación con el artículo 2.1]. Así, el hecho de que las variables sociodemográficas sean estadísticamente predictoras del riesgo de impago no puede justificar una vulneración del derecho a la igualdad si existe una alternativa menos lesiva, como evaluar únicamente la capacidad económica individual (cfr. artículo 2. II Ley 15/2022). Por tanto, si se acredita que el score fue negativo, a pesar de la capacidad económica individual del interesado para cumplir el contrato, debido a una agregación estadística derivada del domicilio o de variables sociodemográficas no individualizadas, estaríamos ante una decisión automatizada que podría vulnerar el principio de no discriminación del artículo 21 de la Carta (artículo 14. 1 CE), concretado en el artículo 6 Directiva (UE) 2023/2225.

Así pues, es posible que en tal caso el interesado tuviera derecho a una indemnización frente a quien obtuvo o utilizó el score, en virtud del artículo 25 Ley 15/2022. Porque acreditada la discriminación, se presumirá la existencia de daño moral (artículo 27 Ley

15/2022). También podría el interesado exigir una indemnización con fundamento en el artículo 82 RGPD, siempre que pruebe que el responsable del tratamiento ha infringido el RGPD y que ello causa al interesado un daño.

4.2.5. El caso Bosco

La STS, Sala III, 1119/2025, de 17 de septiembre (caso "BOSCO"), si bien referida al ámbito de la Administración Pública, constituye un hito en esta materia. El litigio se originó cuando la Fundación Civio solicitó al Ministerio para la Transición Ecológica el acceso a documentación técnica y al código fuente de la aplicación informática BOSCO, utilizada por los comercializadores eléctricos para verificar si los solicitantes cumplen los requisitos legales del bono social. La Administración denegó el acceso al código invocando la protección de la propiedad intelectual y riesgos para la seguridad del sistema y de los datos personales tratados (ingresos, discapacidad, condición de víctima, etc.). El Consejo de Transparencia estimó parcialmente la reclamación, pero mantuvo la negativa respecto del código fuente; la Audiencia Nacional confirmó este criterio por entender acreditados los riesgos de seguridad derivados de revelar el código, apoyándose en informes técnicos contradictorios aportados por las partes.

En casación, el Tribunal Supremo declaró que el derecho de acceso a la información pública del artículo 105 b) CE incluye, en principio, el código fuente de los algoritmos utilizados por la Administración cuando participan en decisiones automatizadas con impacto en los ciudadanos. El Tribunal sostuvo que el principio de transparencia es inherente al Estado de Derecho incluso cuando la decisión se implementa mediante software y que la propiedad intelectual o las razones genéricas de seguridad no pueden operar como límites absolutos al derecho a conocer cómo funciona un algoritmo público. Subrayó que, en un caso como BOSCO—un sistema que traduce criterios normativos a código informático—, el acceso desempeña una función esencial para verificar la legalidad y exactitud del proceso decisorio. Así, la sentencia eleva a categoría de principio general el carácter constitucional de la transparencia algorítmica. Según la Sala, esta garantía no se limita al sector público: su fundamento—el derecho a conocer las reglas que determinan decisiones automatizadas que afectan a las personas—posee una clara proyección transversal hacia el sector privado y, en particular, hacia el derecho de consumo.

4.3. Conclusión

En la evaluación automatizada de solvencia, los distintos instrumentos normativos reconocen al consumidor un conjunto de derechos que buscan garantizar transparencia, control efectivo y protección frente a decisiones opacas o discriminatorias. El primer derecho común a todos los regímenes es el de saber si la decisión ha sido adoptada —total o parcialmente— mediante un sistema automatizado, así como comprender de forma clara los factores que han influido en el resultado. Este derecho a la explicación se articula tanto a través del RGPD como de la Directiva (UE) 2023/2225 y del AI Act, y permite al consumidor entender por qué se le concede o deniega un contrato.

En segundo lugar, el consumidor dispone de derechos de intervención que aseguran que la decisión no quede íntegramente en manos del algoritmo. Puede aportar información adicional, expresar su punto de vista y exigir una revisión humana cuando la decisión derive de un tratamiento automatizado. Esta garantía, prevista tanto en el artículo 22.3 RGPD como en el artículo 18.8 de la Directiva 2023/2225, impide que una valoración algorítmica determine de forma definitiva el acceso a servicios esenciales. No obstante, ello no implica un derecho subjetivo a la concesión del crédito o a la prórroga contractual, sino únicamente a que la decisión sea revisada de manera individual y con criterios no discriminatorios.

En tercer lugar, el consumidor tiene derecho a que la evaluación de solvencia se base únicamente en datos pertinentes, exactos y proporcionados, y a que no se utilicen fuentes intrusivas o de dudosa fiabilidad. La normativa prohíbe expresamente el uso de datos sensibles y excluye, en determinados regímenes, la utilización de datos procedentes de redes sociales o de otras fuentes que puedan generar inferencias injustificadas sobre la solvencia. Estas restricciones buscan evitar que variables marginales o proxies socioeconómicos distorsionen la valoración.

Finalmente, el consumidor está protegido frente a decisiones que incorporen criterios discriminatorios, tanto directos como indirectos. No puede verse perjudicado por variables que funcionen como marcadores de condiciones sociales o étnicas —como el código postal o determinados indicadores sociodemográficos— cuando su capacidad económica individual demuestra que puede cumplir el contrato. La normativa antidiscriminación, junto con el RGPD, la Directiva 2023/2225 y el AI Act, convergen así en un principio de igualdad material que impide denegaciones basadas en agregaciones estadísticas que no reflejan la solvencia real del interesado.

En conjunto, el régimen vigente reconoce al consumidor derechos de explicación, intervención, revisión humana, control sobre los datos utilizados y protección frente a discriminación. Se configura así un marco coherente destinado a garantizar que decisiones determinantes para el acceso a servicios básicos no se adopten de forma opaca, arbitraria o discriminatoria, sino sobre la base de criterios transparentes, pertinentes y respetuosos con los derechos fundamentales.

5. Risk scoring

5.1. Riesgos

El big data y la IA están transformando la valoración del riesgo en el contrato de seguro. Ciertas aseguradoras utilizan sistemas de AI risk scoring que asignan puntuaciones de riesgo a solicitantes y asegurados a partir de grandes volúmenes de datos propios y externos. Estos sistemas permiten ajustar primas y condiciones con mayor precisión actuarial, pero generan riesgos significativos, como discriminación directa o indirecta,

uso de variables proxy, incrementos de precio no justificados por el riesgo, exclusión del acceso al seguro y opacidad en los factores que determinan la prima[81].

La tecnología altera la lógica tradicional de la LCS. La valoración del riesgo ya no depende exclusivamente de la declaración del tomador (cfr. artículo 10), sino que puede basarse en inferencias obtenidas por la aseguradora mediante datos adicionales de diversa procedencia. Esto reduce la aleatoriedad del contrato y facilita una segmentación intensiva del riesgo.

El impacto principal se produce en la fase precontractual y en la determinación de la prima. Los modelos de IA permiten hiperpersonalizar precios para riesgos antes homogéneos y favorecen prácticas como primas individualizadas que no se corresponden con el riesgo real, incrementos vinculados a factores ajenos al riesgo (por ejemplo, la inercia del asegurado o su menor propensión a cambiar de entidad), precios basados en la "disposición a pagar" que pueden generar efectos discriminatorios o excluyentes.

Estas dinámicas contribuyen a fenómenos de infraseguración en ámbitos clave como hogar, salud o responsabilidad civil. Además, la opacidad de los modelos dificulta al asegurado comprender cómo se ha calculado su prima, qué datos se han utilizado o si el sistema ha cometido errores o sesgos al estimar su riesgo. Si, por ejemplo, se descubriera que un algoritmo de seguros cobra primas más altas a personas de cierta nacionalidad, la discriminación sería flagrante (y contraria a la Directiva 2004/113/CE, de 13 de diciembre de 2004, por la que se aplica el principio de igualdad de trato entre hombres y mujeres al acceso a bienes y servicios y su suministro, que prohíbe discriminación por género en seguros, y similares).

En términos de protección del asegurado, resultan necesarias medidas de transparencia: informar de que la prima se ha calculado mediante sistemas de IA, proporcionar una explicación comprensible de la relación riesgo/precio y habilitar mecanismos de revisión humana cuando existan indicios de error, sesgo o discriminación. También debe advertirse que rechazar determinadas formas de personalización puede conllevar primas más elevadas al disponer de menos información, de modo que el tomador adopte una decisión plenamente informada[82].

5.2. Marco normativo

5.2.1. *Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras*

[81] Vid. APARACIO ARAQUE, B., El impacto de la Inteligencia Artificial en el contrato de seguro, Web CESCO,https://centrodeestudiosdeconsumo.com/images/El_impacto_de_la_Inteligencia_Artificial_en_el_contrato_de_seguro.pdf

[82] PÉREZ MORIONES, A., "Contrato de seguro e inteligencia artificial: el inexcusable replanteamiento de la posición del asegurado", Revista española de seguros: Publicación doctrinal de Derecho y Economía de los Seguros privados, núm. 197, 2024

La LOSSEAR no regula de forma específica el uso de modelos algorítmicos o de IA para la valoración del riesgo, pero establece el marco general dentro del cual se fijan las primas. El artículo 95 permite a las aseguradoras no publicar sus bases técnicas ni sus tarifas, lo que incrementa la opacidad en un contexto en el que las primas pueden ser calculadas mediante sistemas automatizados de risk scoring. Aunque la LOSSEAR exige que las tarifas sean suficientes, no discriminatorias y coherentes con los riesgos asumidos (artículos 93 y 94), no contempla obligaciones de transparencia sobre los datos, parámetros o inferencias utilizados por los modelos de IA para estimar el riesgo individual del tomador. En consecuencia, las aseguradoras pueden utilizar sistemas complejos de segmentación sin deber alguno de explicar al consumidor cómo se ha determinado su prima ni qué factores han influido en su cálculo, salvo las obligaciones derivadas del RGPD y del AI Act, que operan de forma transversal sobre el tratamiento de datos y las decisiones automatizadas[83].

5.2.2. Protección de datos

En el risk scoring asegurador, cuando la aceptación o denegación del seguro o la fijación de la prima depende de un sistema automatizado, nos encontramos ante una decisión exclusivamente automatizada en el sentido del artículo 22 RGPD. Ello activa los derechos específicos del interesado: a no quedar sometido a este tipo de decisiones sin que concurra una de las excepciones del artículo 22.2, y, en todo caso, a obtener intervención humana, expresar su punto de vista e impugnar el resultado. Por otro lado, el RGPD exige proporcionar información significativa sobre la lógica aplicada, la importancia del tratamiento y sus consecuencias, en virtud de los artículos 13, 14 y 15, que obligan a explicar de forma comprensible cómo los datos han contribuido al cálculo de la prima o a la decisión final, incluso cuando los datos proceden de terceros.

Además, si en el risk scoring se tratan categorías especiales de datos en el sentido del artículo 9 RGPD (por ejemplo, datos de salud en seguros médicos), el tratamiento solo es lícito si concurre una base habilitante específica del artículo 9.2, junto con garantías reforzadas de protección. A ello se suma la obligación de aplicar privacidad desde el diseño y por defecto (artículo 25 RGPD) y los principios de minimización de datos (artículo 5.1 c), limitación de la finalidad y exactitud (artículo 5.1 d), que exigen emplear únicamente información pertinente y actualizada para la valoración del riesgo, evitando que el modelo incorpore datos excesivos, no fiables o que puedan distorsionar el cálculo de la prima.

5.2.3. *Crédito al consumo*

Aunque la Directiva (UE) 2023/2225 no regula la fijación del riesgo en seguros, su lógica estructural (en particular, la restricción de fuentes de datos, la exclusión de categorías especiales del artículo 9.1 RGPD y la prohibición de utilizar información comportamental

[83] QUINTÁNS-EIRAS, M.ª R., "Digitalización y seguro: hacia una nueva declaración del riesgo", en Contratación mercantil digitalización y protección del cliente-consumidor (Dirs. Miranda Serrano y Pagador López), Marcial Pons, 2023, pp. 803-833.

ajena a la finalidad de la evaluación) ofrece un criterio orientativo para delimitar qué datos pueden emplearse legítimamente en procesos de risk scoring automatizado. La valoración del riesgo asegurado exige una conexión directa y demostrable entre el dato utilizado y el riesgo cubierto; recurrir a información que no presente una relación causal o estadística con la siniestralidad (por ejemplo, actividad en redes sociales o variables proxys no transparentes) puede vulnerar los principios de minimización y de limitación de la finalidad, además de generar discriminación indirecta. En esta línea, la estructura garantista de la Directiva (basada en pertinencia, proporcionalidad, transparencia y control humano) anticipa el estándar que previsiblemente se consolidará en los seguros que incorporen modelos algorítmicos de valoración del riesgo.

5.2.4. *Reglamento de Inteligencia Artificial*

Los sistemas de IA utilizados para la evaluación del riesgo y la fijación de primas se consideran sistemas de alto riesgo en el sentido del AI Act, lo que impone a la aseguradora obligaciones reforzadas: los conjuntos de datos deben cumplir los requisitos de calidad (artículo 10), evitando sesgos indebidos y garantizando resultados fiables; el sistema debe estar documentado y ser trazable (artículo 12), debe existir supervisión humana significativa a lo largo de su ciclo de vida (artículo 14) y debe ofrecerse una explicabilidad adecuada sobre el papel del sistema en la evaluación del riesgo y en la determinación del precio (artículo 86). Como medidas complementarias, coherentes con las prácticas propias de los AI Risk Scoring Systems, resultan necesarias auditorías periódicas de calidad de datos (representatividad, equilibrio y detección de drift) y pruebas de sesgos y robustez antes y después del despliegue, con el fin de evitar tanto degradación del rendimiento como efectos discriminatorios.

5.3. Conclusión

En la valoración automatizada del riesgo, el asegurado dispone hoy de un conjunto de derechos destinados a garantizar transparencia, control y protección frente a segmentaciones opacas o discriminatorias. En primer lugar, tiene derecho a saber si su prima o la aceptación del seguro han sido determinadas mediante un sistema automatizado y a recibir una explicación comprensible de los factores que han influido en esa valoración. Esto incluye entender qué datos se han utilizado, qué papel ha desempeñado el modelo y cómo esos elementos se han traducido en la prima o en la decisión final.

En segundo lugar, el asegurado tiene derecho a intervenir activamente cuando la decisión se ha basado total o parcialmente en un sistema de IA. Puede aportar información adicional, expresar su punto de vista y exigir una revisión humana que verifique si la decisión es adecuada, si refleja correctamente su situación y si no se han cometido errores o sesgos que afecten a su clasificación de riesgo.

El asegurado también tiene derecho a que la valoración del riesgo se base únicamente en datos pertinentes, exactos y proporcionados, evitando el uso de información irrelevante,

excesiva, desactualizada o intrusiva. Queda excluido el empleo de datos sensibles sin justificación válida y de fuentes que no guardan conexión con el riesgo asegurado, reduciendo así el peligro de inferencias inapropiadas o de prácticas que excedan lo necesario para calcular la prima.

Por último, el asegurado está protegido frente a tratamientos discriminatorios, tanto directos como indirectos. No puede verse perjudicado por variables que operen como proxies de condiciones sociales, étnicas o de vulnerabilidad (como ciertos datos sociodemográficos) cuando existan alternativas menos lesivas para valorar su riesgo real. Si la prima resulta de criterios que generan un impacto desproporcionado sobre determinados colectivos, el asegurado puede impugnar la decisión y exigir su corrección. En conjunto, el consumidor cuenta con derechos de información, explicación, revisión humana, control de los datos utilizados y protección frente a discriminación, configurando un marco destinado a evitar que la fijación automatizada de primas derive en decisiones opacas, injustificadas o excluyentes.

III. CHATBOTS Y ASISTENTES VIRTUALES

1. Riesgos en torno a chatbots

Los chatbots se utilizan cada vez más en las relaciones de consumo, tanto en la fase precontractual como en el servicio posventa. Facilitan que el consumidor formule consultas y obtenga respuestas en tiempo real mediante sistemas basados en procesamiento de lenguaje natural, que pueden funcionar con reglas predefinidas o —cada vez más— con modelos de IA generativa. En todo caso, la interacción inicial suele producirse sin intervención humana.

En la fase precontractual, se emplean para proporcionar información sobre productos y servicios, plazos de entrega, garantías o políticas de devolución, así como para guiar al usuario en el proceso de compra mediante asistentes conversacionales integrados en sitios web o aplicaciones móviles. Su uso agiliza la experiencia y reduce la necesidad de atención humana, pero también genera riesgos evidentes cuando la información ofrecida es incompleta, imprecisa o contradictoria con las condiciones contractuales.

Un ejemplo paradigmático es el caso de Air Canada. En 2022, el chatbot de la aerolínea informó erróneamente a un cliente sobre el plazo para solicitar un reembolso tras el fallecimiento de un familiar. El pasajero confió en esa información y presentó la solicitud fuera de plazo, pero un tribunal canadiense obligó a la compañía a respetar lo dicho por su chatbot, recordando que la empresa no puede desvincularse de la responsabilidad de la información facilitada por sus sistemas automatizados.

El uso más intensivo de los chatbots se produce, sin embargo, en el contexto del servicio posventa o de atención al cliente. Los chatbots pueden mejorar la eficiencia en la comunicación con los consumidores, pero su utilización exclusiva o por defecto puede

dificultar el ejercicio de derechos. La imposibilidad de acceder a un interlocutor humano puede funcionar como un obstáculo técnico que, en la práctica, impida resolver incidencias, ejercer el desistimiento o solicitar reparaciones. Según la encuesta de la Comisión publicada en 2024, el 44 % de los consumidores experimentó dificultades para resolver un problema porque solo tenían acceso a un chatbot, y el 64 % considera preocupante que los comerciantes se comuniquen exclusivamente por este medio. Por ello, el 65 % de las partes interesadas pidió reconocer el derecho a solicitar la intervención de un humano cuando los chatbots gestionan reclamaciones u otras consultas[84].

Además, surgen dudas sobre en qué medida los chatbots pueden garantizar el cumplimiento de las obligaciones de derecho de consumo cuando integran contenidos patrocinados o comunicaciones comerciales. Si el comerciante recibe pagos por promocionar productos de terceros a través del chatbot, deberá garantizar que esta publicidad sea claramente identificable, como ocurre en los mercados en línea o los motores de búsqueda. Más incierta es la situación cuando el proveedor del chatbot no recibe pagos, pero el contenido generado por el sistema incorpora sesgos o preferencias derivadas del entrenamiento del modelo. A medida que estas herramientas se utilicen como motores de búsqueda conversacionales, será necesario supervisar su impacto sobre la transparencia publicitaria en el recorrido transaccional del consumidor.

2. Riesgos en relación con asistentes virtuales

El despliegue de tecnologías como la IA y los sistemas automatizados está permitiendo que determinados contratos se celebren y ejecuten con una intervención humana cada vez menor. En el ámbito B2C, el principal caso de uso son los asistentes virtuales que facilitan la compra automatizada de productos y servicios. Estos sistemas pueden informar, recomendar, comparar opciones y, en algunos casos, ejecutar transacciones en nombre del consumidor. Pueden funcionar como servicios digitales independientes o integrarse en dispositivos IoT (por ejemplo, impresoras que realizan pedidos automáticos de tinta cuando detectan niveles bajos)[85].

En la práctica, predominan todavía los asistentes que informan o recomiendan, mientras que las herramientas realmente autónomas que toman decisiones de compra de forma independiente aún no están extendidas en los mercados B2C. No obstante, el desarrollo de modelos basados en IA incrementa progresivamente el grado de autonomía funcional de estos sistemas.

[84] European Commission, Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness, SWD (2024) 230 final, Brussels, 3 October 2024.
[85] PACHECO JIMENEZ, N., "Contratos algorítmicos y toma de decisiones automatizada. El papel de la normativa europea de consumo", *Web CESCO*, 2024, https://centrodeestudiosdeconsumo.com/images/Contratos_algoritmicos_y_toma_de_decisiones_automatizada.pdf

El uso de asistentes virtuales[86] implica una delegación parcial del control contractual. Algunos permiten que el consumidor apruebe cada operación antes de su perfección jurídica; otros solo admiten un control ex post, como la posibilidad de anular la transacción durante un corto período; y los más avanzados, basados en aprendizaje automático, pueden actuar con un margen muy reducido de supervisión humana.

Esta externalización del proceso decisorio genera riesgos específicos. El consumidor puede enfrentarse a compras no deseadas (como suscripciones involuntarias), o a dificultades técnicas o contractuales para desactivar la herramienta y recuperar la contratación manual. También pueden existir déficits de transparencia sobre el funcionamiento del asistente. Por ejemplo, qué proveedores tiene integrados, qué criterios utiliza para seleccionar productos o si favorece indebidamente a operadores vinculados, así como incertidumbre sobre la utilización de los datos personales empleados para alimentar el sistema.

A ello se añaden riesgos derivados de la interacción con los comerciantes. Aunque muchos operadores aceptan transacciones automatizadas, otros pueden bloquear el acceso de estas herramientas a su interfaz, exigir confirmación humana para validar la operación o introducir cláusulas que limiten o invaliden contratos celebrados mediante automatización. En otros casos, la falta de interoperabilidad o de legibilidad mecánica de la web puede impedir directamente la operativa del asistente. Estas salvaguardias pueden proteger al consumidor frente a compras indeseadas, pero también pueden convertirse en obstáculos o incluso en discriminaciones frente a quienes optan por utilizar herramientas automatizadas[87].

3. Marco normativo

3.1. Reglamento de Inteligencia Artificial

El uso de chatbots o asistentes digitales activa las obligaciones de transparencia previstas en el artículo 50 AI Act. Este precepto exige que, cuando una persona física interactúe con un sistema de IA destinado a tratar directamente con usuarios, debe ser informada de que la interacción se produce con un sistema automatizado (artículo 50.1). La información debe facilitarse de manera clara y distinguible, a más tardar con ocasión de la primera interacción, y cumplir los requisitos de accesibilidad aplicables (art 50.4). Esta obligación no es exigible cuando el carácter automatizado del servicio resulte evidente para una persona razonablemente informada, atenta y perspicaz, teniendo en cuenta el contexto y las circunstancias de uso (artículo 50.1).

[86] El artículo 2.12 RMD define al "asistente virtual" como un software que puede procesar peticiones, tareas o preguntas, también las formuladas mediante sonidos, imágenes, texto, gestos o movimientos y que, basándose en dichas peticiones, tareas o preguntas, proporciona acceso a otros servicios o controla dispositivos físicos conectados;

[87] European Commission, Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness, SWD (2024) 230 final, Brussels, 3 October 2024.

Además, el AI Act exige que en todos los sistemas de IA de alto riesgo haya supervisión humana (artículo 14) y que las personas afectadas puedan solicitar una explicación sobre decisiones adoptadas sobre la base de la salida del sistema de IA (artículo 86). Con todo, es probable que los chatbots no se consideren sistemas de IA de alto riesgo (cfr. artículo 5 y Anexo III AI Act).

3.2. Servicios digitales

El DSA ofrece una referencia útil para comprender los límites de la automatización en los servicios digitales, especialmente cuando la interacción afecta a derechos de los usuarios. En primer lugar, el artículo 12 exige que los proveedores de servicios de intermediación en línea (incluidos los mercados, plataformas de alojamiento de contenidos y motores de búsqueda) mantengan un punto de contacto único que no se base exclusivamente en herramientas automatizadas y permita una comunicación efectiva con una persona, cuando así lo solicite el usuario. En segundo lugar, el sistema interno de gestión de reclamaciones de las plataformas en línea debe garantizar que las decisiones motivadas sobre retirada de contenidos, suspensión de cuentas o restricción de la monetización no se adopten exclusivamente por medios automatizados, sino bajo la supervisión de personal adecuadamente cualificado (artículo 20.6).

Estos dos supuestos —punto de contacto único (artículo 12) y sistema interno de reclamaciones (artículo 20)— ilustran el enfoque del DSA: incluso en entornos altamente digitalizados, ciertos puntos de interacción no pueden ser completamente automatizados, porque ello comprometería la posibilidad de defensa del usuario y su derecho a obtener una valoración humana cuando las decisiones tienen un impacto relevante sobre su posición jurídica en la plataforma.

3.3. Servicios financieros a distancia

La Directiva (UE) 2023/2673, introduce un nuevo artículo 16 quinquies en la Directiva 2011/83/UE, cuyo apartado 3 establece el derecho a solicitar intervención humana cuando interactúe con el comerciante a través de interfaces en línea totalmente automatizadas, tales como robots conversacionales (chatbots), asesoramiento robotizado, herramientas interactivas o medios similares (considerando 15). El consumidor siempre debe poder obtener, en la fase precontractual, intervención humana en nombre del comerciante, de manera gratuita y durante el horario comercial del comerciante. El consumidor también debe tener derecho a solicitar intervención humana (en casos justificados y sin que ello suponga una carga indebida para el comerciante) una vez celebrado el contrato a distancia. Esto podría incluir el derecho a una intervención humana cuando se prorrogue un contrato, en caso de dificultades importantes para el consumidor o cuando sea necesaria una explicación más detallada sobre las condiciones contractuales (considerando 40).

3.4. Protección de datos

Como hemos explicado varias veces, el artículo 22 RGPD reconoce el derecho del interesado a no ser objeto de decisiones individuales basadas exclusivamente en tratamiento automatizado de datos personales que produzcan efectos jurídicos sobre él o le afecten de manera significativa. Este límite es especialmente relevante cuando chatbots o asistentes virtuales intervienen en decisiones que determinan la admisión, denegación o modificación de un servicio, o en la gestión de reclamaciones, de modo que la respuesta automatizada pueda condicionar directamente la posición jurídica del consumidor.

Si el resultado generado por el chatbot o el asistente virtual constituye la única base de la decisión adoptada por el comerciante —por ejemplo, denegar la contratación, rechazar una reclamación o imponer condiciones menos favorables—, podría activarse la prohibición del artículo 22. La prohibición no opera cuando el interesado ha otorgado su consentimiento explícito, cuando la decisión es necesaria para la celebración o ejecución del contrato o cuando está autorizada por el Derecho de la Unión o de los Estados miembros. Pero incluso en estos casos, el responsable debe garantizar salvaguardias adecuadas, entre ellas la intervención humana, la posibilidad de que el consumidor exponga su punto de vista y el derecho a impugnar la decisión.

En suma, aunque chatbots y asistentes virtuales pueden automatizar parte de la atención y de la contratación, no pueden reemplazar por completo la supervisión humana cuando sus resultados pueden producir efectos jurídicos o afectar significativamente a los derechos del consumidor.

3.5. Instrumentos financieros: roboadvisors

El asesoramiento automatizado se ha convertido en un elemento clave de la digitalización de los servicios financieros. Comprende plataformas que utilizan sistemas algorítmicos para perfilar al cliente, recomendar productos, ejecutar órdenes de inversión y reajustar carteras de manera periódica.

En el mercado español predominan modelos híbridos, en los que el algoritmo realiza la mayor parte del trabajo de análisis, asignación de activos y rebalanceo, mientras existe supervisión humana para validar las recomendaciones y monitorizar el servicio. Este modelo permite ofrecer carteras diversificadas y adaptadas al perfil de riesgo del cliente con costes muy reducidos, abriendo el acceso al asesoramiento a un público minorista más amplio. La tendencia es hacia una automatización cada vez más completa y hacia la hiperpersonalización de las recomendaciones mediante el uso de big data e IA.

El régimen jurídico de los roboadvisors debe determinarse atendiendo a las funcionalidades efectivamente prestadas. Cuando el sistema emite recomendaciones personalizadas, se configura como asesoramiento en materia de inversión (artículo 4.1.4 MiFID II). Si, además, gestiona y rebalancea carteras de forma discrecional, se considera

gestión de carteras, con el consiguiente cumplimiento de las obligaciones de autorización, inscripción y supervisión previstas en los artículos 140, 143 y 150 del TRLMV y en el Real Decreto 217/2008. Cuando el sistema ejecuta automáticamente órdenes en el mercado, puede quedar sometido al régimen de negociación algorítmica (artículos 4.1.39 y 17 MiFID II), que exige controles de riesgo, registro de estrategias y supervisión reforzada. En todos los casos, el prestador debe cumplir los deberes de información clara e imparcial, realizar los test de idoneidad y conveniencia, gestionar los conflictos de interés y actuar en el mejor interés del cliente (artículos 209 TRLMV y 54 del Reglamento Delegado 2017/565).

La responsabilidad por el cumplimiento normativo recae en la entidad que despliega el roboadvisor en el mercado, que debe garantizar la calidad y fiabilidad de los algoritmos, sin perjuicio de que pueda exigir contractualmente a los proveedores de tecnología garantías y obligaciones de mantenimiento y auditoría.

3.6. Proyecto de ley atención a la clientela

El PLAC admite el uso de sistemas automatizados para la atención a la clientela, pero establece garantías para que no sustituyan por completo la interacción humana ni limiten los derechos de los consumidores.

Según el artículo 8**,** se prohíbe que la atención se realice exclusivamente mediante contestadores automáticos, bots conversacionales o medios análogos. Si se usan estos sistemas, el consumidor debe poder solicitar en cualquier momento ser atendido por un operador humano en tiempo real**,** que se identificará al inicio de la conversación. Si el consumidor no queda satisfecho, puede pedir que le atienda un supervisor o departamento de calidad durante la misma interacción.

Por su parte, el artículo 9 establece que la empresa debe asegurarse de que los medios automatizados estén diseñados y gestionados por personal especializado. Este personal debe contar con formación para garantizar que el sistema sea eficaz y adecuado, incluyendo atención a personas consumidoras vulnerables.

3.7. Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts

El European Law Institute propone un conjunto de reglas no vinculantes para orientar el uso de asistentes virtuales en la contratación con consumidores.[88]

[88] https://www.europeanlawinstitute.eu/projects-instruments/instruments/eli-guiding-principles-and-model-rules-on-digital-assistants-for-consumer-contracts/

Transparencia. El empresario debe informar de forma clara cuando la interacción o la contratación se realiza mediante un chatbot. Si no lo hace, el consumidor puede resolver el contrato sin penalización si acredita que no lo habría celebrado de haber conocido este hecho. No es necesario identificar al chatbot cuando su uso resulte evidente para un consumidor razonable.

Información precontractual. Aunque el proceso sea automatizado, el empresario sigue obligado a proporcionar toda la información precontractual exigida por la ley. Además, debe facilitarla en un formato legible por máquina, que permita al consumidor almacenarla y reutilizarla.

Validez y vinculación jurídica. La intervención de un asistente digital no afecta a la validez del contrato. La empresa queda vinculada por las declaraciones y decisiones generadas por el asistente digital, salvo que concurran fallos graves e imprevisibles del sistema. Así ocurrió en el conocido caso del chatbot de Air Canada, que ofreció erróneamente un descuento: la compañía tuvo que reembolsar al consumidor.

Dark patterns. Cuando el chatbot emplea mecanismos que distorsionan de forma sustancial la capacidad del consumidor para decidir libremente, el consumidor puede dejar sin efecto el contrato.

4. Conclusión

Del análisis anterior se desprende un conjunto definido de derechos que protegen al consumidor frente al uso de chatbots, asistentes virtuales y roboadvisors. Los consumidores tienen derecho a ser informados de que la interacción se realiza con un sistema automatizado cuando ello no resulte evidente, y a recibir por esta vía toda la información precontractual que les deba ser facilitada. Cuando la automatización dificulta resolver un problema, tramitar una reclamación o comprender adecuadamente las condiciones ofrecidas, pueden solicitar la intervención de una persona y acceder a un canal humano efectivo.

IV. SCALPER BOTS

1. Riesgos

Los scalper bots se utilizan para adquirir automáticamente productos de gran demanda con el propósito de revenderlos a un precio más elevado. Aunque estas prácticas se producen sobre todo en la compra de entradas para eventos, hoy afectan también a consolas de videojuegos, tarjetas gráficas o zapatillas deportivas.

Para los consumidores, este fenómeno supone un riesgo claro: los bots acaparan el stock en milésimas de segundo, elevan artificialmente la escasez y fuerzan a muchos compradores a recurrir al mercado de reventa a precios significativamente superiores, limitando el acceso efectivo a bienes muy demandados. En la encuesta realizada por la Comisión Europea, solo el 27 % de los encuestados consideró que el Derecho de consumo

de la UE aporta seguridad regulatoria en un grado moderado o alto respecto al uso de scalping.[89]

2. Marco normativo: prácticas desleales

La Directiva (UE) 2019/2161 modificó el anexo I Directiva 2005/29/CE, para introducir una prohibición del uso de bots automatizados para acaparar entradas de eventos o espectáculos culturales o deportivos con fines de reventa, cuando ello implique eludir los límites impuestos al número de entradas que una persona puede comprar o cualquier otra norma aplicable a la compra de entradas.

En este sentido, el artículo 27.1 LCD establece que se consideran desleales por engañosas las prácticas que consistan en la reventa de entradas de espectáculos a los consumidores o usuarios si el empresario las adquirió empleando medios automatizados para sortear cualquier límite impuesto al número de entradas que puede adquirir cada persona o cualquier otra norma aplicable a la compra de entradas.

3. Conclusión

Fuera del ámbito específico de las entradas para eventos, el uso de scalper bots carece hoy de una regulación directa en el Derecho de consumo de la UE. La intervención normativa se limita a prohibir el acaparamiento automatizado de entradas con fines de reventa, mientras que la utilización de bots para adquirir otros bienes de alta demanda (como consolas o productos electrónicos) no está expresamente cubierta. En estos casos, solo cabría actuar mediante la aplicación general de la Directiva 2005/29/CE, en particular frente a prácticas engañosas vinculadas al proceso de compra o a la información ofrecida al consumidor.

La Comisión Europea ha señalado, además, las dificultades inherentes a una regulación más amplia del scalping: desde la delimitación exacta de la práctica hasta la fijación de precios de reventa admisibles o los problemas de ejecución derivados de su dimensión transfronteriza. En la consulta pública, una mayoría significativa de partes interesadas manifestó su preferencia por una intervención más estricta. En este contexto, la evolución del uso de scalper bots, tanto en el mercado de entradas como en otros bienes, deberá seguir observándose para valorar si el perjuicio a los consumidores justifica una respuesta normativa más amplia[90].

V. RESEÑAS

1. Riesgos

Muchas plataformas en línea, así como los comerciantes individuales, ofrecen a los consumidores la posibilidad de informar a otros consumidores de su experiencia con

[89] European Commission, Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness, SWD (2024) 230 final, Brussels, 3 October 2024.
[90] European Commission, Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness, SWD (2024) 230 final, Brussels, 3 October 2024.

diferentes productos o comerciantes. Los servicios de reseñas se suelen incluir en los mercados en línea, los motores de búsqueda, los sitios web especializados en la valoración de viajes, las herramientas comparativas y las redes sociales. Diversos estudios demuestran la importancia de las reseñas para las decisiones de compra de los consumidores[91]. Por lo tanto, es importante que los comerciantes que dan acceso a las reseñas de los consumidores adopten medidas razonables y proporcionadas para garantizar que reflejan la experiencia de consumidores reales con el producto de que se trate.

Sin embargo, se han detectado una serie de prácticas desleales en este ámbito. Los comerciantes utilizan diferentes técnicas para aumentar el número de reseñas positivas de sus productos en las plataformas o para reducir o restar importancia al número de reseñas negativas. Para impulsar sus productos, algunos comerciantes organizan la publicación de reseñas positivas falsas mediante, por ejemplo, la participación de empresas especializadas que contratan a consumidores reales a través de redes sociales u otros medios. A continuación, estos consumidores compran los productos de los respectivos comerciantes en plataformas en línea y dejan calificaciones de cinco estrellas a cambio de beneficios específicos, o los comerciantes incentivan a los consumidores para probar sus productos a cambio de publicar sus reseñas (reseñas patrocinadas) sin desvelar el patrocinio[92].

Un ejemplo real es el de un comerciante que publicó "me gusta" en sus productos dentales en su propio sitio web y declaró que se trataba de "reseñas garantizadas de clientes reales". Posteriormente, asoció los "me gusta" a un sitio web de valoración en el que las reseñas positivas de los clientes se vieron favorecidas en comparación con las neutras o negativas. Un órgano jurisdiccional alemán consideró engañoso que el comerciante declarase que eran 2 reseñas garantizadas de clientes reales[93].

Además, las reseñas incentivadas o falsas pueden influir en la clasificación del producto y, por tanto, en la visibilidad en la plataforma si los parámetros de búsqueda de esta tienen en cuenta la puntuación de las reseñas. Tales prácticas distorsionan las opciones de los consumidores. Aunque algunas plataformas informan de la adopción de medidas para limitar las reseñas falsas, el problema parece ir en aumento[94]. El efecto de estas prácticas engañosas se ve agravado por la constante falta de oferta de reseñas normales, en particular para los nuevos productos o para los recién llegados al mercado[95].

---

[91] https://apachedigital.io/wp-content/uploads/2021/09/210922_ECLLYC_Apache_Informe.pdf

[92] European Commission, Commission Staff Working Document – Fitness Check of EU consumer law on digital fairness, SWD (2024) 230 final, Brussels, 3 October 2024.

[93] OLG Düsseldorf, 19.2.2013, Az. I – 20 U 55/12

[94] https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_25_762/IP_25_762_ES.pdf

[95] Por ejemplo, la Bundeskartellamt alemana estimó que solo el 1 % de los consumidores publican reseñan tras su experiencia de compra; véase «Konsultationspapier zur Sektoruntersuchung Nutzerbewertungen», punto E 1.2: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/18_06_2020_SU_Nutzerbewertungen_Konsultation.html.

Nótese que estas prácticas pueden verse espoleadas por la IA. Un mismo anunciante, mediante bots, puede propagar reseñas ficticias, testimonios inventados, generados por algoritmos de lenguaje natural.

2. Marco normativo: prácticas desleales

La Directiva (UE) 2019/2161 incorporó como práctica desleal la fabricación o difusión de reseñas falsas y la manipulación de reseñas auténticas en línea. En su transposición, el artículo 20.4 TRLGDCU exige que los comerciantes que faciliten acceso a reseñas informen de si garantizan o no que estas proceden de consumidores que realmente han utilizado o adquirido el bien o servicio, así como de la forma en que procesan dichas reseñas. Esta obligación se aplica a cualquier comerciante que proporcione acceso a reseñas, incluso cuando muestre en su interfaz reseñas generadas por terceros, como ocurre con herramientas de valoración especializadas (Google, TripAdvisor, etc.).

El considerando 47 de la Directiva 2019/2161 aclara que la información exigida no se limita a las medidas destinadas a verificar la autenticidad de las reseñas, sino que abarca también el modo en que estas se gestionan en general: si todas las reseñas se publican o existen filtros, cómo se obtienen, cómo se calculan las puntuaciones medias y si pueden estar influidas por reseñas patrocinadas o por relaciones contractuales con los comerciantes alojados en la plataforma. Esta información es relevante para determinar si el comerciante puede presentar legítimamente las reseñas como opiniones de consumidores reales, de conformidad con el artículo 27.7 LCD. Además, debe proporcionarse de manera clara, comprensible y accesible desde la propia interfaz donde se muestran las reseñas, incluso mediante hipervínculos fácilmente identificables.

El artículo 27.7 LCD considera práctica engañosa afirmar, de forma explícita o implícita, que las reseñas proceden de consumidores reales sin adoptar medidas razonables y proporcionadas para verificarlo. No es necesario que el comerciante lo declare expresamente: referencias genéricas como “opiniones de clientes”, “reseñas de consumidores” o similares pueden generar en el consumidor medio la impresión de que las reseñas proceden de usuarios reales. Las medidas razonables y proporcionadas dependen del modelo de negocio, de la magnitud del comerciante y del nivel de riesgo. Un marketplace que publica reseñas de sus propios clientes puede necesitar mecanismos distintos de un servicio de valoración abierto al público. En todo caso, las medidas no deben disuadir injustificadamente a los consumidores reales de dejar reseñas.

Entre las medidas consideradas razonables, el considerando 47 menciona solicitar información que permita verificar la compra (p. ej., número de reserva), exigir registro de usuarios, aplicar controles técnicos (verificación de IP, correo electrónico), establecer reglas que prohíban reseñas patrocinadas no divulgadas, emplear herramientas automáticas de detección de fraude y disponer de procedimientos para tramitar reclamaciones sobre reseñas sospechosas. Esta información permitirá a usuarios y autoridades evaluar las medidas adoptadas por los comerciantes, en comparación también con las mejores prácticas del sector, incluidas las recogidas en la norma ISO 20488:2018 sobre recopilación, moderación y publicación de reseñas.

El artículo 27.8 LCD introduce un segundo bloque de prácticas prohibidas: (i) añadir o encargar reseñas o aprobaciones falsas, y (ii) distorsionar reseñas o aprobaciones sociales auténticas con el fin de promocionar bienes o servicios. El primer grupo incluye, entre otras prácticas, comprar reseñas a terceros (como "fábricas de me gusta" o consumidores incentivados económicamente). Se aplica tanto a profesionales como a consumidores que actúen en nombre o por cuenta del comerciante, pero no alcanza a plataformas que simplemente alojan reseñas sin intervenir en su presentación. El segundo grupo se dirige a comerciantes, incluidas plataformas, que manipulan la presentación de reseñas o aprobaciones sociales, por ejemplo, publicando solo reseñas positivas, eliminando negativas, proporcionando plantillas prediseñadas para fomentar comentarios favorables o agregando puntuaciones según criterios no divulgados. El concepto de "aprobaciones" debe interpretarse ampliamente e incluye prácticas basadas en seguidores, reacciones y visualizaciones falsas.

La prohibición de distorsión de reseñas opera sin perjuicio del derecho, y en ocasiones la obligación, del comerciante de eliminar reseñas negativas falsas cuando ello forme parte de las medidas destinadas a garantizar que las reseñas reflejan la experiencia real de usuarios auténticos. Sin embargo, la supresión de reseñas negativas válidas puede inducir al consumidor medio a mantener la relación con el comerciante o, en el caso de plataformas, a elegir al comerciante manipulado en detrimento de un competidor que no haya incurrido en tales prácticas. Ello también se aplica cuando comerciantes colaboran con consumidores o con otros comerciantes que alojan reseñas para impedir la publicación de opiniones negativas o eliminarlas tras su difusión[96].

Estas disposiciones se aplican tanto a las plataformas y comerciantes que ponen a disposición reseñas como a cualquier comerciante que organice su suministro en beneficio de otros. Las prácticas comerciales están sujetas a la LCD con independencia de que se promocionen productos propios o ajenos. Las normas no se aplican a los consumidores que publican reseñas salvo que actúen en nombre o por cuenta del comerciante. También se extienden a reseñas centradas en el desempeño del comerciante en la venta de sus productos (por ejemplo, calidad del servicio, fiabilidad o rapidez de entrega)— cuando estas influyen en la decisión del consumidor sobre la transacción. En cambio, quedan excluidas las reseñas sobre aspectos no relacionados con la relación B2C, como responsabilidad social, condiciones laborales, fiscalidad o cuestiones éticas.

3. Conclusión

Del análisis anterior se desprende que, en materia de reseñas, los consumidores tienen derecho a recibir información veraz y a que el empresario les comunique de forma clara si verifica o no la autenticidad de las opiniones publicadas. También tienen derecho a saber qué medidas se aplican para comprobar que las reseñas proceden de personas que han adquirido o utilizado realmente el bien o servicio. Asimismo, están protegidos frente

[96] 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), p. 95

a la inclusión de reseñas falsas o manipuladas, que constituyen prácticas engañosas y distorsionan la capacidad del consumidor para formarse una decisión informada.

VI. FALTAS DE CONFORMIDAD DE PRODUCTOS QUE INCORPORAN IA

Los productos y servicios digitales que integran sistemas de IA, como asistentes virtuales, aplicaciones que generan contenidos, robots domésticos con navegación autónoma o vehículos que incorporan funciones avanzadas de ayuda a la conducción, no cuentan con un régimen específico en las Directivas europeas de conformidad. Ni la Directiva 2019/770 sobre contenidos y servicios digitales ni la Directiva 2019/771 sobre compraventa de bienes, también de los que incorporan elementos digitales, transpuestas ambas al TRLGDCU, fueron concebidas para abordar cuestiones relativas a las faltas de conformidad o defectos de funcionamiento de los sistemas de IA.

Con todo, una parte relevante de sus requisitos de conformidad sí resulta aplicable cuando un contenido, servicio o bien incorpora IA, especialmente en lo relativo a la funcionalidad, interoperabilidad, instalación y actualizaciones. En particular, tales requisitos pueden ser relevantes para el contrato de suministro de un asistente digital y, por ende, para los problemas que puedan surgir en el funcionamiento de este. Igualmente, ambas directivas son también pertinentes para el contrato algorítmico cuando se trata de un contrato para compraventa de bienes o de un contrato de suministro de contenidos o servicios digitales. De hecho, cualquiera de las dos Directivas constituiría una base jurídica para el consumidor que busca reparación en aquellos supuestos en los que un asistente digital ha actuado de una manera diferente a la razonablemente esperada y esto supone una falta de conformidad del propio asistente digital o del elemento físico que incorpora aquel[97].

En el ámbito de los contenidos y servicios digitales, el artículo 7 de la Directiva 2019/770 (artículo 115 bis TRLGDCU) exige que el producto cumpla lo pactado en el contrato en cuanto a funcionalidad, compatibilidad, interoperabilidad y demás características de rendimiento. Esto puede operar directamente respecto de prestaciones basadas en IA. Por ejemplo, un servicio digital que utiliza IA para editar fotografías debe ofrecer el nivel de precisión anunciado; si el modelo genera resultados defectuosos, reconoce mal objetos o no ejecuta las funciones prometidas, puede apreciarse una falta de conformidad. Asimismo, el empresario debe proporcionar instrucciones claras para la instalación y uso, lo que cobra especial relevancia cuando el funcionamiento del modelo depende de permisos, configuraciones o elementos externos.

El artículo 8 de la Directiva 2019/770 (artículo 115 ter TRLCU) añade requisitos objetivos de conformidad relacionados con lo que un consumidor razonablemente espera de un servicio digital del mismo tipo, como aspectos relativos a la seguridad[98], la funcionalidad o la accesibilidad. Esto es especialmente relevante para sistemas de IA. Por ejemplo, un asistente virtual que aprende del uso debe mantener un nivel razonable de operatividad y

[97] European Law Institute, "Eu Consumer Law and Automated Decision-Making (ADM): Is EU Consumer Law Ready for ADM?", 2023, pp. 44-45.
[98] IZQUIERDO GRAU, G., "La incidencia de la ciberseguridad en la conformidad de los bienes con elementos digitales", *Revista Crítica De Derecho Inmobiliario*, 799, 2731-2748, 2024.

no degradarse de forma inesperada. El empresario debe, además, suministrar las actualizaciones necesarias, incluidas las de seguridad, para mantener la conformidad durante el período esperado, lo que en el caso de la IA puede implicar parches para corregir fallos del modelo, mitigar sesgos o resolver vulnerabilidades detectadas.

Respecto de los bienes con elementos digitales, la Directiva 2019/771 establece obligaciones similares. El artículo 6 exige que el bien posea la funcionalidad, compatibilidad e interoperabilidad acordadas. Así, un robot aspirador con navegación autónoma debe mapear el entorno con la precisión anunciada, identificar obstáculos y mantener un funcionamiento adecuado. El artículo 7 añade requisitos objetivos, como que el bien debe presentar la funcionalidad, compatibilidad y seguridad que el consumidor puede esperar normalmente de un producto similar. En bienes con IA, como electrodomésticos conectados o dispositivos domóticos, se proyecta sobre la estabilidad del modelo, la fiabilidad de sus inferencias y su integración con otros servicios digitales.

El vendedor, además, debe proporcionar actualizaciones necesarias, incluidas las de seguridad (artículo 7.3), lo que resulta especialmente relevante cuando el funcionamiento del bien depende de modelos de IA que requieren mejoras periódicas o corrección de errores. En caso de instalación defectuosa, si se debe a instrucciones inadecuadas, la falta de conformidad se atribuye igualmente al vendedor (artículo 8), algo especialmente frecuente en sistemas que requieren calibración inicial o conexión con otros dispositivos.

En conjunto, aunque las Directivas 2019/770 y 2019/771 no regulan la IA como tal, sí ofrecen un marco jurídico útil para exigir prestaciones mínimas de funcionalidad, interoperabilidad, seguridad y actualización cuando el sistema de IA forma parte del contenido, servicio o bien adquirido. Se trata de un régimen complementario, que no aborda los riesgos específicos del aprendizaje automático, pero que proporciona herramientas jurídicas para reaccionar frente a fallos de funcionamiento o incumplimientos que afecten al rendimiento o a la integridad del sistema de IA integrado en el producto. Como es sabido, el empresario responderá ante el consumidor o usuario de cualquier falta de conformidad que exista en el momento de la entrega del bien, contenido o servicio digital, pudiendo el consumidor o usuario, mediante una simple declaración, exigir al empresario la subsanación de dicha falta de conformidad, la reducción del precio o la resolución del contrato. En cualquiera de estos supuestos el consumidor o usuario podrá exigir, además, la indemnización de daños y perjuicios, si procede (artículo 117 TRLGDCU).

VII. RESPONSABILIDAD CIVIL EXTRACONTRACTUAL POR SISTEMAS DE IA DEFECTUOSOS

1. Planteamiento

Según el considerando 3 de la Directiva (UE) 2024/2853, “la Directiva 85/374/CEE (…) debería *revisarse* a la luz de los avances relacionados con las *nuevas tecnologías, incluida la inteligencia artificial (IA)*”.

Nótese que, a pesar de la señalada necesidad de adaptar la normativa de responsabilidad por los daños causados por productos defectuosos a la IA, lo cierto es que el articulado de la Directiva (UE) 2024/2853 omite cualquier referencia expresa a ella. Las menciones a la IA se limitan a unos pocos considerandos (3, 13, 40 y 48), algunos de ellos prácticamente decorativos, lo que contrasta con la supuesta importancia que tiene la adaptación de la normativa a esta nueva tecnología.

Así pues, surge la duda de si actualmente la IA es tan trascendental en el nuevo marco de responsabilidad por los daños causados por productos defectuosos. A tratar de esclarecer ese interrogante dedicamos las siguientes líneas.

2. Sistema de IA y producto

Según el artículo 4.1 Directiva (UE) 2024/2853, producto es "cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; incluye la electricidad, los archivos de fabricación digital, las materias primas y los *programas informáticos*". Además, el artículo 4.4. Directiva (UE) 2024/2853 define como componente a "cualquier artículo, ya sea tangible o intangible, materia prima o servicio conexo, que está integrado en un producto o interconectado con él".

Como se observa, ni rastro del sistema de IA en las definiciones de producto y de componente. Con todo, el considerando 13 Directiva (UE) 2024/2853, al poner ejemplos de programas informáticos, incluye los "sistemas de IA". Posteriormente, dicho considerando manifiesta que el proveedor de sistemas de IA, en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, AI Act), debe ser tratado como un fabricante.

Por lo tanto, teniendo en cuenta que el articulado de la Directiva (UE) 2024/2853 incluye los programas informáticos como productos y que el considerando 13 menciona específicamente a los sistemas de IA como ejemplos de tales programas, parece razonable concluir que, en principio, un sistema de IA puede ser un producto en sí mismo o un componente de un producto.

3. Sistemas de IA que se utilizan en la actualidad por consumidores

El artículo 4.1 AI Act define el sistema de IA como "un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales".

Pues bien, cabe preguntarse qué productos o componentes de productos que se utilizan hoy en día por los consumidores y otras personas físicas encajarían en la definición de sistema de IA.

Por un lado, hay sistemas de IA que son productos (intangibles) en sí mismos, como Chat GPT, cuya función es generar texto (o voz, como Alexa y Siri) a partir del input que reciben. Con todo, estos sistemas de IA no entrarían en el ámbito de aplicación de la Directiva (UE) 2024/2853. En efecto, tanto el TJUE (sentencia 10 junio 2021, Krone-Verlag, C-65/20) como la propia Directiva (UE) 2024/2853 (considerando 13) consideran que la información no debe considerarse un producto, si bien la Directiva (UE) 2024/2853 se refiere a archivos digitales (archivos multimedia o libros electrónicos) o al mero código fuente de los programas informáticos. La razón de esta exclusión descansa en que el daño cubierto por la Directiva (UE) 2024/2853 debe ser causado directamente por el producto defectuoso (prótesis, botella de vidrio, automóvil, fármaco, avión, gas butano, insecticida, cohete, alimento, etc.) y no por la información emitida por él. Nótese que la información procedente de Chat GPT, y otros chatbot similares, no causaría de forma directa daños a las personas o a los bienes, daños que únicamente acaecerían si intervienen en el curso causal factores intermedios, como la conducta de la propia víctima. Es decir, el daño sería una consecuencia remota de la información de salida "defectuosa". Por lo demás, la información defectuosa emitida por algunos chatbot podría causar daños económicos en el ámbito contractual, daños que escaparían de la Directiva (UE) 2024/2853. Así sucedería cuando el chatbot de Air Canada informa a un usuario sobre un descuento en el precio de unos billetes, descuento que realmente no era ofrecido por la compañía, quien, por consiguiente, no quiere reembolsar el importe al cliente.

Por otro lado, los sistemas de IA se incorporan a productos tangibles. Un ejemplo común son los vehículos que circulan por vías públicas. Algunos funcionan de forma totalmente autónoma, sin conductor, como la flota de robo-taxis Waymo (de Google), operativos solo en zonas específicas de EE. UU. Según la clasificación del nivel de automatización de vehículos de la *"Society of Automotive Engineers"* (SAE), que clasifica el nivel de automatización en función del nivel de atención e intervención del humano en la conducción, los Waymo poseen un nivel de autonomía 4 (de 5 niveles posibles), de modo que realizan todas las tareas de conducción, incluso si el conductor (un humano en remoto) no responde a una solicitud de intervención.

Con todo, los vehículos totalmente autónomos (niveles 4 y 5 SAE) prácticamente no operan en el mercado. Los que sí operan con más fuerza son coches equipados con sistemas de nivel 1 o 2. En el nivel 1, el coche nos ayuda en las funciones de dirección (asistente activo de mantenimiento de carril) o de frenada y aceleración, como un control de crucero activo. En el nivel 2, el coche pasa a poder controlar ambas funciones en un entorno controlado (dirección y aceleración o frenado), como por ejemplo el Autopilot FSD de Tesla. Es a partir del nivel 3 cuando se puede decir que el coche conduce solo, pero en determinadas circunstancias. En este nivel 3, en caso de necesidad, el coche requerirá que el conductor retome el control del coche. Nótese que, actualmente, en Europa, sólo el Mercedes (clases C o S) con sistema Drive Pilot es un coche equipado

con sistemas de nivel 3. Además, el coche solo opera en Alemania, gracias a la actualización de su Ley de Tráfico, que ha creado un marco normativo para el uso de esta tecnología. En España se está tramitando la aprobación de un Real Decreto para vehículos totalmente automatizados cuya aprobación se encuentra en curso[99].

Por lo demás, los sistemas de IA también se integran no ya en vehículos de circulación propiamente dichos, sino en robots de reparto, de forma que estos operan de forma prácticamente autónoma (Starship).

Asimismo, encontramos electrodomésticos que incorporan sistemas de IA. Por ejemplo, a lavadora Samsung AI Ecobubble, que utiliza algoritmos para analizar patrones de lavado y ofrecer recomendaciones personalizadas. También el robot aspirador Roomba, que funciona autónomamente después de una fase previa de entrenamiento. Asimismo, se venden frigoríficos inteligentes, que pueden recomendar recetas según los alimentos depositados o avisar de cuando estos están caducados (Bespoke 4-Door Flex de Samsung).

En el ámbito sanitario, aunque se habla con frecuencia de la transformación que la IA aportará al diagnóstico y tratamiento de enfermedades, lo cierto es que su utilización no se ha implementado aún de manera planificada ni como parte de una estrategia corporativa consolidada. Si bien es presumible que en un futuro cercano la IA se integre de forma estructurada en los sistemas de salud, actualmente su aplicación a gran escala no es una realidad.

Lo que sí es una realidad son las aplicaciones sanitarias que no necesitan prescripción médica. Por ejemplo, gluQUO permite que el usuario registre los alimentos ingeridos, la actividad realizada y los niveles de glucosa. Su característica más destacable es la calculadora de bolos: a partir de la información registrada, la aplicación indica qué cantidad de insulina debe suministrarse el usuario diabético. En este caso, al contrario que sucede con Chat GPT, podría dudarse de si la información de salida es "defectuosa" y de si entra en el ámbito de aplicación de la Directiva (UE) 2024/2853. Imaginemos que gluQUO realiza una recomendación de insulina incorrecta, y un usuario, confiando en ella, se administra la dosis recomendada, sufriendo una hipoglucemia. Aunque es controvertido, podría razonarse que aquí la información proporcionada por la aplicación no es genérica, sino vinculada directamente con cuestiones médicas, lo que podría generar una expectativa razonable en el usuario de que la información será fiable y precisa, aumentando la conexión de la información errónea con el daño.

4. Sistema de IA y defecto de seguridad

[99] Proyecto de Real Decreto por el que se modifican el Reglamento General de Circulación, aprobado por Real Decreto 1428/2003, de 21 de noviembre y el Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, en materia de conducción automatizada

Según el artículo 7.1 Directiva (UE) 2024/2853, un producto "se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional".

De este modo, el defecto en el producto (el sistema de IA) no es un defecto cualquiera, sino que el defecto debe poner en riesgo la salud de las personas, pero también la integridad de los bienes, distintos del propio producto (cfr. artículo 6 Directiva (UE) 2024/2853).

Nótese que en productos como los electrodomésticos o wereables inteligentes, el defecto en el sistema de IA seguramente no ponga en peligro la salud y la seguridad de las personas o los bienes, y por tanto no se trate de un defecto de seguridad, sino de una falta de conformidad. Si el Roomba, por un error de los algoritmos, no sigue las rutas programadas y se choca con los muebles, no pone realmente en riesgo la salud de las personas o la seguridad de los bienes. Es cierto que podría pensarse que la lavadora con IA podría tomar decisiones erróneas, como ordenar un llenado excesivo de agua, causando una inundación en la vivienda. Con todo, si la lavadora provoca una inundación en la casa, o el frigorífico un incendio, probablemente se deba a un defecto en un componente mecánico o eléctrico, no en el sistema de IA.

Así pues, aparte de los vehículos totalmente autónomos o los que poseen sistemas de asistencia a la conducción, parece que la mayoría de los sistemas de IA incorporados a los productos utilizados hoy en día por los consumidores y otras personas físicas no son susceptibles de tener defectos de seguridad.

En nuestra opinión, para que el sistema de IA sea susceptible de tener defectos de seguridad deberá incorporarse en productos tangibles cuya utilización ponga en riesgo la salud de las personas o la integridad de los bienes (vehículos, aviones, máquinas, ascensores, robots, etc.), o estar destinados a utilizarse en personas (productos sanitarios), en cuyo caso serán algo parecido a componentes de un cuerpo físico.

5. Sistema de IA y daños personales o a bienes

Consecuencia de que el defecto del producto debe ser un defecto de seguridad, el artículo 6 Directiva (UE) 2024/2853 cubre los daños personales (muerte y lesiones corporales, entre ellas los daños para la salud psicológica reconocidos medicamente). Aunque también se indemnizan los daños a bienes, distintos del propio producto, siempre que no se utilicen exclusivamente con fines profesionales (una vivienda, por ejemplo). Entre los daños a bienes también se incluye la destrucción o corrupción de datos que no se utilicen con fines profesionales. Asimismo, se cubren los daños morales que deriven de los daños anteriores. Con todo, quedan fuera las pérdidas económicas puras (que no deriven de muerte, lesiones corporales y daños a bienes), los ataques a la intimidad o la discriminación, el daño por infracción de la normativa de protección de datos personales y, en general, cualquier daño que esté cubierto por un régimen específico de responsabilidad (artículo 2.4 c y considerando 24 Directiva (UE) 2024/2853).

Pues bien, después de un examen de incidentdatabase.ai, que es una base de datos que reporta incidentes de todo el mundo relacionados con la IA, puede concluirse que hoy en día los sistemas de IA que están involucrados en daños a las personas o a los bienes están incorporados a bienes tangibles y, en particular, a vehículos de circulación, con o sin conductor, o a robots de reparto.

6. La IA en la apreciación del defecto

Una nueva circunstancia para apreciar que el producto no ofrece la seguridad esperada, pues no estaba prevista en la DRPD 85, es "el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio" [artículo 7.2. c) Directiva (UE) 2024/2853]. En la seguridad del producto habrá de valorarse, "cuando lo requiera la naturaleza del producto, las funcionalidades de evolución, aprendizaje y predicción del producto" [artículo 6.1 h) RGSP].

Esta circunstancia es una clara referencia, por un lado, a los sistemas dotados de IA, pues la capacidad de autoaprendizaje es una característica de algunos de estos sistemas. De otro, es una alusión evidente a los productos digitales, que pueden adquirir nuevas características a través de la instalación de nuevos softwares o la actualización de los ya instalados. Aunque la Directiva (UE) 2024/2853 incluye la capacidad de autoaprendizaje de algunos productos como una circunstancia para valorar su seguridad, no se entiende muy bien cómo se aplicará a la hora de apreciar la existencia del defecto. Acaso cabría pensar que el legislador europeo identifica autoaprendizaje con imprevisibilidad, peligro, falta de seguridad y por ello con defecto. Así, cuando el producto con IA con capacidad de autoaprendizaje ocasiona un daño, revelaría la existencia de un defecto de fabricación[100].

7. Medidas para aligerar la carga de la prueba

Al igual que en el régimen de la DRPD 85, el demandante debe demostrar: el carácter defectuoso del producto, el daño sufrido y el nexo causal entre carácter defectuoso y daño (artículo 10.1 Directiva (UE) 2024/2853).

Pero muchas veces los perjudicados se encuentran con dificultadas significativas para probar el defecto, el nexo causal o ambos, lo que puede ocurrir en caso de tecnologías complejas como la IA. En consecuencia, la Directiva (UE) 2024/2853 establece varias

[100] MARTÍN FABA, J. M., 'Responsabilidad por productos defectuosos con elementos digitales y basados en inteligencia artificial', en M. del P. Cámara Águila (dir.) y A. Agüero Ortiz (dir.), Derecho privado y tecnología, 2025, pp. 491-559, ISBN 978-84-1163-866-1; SOLÉ FELIU, Josep: «De nuevo sobre el defecto del producto. Análisis del artículo 7 de la Directiva (UE) 2024/2853, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos» (52 pp.)

técnicas para a aliviar la carga de la prueba. La primera técnica es la prevista en el artículo 9 Directiva (UE) 2024/2853, sobre exhibición de pruebas. La segunda técnica se basa en la presunción del defecto y/o la relación de causalidad entre este y el daño si se cumplen una serie de circunstancias (artículos 10.2 y 3 Directiva (UE) 2024/2853).

7.1. Exhibición de pruebas

Como hemos dicho, es necesario facilitar el acceso de los demandantes a las pruebas que vayan a utilizarse en los procedimientos judiciales. Tales pruebas incluyen los documentos que el demandado deba crear *ex novo* mediante la compilación o clasificación de las pruebas disponibles.

El artículo 9.1 Directiva (UE) 2024/2853 reza que los EEMM "garantizarán que, a petición de una persona que reclame una indemnización en un procedimiento ante un órgano jurisdiccional nacional por los daños causados por un producto defectuoso, y que haya presentado hechos y pruebas suficientes para respaldar la verosimilitud de la demanda de indemnización, se exigirá al demandado que exhiba las pruebas pertinentes de que disponga, de acuerdo con las condiciones establecidas en el presente artículo". La consecuencia al incumplimiento de esta obligación de exhibición de pruebas es la presunción del defecto (artículo 10.2 Directiva (UE) 2024/2853).

Para que el demandado tenga que exhibir las pruebas se exige a la víctima que haya presentado *hechos y pruebas suficientes para respaldar la verosimilitud de la reclamación*. El precepto parece significar que solo procederá la exhibición de pruebas cuando la demanda indemnizatoria no sea *prima facie* infundada o inverosímil.

Pero es que, además, habida cuenta de que los demandados también podrían necesitar acceder a las pruebas a disposición de la víctima demandante para oponerse a una demanda de indemnización, los demandados deben tener la posibilidad de acceder a las pruebas. En efecto, según el artículo 9.2 Directiva (UE) 2024/2853, los EEMM "garantizarán que, a petición del demandado que haya presentado hechos y pruebas suficientes para demostrar su necesidad de pruebas a efectos de oponerse a una demanda de indemnización, el demandante esté obligado, de conformidad con el Derecho nacional, a exhibir las pruebas pertinentes que estén a su disposición.".

Por su parte, el artículo 9.3 Directiva (UE) 2024/2853 establece que los EEMM "garantizarán que la exhibición de pruebas con arreglo a los apartados 1 y 2, y de conformidad con el Derecho nacional, se limite a lo que sea necesario y proporcionado". Como establece el artículo 9.4 Directiva (UE) 2024/2853, "a la hora de determinar si la exhibición de pruebas solicitada por una parte es necesaria y proporcionada, los órganos jurisdiccionales nacionales tengan en cuenta los intereses legítimos de todas las personas afectadas, incluidos terceros, en particular en relación con la protección de la información confidencial y los secretos comerciales.".

Además, el artículo 9.5 Directiva (UE) 2024/2853 establece que los EEMM "garantizarán que, cuando se exija a un demandado divulgar información que sea un secreto comercial o un presunto secreto comercial, los órganos jurisdiccionales nacionales estén facultados, previa solicitud debidamente motivada de una parte o por propia iniciativa, para adoptar las medidas específicas necesarias para preservar la confidencialidad de esa información cuando se utilice o se mencione en el transcurso del procedimiento judicial o después de este". Así, se pretende lograr un equilibrio justo y proporcionado entre el interés de confidencialidad del poseedor del secreto comercial y el interés de la persona perjudicada en acceder a la información para poder aportar la prueba en su reclamación. Esto debería incluir al menos medidas para restringir el acceso a los documentos que contengan secretos comerciales o presuntos secretos comerciales y el acceso a las audiencias a un número limitado de personas, o permitir el acceso a documentos previamente depurados (considerando 45 Directiva (UE) 2024/2853).

Con todo, la exhibición de pruebas puede ser insuficiente, pues los perjudicados pueden no comprender la información revelada, encontrándose con importantes dificultades para probar un defecto y la relación causal entre un defecto y un daño. Teniendo en cuenta la complejidad de determinados tipos de pruebas, por ejemplo, las pruebas relativas a productos digitales, los órganos jurisdiccionales nacionales deben poder exigir que dichas pruebas se presenten de manera fácilmente accesible y comprensible, siempre que se cumplan determinadas condiciones (considerando 42 Directiva (UE) 2024/2853).

Por ello, el artículo 9.6 Directiva (UE) 2024/2853 establece que los EEMM "garantizarán que, cuando se exija a una parte la exhibición de pruebas, los órganos jurisdiccionales nacionales estén facultados, previa solicitud debidamente motivada de la parte contraria o cuando el órgano jurisdiccional nacional de que se trate lo considere apropiado y de conformidad con el Derecho nacional, para exigir que dichas pruebas se aporten de manera fácilmente accesible y comprensible, si el órgano jurisdiccional nacional considera que dicha aportación es proporcionada en términos de costes y esfuerzo para la parte requerida". Así, para que la parte tenga la obligación de presentar las pruebas de manera clara y comprensible, la contraparte debe solicitarlo o el juez debe considerarlo apropiado, siempre que esa explicación accesible no resulte desproporcionada económica o intelectualmente para la parte que la tenga que realizar.

Finalmente, la Directiva (UE) 2024/2853 armoniza las normas sobre exhibición de pruebas únicamente en la medida en que tales cuestiones estén reguladas por ella. Entre las cuestiones no reguladas por la Directiva (UE) 2024/2853 se encuentran las normas sobre la exhibición de pruebas en relación con: los procedimientos preliminares; el grado de especificidad que debe tener la solicitud de pruebas; los terceros; los casos de acciones declarativas y sanciones por incumplimiento de la obligación de exhibir pruebas (considerando 43 Directiva (UE) 2024/2853). En consecuencia, el artículo 9.7 Directiva (UE) 2024/2853 establece que la regulación sobre la exhibición de pruebas no afecta a "no afecta a las normas nacionales relativas a la exhibición preliminar de pruebas, en caso de que tales normas existan".

7.2. Presunción del defecto

La Directiva (UE) 2024/2853 ha considerado que, bajo determinadas condiciones, no es necesario probar el defecto en el producto, pues este se presume. En algunos casos, para que se aplique la presunción, la víctima tendrá que probar algunos hechos, lo que puede significar un guiño a los operadores económicos. Sería algo similar al recurso a las presunciones judiciales a las que se refiere el artículo 386 LEC, mecanismo conforme al cual, a partir de un hecho admitido o probado, el tribunal podrá presumir la certeza de otro hecho, si entre el admitido o demostrado y el presunto existe un enlace preciso y directo según las reglas del criterio humano.

En primer lugar, para incentivar el cumplimiento de la obligación de revelar información, los órganos jurisdiccionales nacionales deben presumir el carácter defectuoso de un producto cuando el demandado no haya exhibido las pruebas pertinentes de conformidad con el artículo 9.1 Directiva (UE) 2024/2853 [artículo 10.2. a) Directiva (UE) 2024/2853]. En este caso cabe pensar, aunque el precepto no lo diga así expresamente, que si el demandado no revela las pruebas no está probando la inexistencia del defecto[101].

En segundo lugar, se presumirá el defecto cuando "el demandante demuestre que el producto no cumple los requisitos obligatorios de seguridad del producto establecidos en el Derecho de la Unión o en la legislación nacional que tienen por objeto proteger contra el riesgo del daño sufrido por la persona perjudicada" [artículo 10.2. b) Directiva (UE) 2024/2853]. Presumir en esos supuestos la existencia de un defecto en el producto puede considerarse como una medida para incentivar el cumplimiento de las obligaciones de seguridad. Ahora bien, puede ser difícil para la víctima demostrar que el producto no cumple con los requisitos obligatorios de seguridad dispuestos en la legislación. De hecho, puede conllevar la misma dificultad probatoria acreditar el defecto en el producto que el incumplimiento de los requisitos obligatorios de seguridad previstos en las leyes.

Además, para presumir el defecto, el perjudicado debe probar que la norma de seguridad incumplida tiene por objeto proteger contra el riesgo del daño sufrido. En efecto, si la norma de seguridad incumplida no tiene como fin evitar los daños que son objeto de reclamación, no se puede presumir el defecto, pues no operaría el criterio de imputación objetiva del "fin de protección de la norma violada", que se utiliza para imputar los daños en el ámbito de la causalidad jurídica[102].

En tercer y último lugar, debe presumirse el defecto cuando "el demandado demuestre que el daño fue causado por *un mal funcionamiento evidente* del producto durante el *uso razonablemente previsible* o en circunstancias normales" [artículo 10.3 c) Directiva (UE)

[101] GÓMEZ LIGÜERRE, C., "La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos", *InDret*, núm. 4, 2022, p. 5.
[102] ATIENZA NAVARRO, M.ª L., "¿Una nueva responsabilidad por productos defectuosos?", *InDret*, núm. 2, 2023, p. 30.

2024/2853]. Por tanto, tiene que darse un fallo notorio del producto durante un uso normal. El uso normal o razonablemente previsible abarca el uso al que está destinado un producto de conformidad con la información facilitada por el fabricante o el operador económico que lo introduzca en el mercado, el uso ordinario determinado por el diseño y la construcción del producto, y el uso que pueda preverse razonablemente cuando dicho uso pueda derivarse de un comportamiento humano lícito y fácilmente previsible (considerando 46 Directiva (UE) 2024/2853). Por ello, cuando el mal funcionamiento se deba a un uso indebido imprevisible de la víctima, la presunción no se aplica. Un ejemplo de *mal funcionamiento evidente* del producto durante el *uso razonablemente previsible* sería una botella de vidrio que explota cuando el perjudicado estaba bebiendo. En este caso es innecesariamente gravoso exigir al demandante que demuestre la existencia de un defecto cuando las circunstancias son tales que su existencia es *indiscutible.*

El precepto positiviza la regla según la cual, si la inferencia del defecto puede ser apropiadamente puesta en conexión con el daño, el demandante no ha de probar el defecto. Es decir, el principio *res ipsa loquitur*: No se requiere la prueba del defecto cuando según las máximas de la experiencia el daño no se hubiera producido en ausencia de defecto. Por ejemplo, si un avión se estrella, no se debe probar si el defecto estaba en las turbinas o en el depósito de combustible[103].

7.3. Presunción del nexo causal

Por otra parte, "se presumirá el nexo causal entre el carácter defectuoso del producto y el daño cuando se haya *comprobado que el producto es defectuoso* y el *daño causado sea de un tipo compatible normalmente con el defecto en cuestión*" (artículo 10.3 Directiva (UE) 2024/2853).

Así, en primer lugar, el juez deberá comprobar que el producto es defectuoso, lo que se ha podido realizar mediante el juego de presunciones anteriores. En segundo lugar, que el daño es *compatible normalmente con el defecto* en cuestión. Aunque el concepto compatible normalmente es bastante indeterminado, parece querer significar lo siguiente. No se presumirá el nexo causal entre un airbag defectuoso que no se activó y la lesión en una muñeca sufrida por el conductor, pues el airbag está destinado a evitar o minorar las contusiones craneales y torácicas y la lesión que en este caso se produjo fue resultado directo del accidente de tráfico, sin que tal daño tuviera origen en el defecto de airbag, pues, aunque este hubiese funcionado, tal lesión en la muñeca se habría producido igualmente[104]. En ese caso *el daño producido no sería compatible normalmente con el defecto en cuestión*, y por ello no podría presumirse el nexo causal entre defecto y daño. Con todo, si en el ejemplo propuesto los daños hubieran sido lesiones craneales o torácicas, esos daños serían compatibles con el defecto del airbag y se podría presumir el nexo causal.

---

[103] AMERICAN LAW INSTITUTE, *Restatement of the Law Third. Torts. Product Liability,* 1998, p. 114 a 116.
[104] SAP Sevilla de 27 de diciembre de 2002 (JUR 2003, 170863).

7.4. Presunción del defecto y del nexo causal por dificultades excesivas en casos complejos

Según el artículo 9.4. Directiva (UE) 2024/2853 "el órgano jurisdiccional nacional presumirá el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambas cosas, cuando, a pesar de la exhibición de pruebas de conformidad con el artículo 9 y teniendo en cuenta todas las circunstancias pertinentes del caso: a) el demandante se enfrente a dificultades excesivas, en particular debido a la complejidad técnica o científica para demostrar el carácter defectuoso del producto o el nexo causal entre su carácter defectuoso y el daño, o ambas cosas; y b) el demandante demuestre que es probable que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso y el daño, o ambos".

La precisión parece estar pensada para tecnologías digitales emergentes como la IA, dotadas de una gran complejidad técnica que, unida a su opacidad, dificultan enormemente la prueba. Cuando se trata de este tipo de productos, a pesar de que el demandado cumpla su deber de exhibición de pruebas y de información, el demandante, carente de conocimientos tecnológicos, continuará teniendo dificultades para probar el defecto o su relación de causalidad con el daño. Por ese motivo, como explica el considerando 48 Directiva (UE) 2024/2853, en casos de complejidad técnica o científica, exigir dichas pruebas socavaría indudablemente la efectividad del derecho a la indemnización, con lo que parece lógico que sean los operadores económicos, que son quienes disponen de esos conocimientos especializados, los que refuten, en su caso, dicha presunción. Seguramente la jurisprudencia del TJUE que se ha pronunciado sobre casos en los que los usuarios tienen dificultades excesivas para probar el defecto o el nexo causal, debido a la complejidad del producto, también ha influido en la introducción de la presunción contenida en el artículo 9.4 Directiva (UE) 2024/2853.

Para que se aplique la presunción, debe cumplirse un doble requisito: (i) que el perjudicado se encuentre en dificultades excesivas, debido a la complejidad técnica, para probar el defecto en el producto o el nexo causal; y (ii) que el perjudicado pruebe que es probable que el producto es defectuoso o el nexo causal.

Por tanto, el primer lugar, el perjudicado se tiene que encontrar, a pesar de la exhibición de las pruebas, con "dificultades excesivas", debido a una "complejidad técnica o científica". La evaluación de las dificultades excesivas debe ser realizada por los órganos jurisdiccionales nacionales, caso por caso. Con todo, no está claro si el requisito de dificultades excesivas debe analizarse desde una perspectiva subjetiva u objetivamente. Si bien el demandante debe aportar argumentos para demostrar la existencia de dificultades excesivas, no debe exigirse la prueba de tales dificultades. Por ejemplo, en una demanda relativa a un sistema de IA, para que el órgano jurisdiccional decida que existen dificultades excesivas, no debe exigirse al demandante que explique las características específicas del sistema de IA ni cómo estas características dificultan la determinación del defecto o el nexo causal (considerando 48 Directiva (UE) 2024/2853).

No obstante, como el legislador europeo tiene siempre presente la necesidad de no frenar la inversión en el desarrollo tecnológico, matiza que el demandado podrá acreditar que no existen realmente dificultades excesivas para probar el defecto o la relación de causalidad entre este y el daño (artículo 10.5 Directiva (UE) 2024/2853).

La "complejidad técnica o científica" también debe ser determinada por los órganos jurisdiccionales nacionales caso por caso, teniendo en cuenta diversos factores. Estos factores deben incluir la naturaleza compleja del producto, como un producto sanitario innovador; la naturaleza compleja de la tecnología utilizada, como el aprendizaje automático; la naturaleza compleja de la información y los datos que debe analizar el demandante; y la naturaleza compleja del nexo causal, como la relación entre un producto farmacéutico o alimenticio y la aparición de una enfermedad, o una relación que, para ser probada, requeriría que el demandante explicara el funcionamiento interno de un sistema de IA (considerando 48 Directiva (UE) 2024/2853).

Para que la complejidad técnica o científica del producto no se convierta, sin más, en un motivo para invertir la carga de la prueba, se exige al perjudicado, en segundo lugar, que "demuestre que es probable que el producto sea defectuoso o que exista un nexo causal entre el carácter defectuoso y el daño, o ambos". Es decir, debe acreditar que es probable que el producto defectuoso contribuyó a los daños o que es probable que el producto es defectuoso. Nótese que el criterio de la probabilidad razonable puede coincidir con lo que ya constituye un criterio de imputación objetiva empleado en España en el ámbito de la causalidad civil, esto es, la causalidad adecuada o adecuación, consistente en la apreciación de que el resultado dañoso es una consecuencia natural, adecuada y suficiente de la acción u omisión que la precede[105].

No obstante, si es el perjudicado quien tiene que acreditar la probabilidad del carácter defectuoso o del nexo causal entre el defecto y el daño, seguiría ostentando la carga de acreditar estos hechos mediante el criterio de la imputación objetiva de la adecuación. Finalmente, el criterio de la probabilidad encierra algunas dificultades de interpretación. Por ejemplo, como solo se exige que la víctima demuestre que existe una "probabilidad" de la existencia del defecto o nexo causal, parece que la prueba de una probabilidad del 51% sería suficiente, sin que sea necesario la acreditación de una probabilidad reforzada, superior al 51%[106].

8. Conclusión

Cuando un consumidor sufre alguno de los daños cubiertos por la Directiva (UE) 2024/2853 como consecuencia de un sistema de IA, se activa el régimen de

[105] MARTÍ GRAU, R., "Reflexiones acerca de la Propuesta de Directiva sobre responsabilidad por daños derivados de la inteligencia artificial y su impacto en el Derecho español de daños", *Revista Aranzadi Doctrinal*, núm. 4, 2023, p. 6.
[106] EUROPEAN LAW INSTITUE, F*eedback on European Commission's Proposal for a Revised Product Liability Directive*, 2022, p. 22.

responsabilidad objetiva del fabricante: el perjudicado tiene derecho a ser indemnizado por el fabricante sin necesidad de probar culpa, debiendo acreditar únicamente el daño, el defecto de seguridad y el nexo causal. La Directiva solo cubre daños personales —incluida la salud psicológica reconocida médicamente—, daños materiales en bienes de uso o consumo privado distintos del propio producto y la destrucción o corrupción de datos no profesionales; quedan excluidas las pérdidas económicas puras, los daños contractuales, los perjuicios derivados de infracciones del RGPD, los ataques a la intimidad o la discriminación y, en general, cualquier daño ajeno a estas categorías.

Para hacer efectivo el derecho a la indemnización, el consumidor dispone de mecanismos probatorios reforzados que resultan especialmente relevantes ante la complejidad técnica de los sistemas de IA. Puede solicitar la exhibición de las pruebas pertinentes que estén en poder del fabricante u operador y, cuando proceda, exigir que se aporten de forma accesible y comprensible, siempre que dicha carga no sea desproporcionada.

Además, la Directiva (UE) 2024/2853 establece varias presunciones legales: se presume el defecto si el demandado incumple su deber de exhibición de pruebas, si se prueba el incumplimiento de requisitos obligatorios de seguridad destinados a evitar el daño sufrido, o cuando existe un mal funcionamiento evidente en un uso normal o razonablemente previsible. También se presume el defecto y/o la causalidad cuando, pese a la exhibición de pruebas, el perjudicado afronta dificultades excesivas derivadas de la complejidad técnica o científica del producto y aporta indicios que hacen probable el defecto o el vínculo causal. En conjunto, estos instrumentos garantizan que la opacidad técnica de los sistemas de IA no impida al consumidor obtener reparación cuando un producto digitalizado presenta un defecto de seguridad y causa uno de los daños estrictamente comprendidos en el ámbito de la Directiva (UE) 2024/2853.

VIII. CUADRO SINTÉTICO: PRÁCTICAS DE IA EN CONSUMO, RIESGOS Y NORMATIVA APLICABLE

Práctica basada en IA	Riesgos para consumidores	Normativa aplicable
Personalización de contenidos, anuncios y ofertas	Opacidad; manipulación; explotación de vulnerabilidades; discriminación; impacto en menores	RGPD: artículos 4.4, 13.2.f, 14.2.g, 15.1.h, 22. TRLGDCU: artículo 20.3, artículo 97 bis. LCD / Directiva 2005/29/CE: artículo 26.2. DSA:

Práctica basada en IA	Riesgos para consumidores	Normativa aplicable
		artículos 26, 27, 28, 38. DMA: artículo 5.2. LGCA: artículo 90 y ss.
Dark patterns	Distorsión de la autonomía; interferencia en la decisión; explotación de vulnerabilidades	LCD / Directiva 2005/29/CE: artículos 5–9, artículo 5.3. DSA: artículo 25. Directiva (UE) 2023/2673: introduce artículo 16 quinquies en la Directiva 2011/83/UE.
Personalización de precios	Discriminación; falta de transparencia; trato desigual; uso de datos no pertinentes	Directiva 2006/123/CE: artículo 20. Reglamento (UE) 2018/302: artículo 4. TRLGDCU: artículos 20.1.c, 97.1.f. (Directiva (UE) 2019/2161); RDL 8/2024: DF 1.ª (modificación artículo 20.1.c TRLGDCU); PLAC
Evaluación automatizada de solvencia	Denegaciones opacas; discriminación indirecta; uso de proxies; falta de revisión humana	RGPD: artículos 13.2.f, 14.2.g, 15.1.h, 22, 82. AI Act: artículo 14, artículo 86, Anexo III. Directiva (UE) 2023/2225: artículo 6, artículos 18.3, 18.8, 18.9. Ley 15/2022: artículos 2, 6, 17, 25, 27. Carta DFUE: artículo 21.
Risk scoring asegurador	Discriminación; exclusión; opacidad en tarificación; uso de datos sensibles	LOSSEAR: artículos 93, 94, 95. RGPD: artículos 9.1, 9.2, 13, 14, 15, 22, 25. Directiva 2004/113/CE: artículos 4–5. AI Act: artículo 14, artículo 86.
Chatbots (atención automatizada)	Información errónea; bloqueo del acceso a un humano; efectos jurídicos sin revisión; falta de transparencia	RIA: artículo 50, artículo 14, artículo 86, artículo 5 y Anexo III. DSA: artículo 12, artículo 20.6. Directiva (UE) 2023/2673: artículo 16 quinquies (Dir. 2011/83/UE). RGPD: artículo 22.
Asistentes virtuales y roboadvisors	Compras involuntarias; conflictos de interés; errores de recomendación	MiFID II: artículo 4.1.4. TRLMV: artículos 140, 143, 150. RD 217/2008: (sin artículos citados).
Scalper bots	Acaparamiento; precios abusivos; escasez artificial	LCD / Directiva 2005/29/CE: artículo 27.1 (tras la reforma por Directiva 2019/2161).
Reseñas falsas	Distorsión del mercado; engaño; pérdida de confianza	Directiva 2005/29/CE: artículo 7.6 y lista negra modificada por Dir. 2019/2161. LCD: artículo 26.

Práctica basada en IA	Riesgos para consumidores	Normativa aplicable
Bienes y servicios digitales con IA integrada	Pérdida de funcionalidades; fallos tras actualizaciones; falta de interoperabilidad	Directiva (UE) 2019/770: artículos 7–10. Directiva (UE) 2019/771: artículos 6–8. TRLGDCU / RDL 7/2021: artículos 114–120.
Responsabilidad por IA defectuosa	Daños personales o materiales; dificultad probatoria; nexo causal complejo	DRPD 2024: artículos 4, 6, 7, 9, 10. AI Act: artículo 4.1.

CAPÍTULO IV. DERECHOS DE LOS CONSUMIDORES Y HERRAMIENTAS DE PROTECCIÓN

I. INTRODUCCIÓN

La IA se encuentra presente en todos los sectores, incluida la administración pública, habiendo hecho posible la automatización de procesos, pero también poniendo en riesgo algunos de los más valiosos derechos fundamentales.

En los últimos años numerosas tareas habituales que antes realizábamos de manera tradicional, como la compra de un electrodoméstico, se han automatizado, incluyendo ahora múltiples factores en este proceso. En el caso de las compras por internet, de los diversos datos que quedan almacenados en los usuarios en la nube en muchas ocasiones se crea un perfilado automático, que puede influir, por ejemplo, en el precio de ese producto que va a adquirirse a posteriori. Pese a que este tipo de sistemas permiten un gran ahorro de tiempo, la automatización de tareas que, aunque a simple vista son sencillas y repetitivas, cuando se deshumanizan, pueden derivarse una serie de riesgos que no son previsibles en una primera instancia. La presencia de sesgos en los sistemas de IA, unido a su falta de transparencia, lo que lleva a que también se denominen "black box" (caja negra), no la convierten en la sustituta adecuada de la actividad humana, sino que las actuaciones realizadas a través de este tipo de sistemas deben ser supervisadas, al menos por el momento, por una persona física que pueda advertir determinados fallos.

A lo largo del presente capítulo expondremos cuáles son los derechos de los consumidores que deben ser tenidos en cuenta cuando se incluyen sistemas de IA en diferentes procedimientos, de entre los que destacan el derecho a la transparencia algorítmica y a la explicabilidad, de forma que los ciudadanos sepan por qué se han tomado determinadas decisiones, en base a qué información, cuál es la fuente de la que proceden sus datos, cómo y cuándo se ha otorgado el consentimiento, etc. De igual forma, analizaremos diferentes resoluciones judiciales en las que se estudia el posible menoscabo de derechos de los consumidores en diferentes situaciones. Para finalizar, explicaremos cuál es el procedimiento de reclamación para OMIC´S ante una indeseable situación vivida por el consumidor. También encontraremos una guía explicativa dirigida a los consumidores que indique qué se debe reclamar y cómo.

II. LOS DERECHOS DEL CONSUMIDOR ANTE LA IRRUPCIÓN DE LA INTELIGENCIA ARTIFICIAL

A nivel global, ya en la Recomendación sobre la ética de la IA, adoptada el 23 de noviembre de 2021 por la UNESCO (instrumento no vinculante) se indicaba que las personas pueden interactuar con los sistemas de IA, siempre y cuando su dignidad, sus derechos humanos o sus libertades fundamentales sean menoscabados de ninguna manera. En este sentido, se destacaba que tanto los gobiernos, como el sector privado debían respetar los instrumentos y marcos de derechos humanos en sus intervenciones en los procesos que rodean el ciclo de vida de los sistemas de IA.

Dentro de los derechos y principios que se establecen en este instrumento, destacan los siguientes. En primer lugar, el principio de necesidad, de forma que la decisión de utilizar sistemas de IA y la elección del método de IA deben justificarse atendiendo a lo que sea más adecuado para lograr un objetivo específico determinado, y siempre y cuando no se vulneren los derechos fundamentales. En segundo lugar, el derecho a la igualdad y no discriminación, de forma que pueda garantizarse que los beneficios de las tecnologías de la IA estén disponibles y sean accesibles para todos, teniendo en cuenta las necesidades específicas de los diferentes grupos de edad, los sistemas culturales, las personas con discapacidad, etc. En tercer lugar, el derecho a la intimidad y protección de datos, de forma que la capacidad de actuar de los seres humanos debe ser respetada, protegida y promovida a lo largo del ciclo de vida de los sistemas de IA. Además, es importante que los datos que alimentan a este tipo de sistemas de recopilen de la manera más acorde al derecho internacional, así como que se realicen las oportunas evaluaciones adecuadas del impacto en la privacidad. En cuarto lugar, la transparencia y explicabilidad, que son fundamentales para que los regímenes en materia de responsabilidad funcionen eficazmente. Esto es porque la falta de transparencia puede mermar la posibilidad de impugnar eficazmente las decisiones basadas en resultados producidos por sistemas de IA.

De otro lado, a nivel europeo hay varios instrumentos jurídicos reseñables que también indicen en la importancia de estos derechos. En este sentido, destaca el Informe sobre la IA en la era digital del Parlamento Europeo, de 5 de abril de 2022, haciendo hincapié en la importancia por el pleno respecto de los derechos fundamentales, siendo necesaria una estricta vigilancia democrática, normas claras de transparencia, una infraestructura informática, empleados altamente cualificados y acceso a grandes cantidades de datos de alta calidad.

En nuestro país, destaca la Carta de Derechos Digitales (marco orientador), publicada en julio de 2021, que no trata de crear nuevos derechos sino de perfilar los más importantes teniendo en cuenta el entorno digital. Entre los derechos reflejados, destacan los siguientes: derecho a la protección de datos, el derecho a no ser localizado y perfilado, el derecho a la seguridad digital, derecho a la igualdad y no discriminación en el entorno digital, la protección de menores, mayores y personas con discapacidad, derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas, etc.

1. Derechos reconocidos en el Reglamento de Inteligencia Artificial

En primer lugar, destaca el artículo 50[107], en el que se establecen las obligaciones de transparencia que deben ser seguidas por los proveedores y responsables del despliegue de determinados sistemas de IA, de forma que es carga de los proveedores garantizar que los sistemas de IA destinados a interactuar directamente con personas físicas se diseñen y desarrollen de tal mañanera que esas personas físicas estén informadas de que están

[107] El artículo 50 del AI Act recoge las obligaciones de transparencia en la interacción y marcado de contenidos, mientras que el artículo 86 hace referencia a las explicaciones *ex post* en decisiones apoyadas en sistemas de alto riesgo.

interactuando con un sistema de IA, a no ser que resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz, teniendo en cuenta el contexto. También regula la transparencia en la interacción con chatbots y sistemas generativos. Respecto a los proveedores de sistema de IA de uso general que generan contenido sintético de audio, imagen, vídeo o texto, se debe velar porque los resultados de salida del sistema estén marcados en un formato legible por máquina, siendo posible detectar que han sido generados o manipulados por IA. En cuanto a los responsables del despliegue de un sistema de reconocimiento de emisiones o de un sistema de categorización biométrica, deberán informar del funcionamiento del sistema a las personas físicas expuestas a él y deben tratar sus datos personas conforme a lo establecidos en los Reglamentos (UE) 2016/679 y (UE) 2018/1725, y con la Directiva (UE) 2016/680. Por último, los responsables del despliegue de un sistema de IA que genera o manipula imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación, harán público que estos contenidos o imágenes han sido generados o manipulados mediante IA.

En tercer lugar, es preciso traer a colación el artículo 27, referente a la evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo recogidos en el anexo III. Se establece que antes de desplegar uno de los sistemas de IA de alto riesgo, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, deben llevar a cabo una evaluación del impacto respecto a la utilización de dichos sistemas puede tener en los derechos fundamentales[108]. Dicha evaluación consistirá en: descripción de los procesos del responsable del despliegue en los que se utilizó el sistema de IA en consonancia con su finalidad prevista, descripción del período de tiempo durante el que se prevé utilizar cada sistema de IA, las categorías de personas físicas y colectivos que pueden verse afectados, etc.

En tercer lugar, destaca el artículo 86, en el que se recoge el derecho a una explicación de las decisiones tomadas individualmente con efectos jurídicos o similares. En este sentido, toda persona que se vea afectada por una decisión que el responsable del despliegue[109] adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo generando un efecto perjudicial para su salud, seguridad u otros derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada[110].

[108] Se conoce como FRIA (Fundamental Rights Impact Assessment).

[109] Es preciso aclarar que cuando nos referimos al "responsable del despliegue" (*deployerr*) se hace referencia a (según se establece en el AI Act): "una persona física o jurídica, o autoridad, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional."

[110] De cualquier manera, las obligaciones establecidas en el AI Act se aplican sin perjuicio de lo recogido en el RGPD, que se analiza a continuación.

A través de este Reglamento, se crea también la AESIA (Agencia Española de Supervisión de Inteligencia Artificial), que es la entidad española encargada de supervisar el cumplimiento del AI Act. Dentro de sus funciones se encuentran la emisión de recomendaciones, la coordinación con autoridades, la atención de reclamaciones, la promoción de buenas prácticas, así como la imposición de sanciones a partir del pasado agosto de 2025[111].

Al hilo de este Reglamento, surge el Convenio de IA del Consejo de Europa[112]. El mismo se ha convertido en un instrumento jurídico vinculante de carácter transversal que promueve la innovación y establece principios sólidos y claros para el desarrollo de sistemas de IA en relación con los derechos humanos, la democracia y el Estado de Derecho. Este instrumento resulta especialmente útil puesto que otorga a los sujetos afectados por la IA determinados derechos y garantías y establece mecanismos para la defensa de estos derechos ante autoridades que deben ser independientes. De especial relevancia es su artículo 16, en el que se exige una evaluación y mitigación continua de los riesgos e impactos adversos de cualquier tipo de sistema de IA[113].

2. Derechos reconocidos en el Reglamento de Protección de Datos

De otro lado, hemos de traer a colación el RGPD. En su artículo 13.2, destaca el derecho de información y acceso a datos personales, indicando que el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la información necesaria en aras a garantizar un tratamiento de datos leal y transparente.

De otro lado, en el artículo 14, apartado segundo, hace referencia a la información que deberá facilitar cuando los datos personales no se hayan obtenido del interesado, indicando que será necesario indicar la existencia de decisiones automatizadas, incluida la elaboración de perfiles, así como la información significativa sobre la lógica aplicada, y las consecuencias previstas de dicho tratamiento para el interesado.

Especial relevancia también adquiere el artículo 15, en el que se define el derecho de acceso del interesado, a través del cual el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En el caso de que el consumidor sea objeto de una decisión automatizada mediante el tratamiento de datos, se aplicará el citado artículo y el consumidor tendrá derecho a una explicación significativa sobre la lógica aplicada.

---

[111] Estas funciones provienen del Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial, BOE núm. 210, de 2 de septiembre de 2023; y del Anteproyecto de Ley para el buen uso y la gobernanza de la Inteligencia Artificial, aprobado el 11 de marzo de 2025.

[112] Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho, de 5 de septiembre de 2024, núm. 225. Es el primer tratado internacional vinculante sobre IA.

[113] En este sentido, véase COTINO HUESO, L., "Cómo abordar jurídicamente el impacto de la inteligencia artificial en los derechos fundamentales", en CASAS BAAMONDE, E. (dir.) PÉRES DEL PRADO, D. (coord.), Derecho y tecnologías, ed. Centro de Estudios Ramón Areces, 2025, págs.137 y 138., en el que se explica detalladamente lo más relevante de instrumento jurídico.

De otro lado, destaca su artículo 22, en el que se reconoce el derecho a no ser objeto de decisiones individuales automatizadas, que tanta repercusión puede tener hoy un día. La principal finalidad de este derecho es garantizar que el ciudadano no sea objeto únicamente en el tratamiento de sus dados (incluyendo la elaboración de perfiles), de forma que después puede producir efectos jurídicos sobre el mismo o le afecte de forma similar. Concretamente, es el responsable del tratamiento el que debe garantizar el derecho a obtener la intervención humana. También debemos incluir que cuando se utilizan algoritmos y datos para usar grandes volúmenes de información de las personas, perfilar, discriminar y tomar decisiones en nombre de una entidad gubernamental, se considera un sistema automatizado de decisiones de la administración pública (SDA)[114]. Ahora bien, este artículo sólo se aplica a decisiones exclusivamente automatizadas con efectos jurídicos o similares, de forma que hay en algunos casos que siempre se aplicará como en la denegación de crédito, la fijación del precio del seguro, o una rescisión automática de un contrato, pero no encuentra encaje en cualquier recomendación automatizada.

Por último, hemos de mencionar el artículo 35 del RGPD, en el que recoge la evaluación de impacto relativa a la protección de datos[115]. En el mismo se indica que, cuando sea probable que un tipo de tratamiento (sobre todo cuando se utilizan nuevas tecnologías) por su determinada naturaleza, alcance o contexto, entrañe un alto riesgo para los derechos y libertades de las personas físicas, será obligación del responsable del tratamiento realizar, antes del tratamiento, una evaluación de impacto de las operaciones de tratamiento en la esfera de datos personales. En el apartado tercero se establecen unos casos donde se requerirá dicha evaluación, como son los casos de evaluación sistemática y exhaustiva de aspectos personas de personas físicas que se base en un tratamiento automatizado, el tratamiento a gran escala de categorías especiales de datos (como los que revelan el origen ético o racial); así como la observación sistemática a gran escala de una zona de acceso público.

Recordemos que el derecho a la protección de datos personales se encuentra recogido en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea[116]. Tal y como advierte la doctrina, los sistemas de IA se entrenan mediante el acceso y análisis de grandes conjuntos de datos, lo que en muchas ocasiones puede revelar información privada de las personas y debe tratarse como sensible[117]. Se han desarrollado sistemas de IA que permiten calcular con precisión la edad, el sexo, la ocupación y el estado civil de una persona solo a partir de los datos de localización de su teléfono móvil, por ejemplo.

---

[114] FINOL ROMERO, L., ESIS VILLARROEL, I., "Transparencia de la inteligencia artificial en la administración pública: una revisión de estándares internacionales", *Brazilian Journal of International Law 21,* núm. 1, septiembre 2024, pág. 176.

[115] También denominada DPIA (Documento de Impacto de Privacidad de la IA).

[116] Carta de los Derechos Fundamentales de la Unión Europea, DOUE núm. 303, de 14 de diciembre de 2007.

[117] "Derechos Humanos en la Era de la Inteligencia Artificial", *Ensayos sobre democracia real y capitalismo,* septiembre 2021, pág. 18.

Es por esta razón por la que el consentimiento respecto a la cesión de estos datos se convierte en esencial, al igual que lo es la posibilidad de oponerse a ser objeto de una decisión automatizada mediante el formulario adecuado (véanse Anexos).

3. Derechos recogidos en la Ley de Competencia Desleal

En la Ley de Competencia Desleal[118] destaca fundamentalmente su artículo 22.6, referente a las prácticas señuelo y las prácticas promocionales engañosas. En este sentido, se debe destacar el término "dark patterns"[119] (patrones oscuros), que se producirán cuando hagan creer erróneamente que se podrán obtener ventajas, todo ello condicionado por sistemas de IA que hacen estas recomendaciones mucho más atractivas. De esta forma, se considera como una práctica desleal crear la falsa impresión, incluso a través de prácticas agresivas, de que el consumidor o usuario ya ha ganado, o incluso conseguirá un premio u otro tipo de ventaja si realiza un acto determinado.

Se considerará competencia desleal en el supuesto de que realmente no exista ese premio o ventaja, o bien, que la realización de algún acto relacionado con esa obtención de la recompensa esté sujeto a la obligación, por parte de este consumidor, de efectuar un determinado pago, realizar la compra de otro bien, o incurrir en cualquier gasto. En este sentido, destaca la sanción interpuesta por la FTC (*Federal Trade Commission*) ascendiente a 193.000 dólares a DoNotPay[120] y a la figura del "abogado robot" que era la imagen de su empresa, por publicidad engañosa. En la sanción, que se dictó tras una investigación del organismo de protección al consumidor, se concluyó que la empresa había incurrido en publicidad engañosa, al presentar su chatbot de IA como sustituto real de un abogado humano, sin contar con prueba alguna que avalase esa afirmación[121].

4. Derechos recogidos en la TRLGDCU

En el TRLGDCU[122] también se encuentran diversos artículos que recogen múltiples derechos que afectan a los consumidores aplicables en el entorno digital. En primer lugar,

---

[118] Ley 3/1991, de 10 de enero, de Competencia Desleal, BOE núm. 10, de 11 de enero de 1991.

[119] Debe advertirse cierta correlación entre este concepto y el de "lista negra", acuñado por la doctrina, refiriéndose al Anexo I de 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, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo (Directiva sobre las prácticas comerciales desleales), en el que aparecen recogidas las prácticas comerciales que de consideran desleales en cualquier circunstancia.

[120] Docket c-4812, marzo 2023. Es una aplicación de inteligencia artificial que se presenta como un "robot abogado", para ayudar a los usuarios a resolver problemas legales de forma automatizada y gratuita, como puede ser apelar multas de tráfico, reducir facturas, etc. La empresa fue fundada por Joshua Browder, con el propósito concreto de ayudar a los usuarios a disputar multas de aparcamiento de Reino Unido.

[121] La resolución se ha convertido en un procedente en la regulación del uso de la IA en el ámbito jurídico, pues dibuja claramente cuáles son los límites concretos que deben respetar las empresas tecnológicas cuando ofrecen servicios que impactan en los derechos de los ciudadanos. Fuente: Confilegal. Consultado en: https://confilegal.com/20250504-la-ftc-sanciona-con-193-000-dolares-a-donotpay-y-su-abogado-robot-por-publicidad-enganosa/. Última fecha de consulta: 25 de noviembre de 2025.

[122] 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 y otras leyes complementarias. BOE núm. 287, de 30 de noviembre de 2007.

el artículo 20.1., en concreto el apartado c), que establece que las prácticas comerciales que incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, y siempre que no pueda desprenderse claramente del contexto, deberán contener la siguiente información: el precio final complejo, incluyendo los impuestos e incorporando el importe de los incrementos o descuentos aplicables a la oferta y los gastos adicionales que se repercutan al consumidor o usuario.

También destaca su apartado tercero, en el que se indica que las prácticas comerciales consistentes en ofrecer a los consumidores y usuarios la posibilidad de buscar bienes y servicios ofertados por diferentes empresarias, o consumidores y usuarios sobre la base de una consulta en forma de palabra clave, deberán contener una sección específica de la interfaz en línea que sea fácil y directamente accesible desde la página en la que se presenten los resultados de búsqueda. También señala que la información del interfaz debe contener las siguientes cuestiones: (i) información general relativa a los principales parámetros que determinan la clasificación de los bienes y servicios prestados al consumidor y usuario como resultado de su búsqueda, y (ii) la importancia relativa de dichos parámetros frente a otros.

De otro lado, en cuanto a la información precontractual de los contratos a distancia y los contratos celebrados fuera del establecimiento mercantil, antes de que el consumidor y usuario quede vinculado por cualquier contrato a distancia o celebrado fuera del establecimiento, el empresario le facilitará toda la información de forma clara y comprensible, con especial atención en caso de que se trate de personas consumidoras vulnerables, a la que se le debe facilitar la información en formatos adecuados, accesibles y comprensibles. También se incide en el apartado f) de este precepto, que se deberá informar, en caso de que proceda, de que el precio se ha personalizado sobre la base de una toma de decisiones automatizada, que es una cuestión que también se encuentra recogida en el artículo 97 TRLGDCU.

Por último, destaca el artículo 97 bis, en el que se recogen los requisitos de información específicos adicionales para contratos celebrados en mercados en línea. Tal y como establece la normativa, antes de que un consumidor o usuario quede obligado por un contrato a distancia, o cualquier oferta que corresponda en un mercado el línea, el proveedor deberá facilitarle de forma clara y comprensible, teniendo en cuenta las técnicas de comunicación a distancia, y con especial atención a las necesidades de personas vulnerables, la información general, facilitada en una sección específica de la interfaz en línea que sea fácil y directamente accesible desde la página en la que se presenten las ofertas, relativas a los principales parámetros que determinan la clasificación de ofertas presentadas al consumidor.

A mayor abundamiento, es preciso señalar que tanto el artículo 20.3 como el 97 bis se derivan de una directiva de armonización plena, como es la Directiva 2019/2161[123], por

[123] Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE

lo que queda limitado el margen autonómico a la hora de añadir información adicional. Por tanto, se pueden establecer medidas autonómicas dirigidas a guías o inspecciones, como veremos posteriormente, pero no a obligaciones sustantivas adicionales. Esto será algo similar a lo que ocurrirá con la trasposición de la Directiva 2024/2853.

Por último, destaca el artículo 82 TRLGDCU, que regula cláusulas abusivas, y aplicable a contratos digitales.

5. Derechos recogidos en el Reglamento de Servicios Digitales

En cuanto al Reglamento de Servicios Digitales[124], destaca su artículo 26, referente a la transparencia de publicidad en las plataformas en línea, en el que se indica que los prestadores de plataformas en línea se deberán asegurar de que, por cada anuncio publicitario concreto presentado a cada destinatario, los destinarios del servicio deben ser capaces de identificar, de forma clara y concisa estas cuestiones: que la información es un anuncio publicitario, cuál es la persona física o jurídica en cuyo nombre se presenta el anuncio, la persona física o jurídica que ha pagado por el anuncio, la información significativa, accesible directa y fácilmente desde el anuncio acerca de los principales parámetros utilizados para determinar el destinatario a quien se presenta el anuncio publicitario, etc. También indica que los prestadores de plataformas en línea ofrecerán a los destinatarios del servicio una funcionalidad para declarar si el contenido que proporcionan es una comunicación comercial o contiene comunicaciones comerciales y que los prestadores de plataformas en línea no presentarán a los destinatarios del servicio anuncios basados en la elaboración de perfiles.

Destaca también el artículo 27, referente a la transparencia del sistema de recomendación, en el cual se indica que los prestadores de plataformas que utilicen sistemas de recomendación establecerán sus condiciones generales, utilizando un lenguaje claro y comprensible, así como los parámetros principales utilizados en sus sistemas de recomendación o cualquier otra opción a disposición de los destinatarios del servicio para modificar o influir en dichos parámetros. En caso de que haya varias opciones disponibles para los sistemas de recomendación que determinen el orden relativo de información que se presente a los destinatarios del servicio, los prestadores de plataformas en línea pondrán a su disposición una funcionalidad que permita al destinatario del servicio seleccionar y modificar en cualquier momento la opción preferida.

En cuanto al artículo 28, articula un mecanismo de protección de los menores en línea, obligando a los prestadores de plataformas en línea accesibles a los menores a establecer medidas adecuadas y proporcionadas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en su servicio.

---

del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. DOUE núm. 328, de 18 de diciembre de 2019.

[124] Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE

Por último, destaca su artículo 38, en el que se añade la obligación de ofrecer "al menos una opción no basada en perfilado" respecto a aquellos prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño (VLOP/VLOSE) que utilicen sistemas de recomendación.

6. Derechos recogidos en la Directiva de créditos al Consumo

Respecto a la Directiva (UE) 2023/2225[125] (normativa de armonización plena), destaca su artículo 13, referente a las ofertas personalizadas basadas en un tratamiento automatizado, que refuerzas el derecho a la intervención humana. En estos casos, y sin perjuicio de lo dispuesto en el RGPD, los Estados miembros exigirán que los prestamistas y los intermediarios de crédito informen a los consumidores de forma clara y comprensible cuando se les presente una oferta personalizada basada en el tratamiento automatizado de datos personales.

7. Derechos recogidos en la Directiva de servicios financieros celebrados a distancia

En cuanto a la Directiva (UE) 2023/2673[126], destaca su artículo 16 bis, en el que se establecen requisitos de información de los contratos a distancia de servicios financieros destinados a los consumidores. En el mismo se indica que, con suficiente antelación al momento en que el consumidor quede vinculado por un contrato a distancia, el comerciante le proporcionará, de forma clara y comprensible, la siguiente información: la identidad y la actividad principal del comerciante, la dirección geográfica de su establecimiento, los datos de contacto en aras a dirigir una posible reclamación, en caso de que esté inscrito en un registro público, que se indique cuál, una descripción de las principales características del servicio, el precio total que debe pagar el consumidor al comerciante, la información sobre las consecuencias de los pagos atrasados, si el servicio financiero está relacionado con otros riesgos, si existen impuestos y costes que no sean facturados por el comerciante, las modalidades de pago y ejecución, la existencia o no del derecho de desistimiento, la duración contractual mínima, etc. El apartado realmente importante de este precepto es el i), en el que se indica que, cuando proceda, deberá informarse de que el precio ha sido personalizado basándose se una toma de decisiones automatizadas.

En este sentido, también destaca introduce el artículo 16 quinquies, apartado 3, que establece el derecho a solicitar intervención humana cuando interactúe con el comerciante a través de interfaces en línea totalmente automatizadas, tales como robots conversacionales (chatbots), asesoramiento robotizado, herramientas interactivas o medios similares. También destaca el considerando 40 (que tiene un alcance primordialmente precontractual), en el que se indica lo siguiente: *" Para garantizar que comprenda los efectos que puede tener el contrato en su situación económica, el*

[125] Directiva (UE) 2023/2225 del Parlamento Europeo y del Consejo, de 18 de octubre de 2023, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 2008/48/CE.

[126] Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023, por la que se modifica la Directiva 2011/83/UE en lo relativo a los contratos de servicios financieros celebrados a distancia y se deroga la Directiva 2002/65/CE

consumidor siempre debe poder obtener, en la fase precontractual, intervención humana en nombre del comerciante, de manera gratuita y durante el horario comercial del comerciante. El consumidor también debe tener derecho a solicitar intervención humana —en casos justificados y sin que ello suponga una carga indebida para el comerciante— una vez celebrado el contrato a distancia. Esto podría incluir el derecho a una intervención humana cuando se prorrogue un contrato, en caso de dificultades importantes para el consumidor o cuando sea necesaria una explicación más detallada sobre las condiciones contractuales."

Es preciso destacar que la trasposición estatal de esta normativa condiciona la ejecución autonómica que quiera lograrse, en materia de información, inspección e incluso tutela administrativa. A continuación, incluimos un cuadro explicativo en el que resumimos la normativa anteriormente citada, junto con los principales artículos destacables de la misma, los derechos reconocidos en ella, así como los mecanismos de protección incluidos:

Normativa	Artículo(s)	Subderechos Reconocidos	Mecanismos de Protección
Reglamento de Inteligencia Artificial (RIA)	Artículo 50, Artículo 86, AESIA, Convenio IA, Código Buenas Prácticas	- Transparencia en interacción con IA - Marcado de contenido sintético - Información sobre sistemas biométricos - Explicación de decisiones automatizadas - Evaluación continua de riesgos - Buenas prácticas	- Supervisión por AESIA - Reclamaciones ante autoridades independientes - Sanciones desde agosto 2025 - Publicación de contenidos manipulados por IA - Coordinación institucional y normativa transversal
Reglamento General de Protección de Datos (RGPD)	Artículo 13.2, 14.2, 15, 22, Artículo 8 Carta DFUE	- Derecho de información - Derecho de acceso - Información sobre decisiones automatizadas - Derecho a no ser objeto de decisiones automatizadas - Consentimiento y oposición al tratamiento automatizado	- Intervención humana garantizada - Formularios de oposición - Supervisión por autoridades de protección de datos - Aplicación del RGPD y Carta de Derechos Fundamentales de la UE

Normativa	Artículo(s)	Subderechos Reconocidos	Mecanismos de Protección
Ley de Competencia Desleal (LCD)	Artículo 22	- Prohibición de prácticas señuelo - Prohibición de promociones engañosas	- Control por autoridades de consumo - Posibilidad de reclamación judicial o administrativa - Aplicación de sanciones por prácticas desleales
Reglamento de Servicios Digitales (RSD)	Artículo 26, Artículo 27	- Identificación clara de publicidad - Transparencia en segmentación publicitaria - Transparencia en sistemas de recomendación - Opción de modificar parámetros de recomendación	- Funcionalidades accesibles en plataformas - Condiciones generales claras - Prohibición de anuncios basados en perfiles - Supervisión por autoridades digitales
Directiva (UE) 2023/2225 (Créditos al Consumo)	Artículo 13	- Información sobre ofertas personalizadas basadas en tratamiento automatizado	- Obligación de informar de forma clara y comprensible - Supervisión por autoridades financieras - Aplicación conjunta con RGPD
Directiva (UE) 2023/2673 (Servicios Financieros a Distancia)	Artículo 16 bis	- Información precontractual completa y clara - Identidad del comerciante - Características del servicio - Precio total y riesgos asociados - Derecho de desistimiento	- Información accesible antes de vinculación contractual - Atención a consumidores vulnerables - Supervisión por autoridades de consumo y financieras
Directiva (UE) 2023/2673 (Servicios Financieros a Distancia)	Artículo 16 quinquies	- Derecho a solicitar intervención humana cuando interactúe a través de chatbots.	- Asistencia humana en la fase precontractual; y una vez celebrado el contrato, en casos justificados (detalle precisiones contractuales)

8. Estudio a fondo: derecho de transparencia e información

Respecto a la información sobre la existencia del sistema de IA, es esencial informar sobre para qué sirve, detallando los fines generales y concretos del modelo y la prioridad de estos. Se trata de información que debe proporcionar el proveedor al usuario, y debe tener en cuenta que la transparencia a la que obliga la normativa en materia de IA es "de un nivel adecuado para que el usuario y el proveedor cumplan las obligaciones previstas". En cuanto al uso público de IA, se debe informar sobre el alcance de la herramienta, para qué ha sido diseñada, o para que no, incluidos los fines ara los que las personas pueden pensar erróneamente que se utilizará las herramientas[127].

Habiendo indicado la importancia de tales conceptos, cuando se realiza uso de estos algoritmos en la Administración del Estado deben ser transparentes, cumplir con los estándares óptimos y dotar de toda la confianza posible a los procesos gubernamentales cuando liberan la toma de decisiones de la subjetividad humana, pues estos procesos deben ser justos, y crear los menos daños posibles. Sin embargo, esto es algo que no ha pasado, tal y como refleja jurisprudencia reciente[128].

En primer lugar, hablamos del caso BOSCO. Esta es una herramienta desarrollada por la Administración y utilizada por las comercializadoras de referencia para decidir quién cumple los requisitos para acceder al bono social. Sin embargo, en vez de convertirse en una herramienta fiable y útil, procedió a negar de forma automática estas ayudas a determinadas personas. Uno de los principales fallos denunciados por la Fundación Civio fue que a las personas viudas con rentas bajas siempre se les negaba la solicitud, aunque cumpliesen los requisitos[129]. No parece que fuese debido a un error de programación, sino que el modelo no sabía las respuestas correctas al no contar con todas las variables explicativas. En este sentido, destaca la sentencia del Tribunal Supremo núm. 3826/2025, de 11 de septiembre de 2025, que resuelve esta problemática. Establece lo siguiente: "La configuración del derecho de acceso a la información pública que hemos expuesto adquiere especial relevancia ante los riesgos que entraña el uso de las nuevas tecnologías en el ejercicio de las potestades públicas o la prestación de servicios públicos, como ocurre con el empleo de sistemas informáticos de toma de decisiones automatizadas en la actividad de las Administraciones públicas, especialmente, cuando, como aquí acontece, tienen por objeto el reconocimiento de derechos subjetivos de los ciudadanos

[127] Últ. ob. cit., pág. 32.
[128] FINOL ROMERO, L., ESIS VILLARROEL, I., ob. cit., pág. 177.
[129] TAHIRÍ MORENO, J. A., "El principio de presunción de fiabilidad de las decisiones algorítmicas desfavorables. Una nueva garantía frente a las decisiones automatizadas y el uso de sistemas de inteligencia artificial en la administración pública", *Revista Aragonesa de Administración Pública,* núm. 60, 2023, pág. 207.

y, más aún, cuando se trata de derechos de carácter social, atribuibles a los ciudadanos más desfavorecidos o necesitados de protección."

De la resolución menciona destacan dos definiciones concretas. En primer lugar, el principio de "transparencia algorítmica", que es el que impone a las Administraciones públicas obligaciones de información pública para facilitar el acceso de los ciudadanos, en mayor o menor medida, a las características fundamentales de los algoritmos empleados en la toma de decisiones o su código fuente, como una manifestación del principio de transparencia (recogido en el artículo 105 b) de la CE). En segundo lugar, el de "democracia digital o electrónica", que nace como consecuencia del uso de las tecnologías digitales por los gobiernos y los ciudadanos y su desarrollo pretende fortalecer las prácticas democráticas tradicionales, entendiendo fundamental para garantizar la misma el acceso a la información público y la transparencia algorítmica".

Es por esto por lo que se entiende que los Poderes públicos tienen la obligación de explicar de forma comprensible el funcionamiento de los algoritmos que se emplean en la toma de decisiones que afectan a los ciudadanos. Por tanto, el derecho de acceso al código fuente es uno de los mecanismos a través de los cuales se garantiza la transparencia algorítmica que demanda el pleno ejercicio del derecho a la información pública. Ahora bien, en el presente caso este derecho se encuentra en conflicto con el derecho de propiedad intelectual de la Administración General del Estado sobre la aplicación BOSCO. En este caso, el Tribunal entiende que el mero riesgo de eventuales perjuicios para el derecho de propiedad intelectual de la Administración pública no puede constituir causa de exclusión del derecho de acceso. Al igual que tampoco es motivo la "imposibilidad de cálculo", pues en ese caso se debería aportar la documentación adicional que lo corroborase, no pudiéndose afirmar esa causa sin soporte técnico concluyente. Por tanto, concluye que la Fundación Ciudadana Civio tiene derecho a acceder al código fuente de la aplicación informática BOSCO con la finalidad de que pueda conocer las operaciones diseñadas para la concesión del bono social y comprobar que se ajustan al marco normativo aplicable.

De otro lado, respecto a si se debe acceder al código fuente para identificar la causa de la denegación del bono social, parte de la doctrina considera que en estos supuestos no sería necesario conocer el mismo, pues solo es la traducción de una norma jurídica a lenguaje informático[130]. También defienden que, si hubiera existido el principio de presunción de fiabilidad[131] probablemente ni un solo ciudadano hubiera quedado excluido del acceso al bono social eléctrico injustamente. El principal motivo para esa denegación son los derechos de propiedad industrial sobre la herramienta tecnológica. En otros casos, referente al acceso al código en el sistema electoral, sí se permite el acceso al mismo, como en Brasil, donde se utiliza para el sistema electrónico electoral, y se permite dicho acceso como garantía de su funcionamiento neutral. Sea como fuere, la doctrina afirma

[130] Últ. ob. cit., pág. 209.
[131] Este principio ha de entender como una mera propuesta doctrinal.

que la transparencia o el acceso íntegro al código fuente *stricto sensu* no es un fin en sí mismo, y no actúa como barrera ante los posibles usos no deseados de los algoritmos[132].

En segundo lugar, es de gran importancia la STJUE de 27 de febrero de 2025, asunto C-203/2022, Dun & Bradstreet, que interpreta por primera vez el alcance del derecho del interesado a obtener "información significativa sobre la lógica aplicada" a decisiones individuales automatizadas y su alcance frente al secreto comercial, en atención al artículo 15.1 h) del RGPD, como un score de solvencia. Esta información debe ser comprensible, accesible y libre de tecnicismos, permitiendo al interesado entender qué datos se usaron y cómo influyeron en el resultado. Además, el Tribunal rechaza que el responsable del tratamiento pueda escudarse en el secreto comercial para denegar esa información. En este sentido, se dice explícitamente: "explicación comprensible, accesible, libre de tecnicismos, con ejemplos; no puede negarse por secreto comercial, salvo canalización a autoridad de control". El responsable del tratamiento no puede negarse a facilitar explicaciones adecuadas sobre la lógica aplicada bajo el pretexto de revelar información protegida por la normativa de secretos comerciales o datos de terceros. Y ello porque, según el TJUE, se puede comunicar esta información únicamente a la autoridad de control o al órgano jurisdiccional competente, que ponderará los intereses en juego a efectos de determinar el alcance del derecho de acceso del interesado. Ahora bien, esta solución comporta una limitación práctica del derecho de acceso, en la medida en que, al implicar la intervención de una autoridad, puede suponer que se sobrepase el plazo de uno o dos meses previsto en el artículo 12.3 del RGPD para atender la solicitud del interesado. Para evitar esta consecuencia y garantizar el pleno ejercicio del derecho de acceso, el responsable del tratamiento podría facilitar directamente al interesado una explicación comprensible sobre la lógica aplicada, sin comprometer información protegida, ya sea relativa a terceros o a secretos comerciales. Como el responsable del tratamiento no tiene que informar sobre cuestiones técnicas ni facilitar información exhaustiva sobre todo el proceso de evaluación, en la mayoría de los casos no se podrá invocar una violación de los derechos de terceros o de los secretos comerciales. Con esta solución se permitiría conciliar el derecho del interesado a una explicación transparente, en un plazo razonable, con la protección de los secretos comerciales y la confidencialidad de los datos de terceros.

III. AFECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES ANTE CIERTAS PRÁCTICAS

Centrándonos en el derecho de consumo, destacan en primer lugar los sistemas de recomendación, que se definen como "un dispositivo que consiste en una base informática de obtención y procesamiento de datos sobre lo que los usuarios hacen en la red, o dentro de una plataforma determinada, y que, mediante la intervención de algoritmos, facilita el encuentro de cada usuario con aquello que podría interesarle[133]. Estas recomendaciones que proporciona el algoritmo encuentran su explicación en el profundo seguimiento y

[132] SIMÓN CASTELLANO, P., "Taxonomía de las garantías jurídicas en el empleo de los sistemas de inteligencia artificial*", Revista de Derecho Político UNED*, mayo-agosto 2023, pág. 163.
[133] ZELER, M., "Sistemas de recomendación en plataformas de streaming audiovisual: las lógicas de los algoritmos", *Artigo Seção Temática*, vol. 17, núm. 2, mayo-agosto de 2023, pág. 3.

análisis de datos que realizan los sistemas de recomendación. Además, estos trabajan con múltiples supuestos. Por ejemplo, en el caso de plataformas de contenido, destacan los siguientes: (i) el consumo como indicio de los gustos; (ii) las propiedades o categorías de los textos como explicación de los gustos; (iii) la relativa estabilidad de los gustos; (iv) la multiplicidad de los gustos; (v) la existencia de afinidad en los gustos de los distintos usuarios; y (vi) la existencia de correlaciones de cierta estabilidad entre el consumo de obras. Los sistemas de recomendación parecen funcionar mediante lógicas abductivas, de forma que en primer lugar se ofrece al usuario diferente opciones, y es a partir de esas primeras elecciones que realiza el usuario cuando el algoritmo comienza a realizar hipótesis acerca de cuáles podrían ser las semejanzas pertinentes entre las diferentes opciones[134]. Sin embargo, también prima la combinación de un volumen masivo de datos acerca de los usuarios y sus comportamientos almacenados en forma digital, sumado a la capacidad y velocidad de procesamiento que tienen los actuales equipos informáticos.

De esta manera, el sistema va acumulando y conociendo los gustos del usuario a lo largo del tiempo. Cuanto más conoce a un usuario, más predomina ese comportamiento que tiende a lo deductivo. Sea como fuere, los algoritmos están programados para darle mayor peso a los consumos recientes, por lo que esos *inputs* se renuevan permanentemente y el funcionamiento abductivo no se abandona[135]. De hecho podemos encontrar diferentes sistemas de recomendación: (i) sistema de recomendación basado en contenido, en el que el enfoque lógico se basa en la recomendación en función de las características de comportamiento y preferencias de los usuarios, siendo necesario tener disponibilidad de datos de los usuarios, creando un perfil de acuerdo a los atributos personales creados por el algoritmo; (ii) sistemas de recomendación enfocados en filtrado colaborativo, que Se basan en que si determinados usuarios compartieron los mismos gustos y preferencias en el pasado, es probable que tengan las mismas tendencias para elegir elementos similares en el futuro; y (iii) sistemas de recomendación de método híbrido, que están estrechamente relacionados con el campo del análisis de datos, en el cual se combinan el poder de múltiples tipos de algoritmos de aprendizaje automático para crear un modelo más robusto[136].

Una vez destacado su funcionamiento, hemos de ver que la principal afección para los consumidores es la protección de sus datos personales, así como el derecho a la transparencia algorítmica, pues estos sistemas suelen ser opacos y a las personas no son conocedoras completamente de su funcionamiento, ni de la relevancia de sus aplicaciones ni consecuencias. En este sentido, son de especial importancia las obligaciones de transparencia algorítmica recogidas en el RSD, que se extienden a los servicios de información, debiendo las plataformas informar, de manera sencilla y comprensible, acerca de cuáles son los parámetros principales utilizados en sus sistemas de recomendación, así como cualquier opción a disposición de los destinatarios del servicio para modificar o influir en dichos parámetros principales. Como mínimo, en el artículo 27 del RSD se indica que se debe proporcionar al destinatario del servicio, a fin de

[134] ZELER, M., ob. Cit., pág. 17.
[135] Últ. ob. cit., pág. 18.
[136] MARTÍNEZ ARROYAVE, M.J., *Sistemas de recomendación para la implementación de ofertas según la necesidad de la empresa Ditrimar*, 2023, pág. 15.

explicarle por qué se le recomienda una determinada información "los criterios más significativos a la hora de determinar la información sugerida al destinatario del servicio", y "las razones de la importancia relativa de dichos parámetros"[137].

Esas obligaciones de transparencia para los sistemas de recomendación se completan para las VLOP (Very Large Online Platforms) y los VLOSE (Very Large Online Search Engines) en el artículo 38. Estos prestadores deberán incluir en sus sistemas de recomendación al menos una opción, para cada uno de sus sistemas, que no se basen en la elaboración de perfiles, en el sentido de lo establecido en el artículo 4 del RGPD.

En segundo lugar, destaca la priorización de ofertas. En este sentido, la priorización de ofertas se refiere al proceso de clasificar y ordenar las ofertas de productos y servicios de acuerdo con su valor y prioridad. Esto implica evaluar las características, beneficios y necesidades de los clientes para determinar cuáles son más valiosas y deben ser priorizadas en el proceso de toma de decisiones.

En tercer lugar, los precios personalizados, que, aunque aparentemente reporten importantes beneficios y ventajas para usuarios y consumidores, son muchas las consecuencias negativas que pueden seguir a la elaboración de perfiles y la adopción de decisiones de personalización, afectando a los derechos de los consumidores, dentro de los que se incluye la intimidad y la protección de datos personales, la discriminación en el acceso a bienes y servicios, la pérdida del excedente contractual esperable, la manipulación de las preferencias, errores en la atribución de uno u otro perfil, etc. Hay muy diversas estrategias y modalidades de personalización en la contratación con consumidores online, de forma que un consumidor puede tener que pagar un precio para acceder al mismo bien, diferente al que debe satisfacer otro consumidor en el mismo sitio web. Los economistas han distinguido diferentes formas de discriminación de precios, y han construido la noción de "discriminación de primer grado"[138], en virtud de la cual el empresario podría estar en condiciones de identificar el precio al que cada consumidor individual estaría dispuesto a contratar y ofrecerle el bien a cambio de este precio individualizado[139]. Son las operaciones de *big data* las que contribuyen a un conocimiento más completo de la predisposición a pagar de cada consumidor.

Si bien es cierto que hay estrategias de discriminación de precios que no se consideran negativas, hay otras que sí, como el suponer que un consumidor acabará pagando un precio superior sólo porque tiene un poder adquisitivo más alto. El principal problema suele aparecer cuando la personalización de las de las ofertas y de la información que perciben los consumidores se utiliza para manipular la predisposición a pagar de los consumidores. Los datos que precisan este tipo de sistemas pueden obtenerse a través de

[137] Véase en este sentido GARRIGA DOMÍNGUEZ, A., "Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales", *Revista Española de la Transparencia,* núm. 17, 2023, pág. 157

[138] Es preciso aclarar que se trata de una categoría económica, no jurídica. De tal forma que para que pueda exigirse cierto reproche jurídico es preciso que se vulnera el derecho a la igualdad, no discriminación o el principio de transparencia algorítmica.

[139] RUBÍ PUIG, A., "Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores", *Revista de Educación y Derecho*, núm. 24, 2021, pág. 6

muy diversas fuentes, como puede ser a través de la aceptación de cookies de navegador, huellas digitales, *web beacons* (que son las balizas web, elementos de seguimiento utilizados en páginas web aplicaciones y correos electrónicos, cuya principal función es verificar que el usuario ha accedido a determinados contenidos, como puede ser visitar una página web), bases de datos estructurales, datos públicos, contenido generado por los usuarios, entre otros. En ocasiones, los responsables del tratamiento pueden aprovecharse de los sesgos cognitivos de los usuarios y contextualizan la información o en el marco en el que los consumidores deben tomar una decisión, para que cedan ante la opción de proporcionar sus datos personales, y esto es lo que se conoce como dark patterns[140].

Es fundamental que se respeten las precisiones recogidas en el artículo 22 del RGPD, cuando estos procedimientos se realicen a través de decisiones automatizadas y dicha decisión produzca efectos jurídicos en el interesado o le afecte de un modo similar. Un ejemplo será si a partir de una determinada elaboración de un perfil, una entidad de crédito deniega un préstamo a un sujeto, de forma que esa decisión afectará a esa persona de modo similar a que si tuviera efectos jurídicos[141]. Destacan también las obligaciones recogidas en los artículos 13 y 14 del RGPD en materia de transparencia, que son deberes que incumben al responsable del tratamiento.

En cuarto lugar, destaca el uso de los asistentes virtuales en materia de contratación. Los asistentes virtuales, también denominados *chatbots,* son aplicaciones de software que pueden basarse en IA y en procesamiento del lenguaje natural para entender las necesidades humanas y guían hacia el resultado deseado con el mínimo trabajo por parte del usuario final, respondiendo como si fuesen una persona y simulando las accesiones con una conversación ayudando a resolver consultas o dando soluciones a problemas, o incluso se prestan como la otra parte en la relación contractual[142]. En el ámbito concreto del consumo, la finalidad del asistente digital es mejorar la eficiencia y la precisión en la gestión de la relación contractual entre el sujeto proveedor y consumidor, en las partes de negociación, conclusión o incluso ejecución del contrato.

En cuanto al funcionamiento del asistente digital, recopila datos relevantes sobre el consumidor, el producto o servicios objeto de contrato, y cualquier otra información pertinente para la toma de decisiones. Esos datos son procesados por el sistema, empleando algoritmos específicos, pudiéndose aplicar técnicas de análisis de datos para identificar patrones o tendencias que ayuden a informar la toma de decisiones[143]. En este sentido, es de especial relevancia el Informe del Instituto de Derecho Europeo[144], que revela una serie de formas típicas en las que pueden intervenir, como puede ser un producto inteligente con un sistema integrado de asistente digital, o una aplicación de

[140] Últ. ob. cit., pág. 10.
[141] Últ. ob. cit., pág. 15.
[142] TRUJILLO VALDIVIEZO, G. et. al, "Los asistentes virtuales y la calidad de servicio al cliente", Revista *Internacional de Tecnología, Ciencia y Sociedad*, 2023, pág. 3.
[143] PACHECO JIMÉNEZ, M.ª N., "Sistemas de inteligencia artificial para la toma automatizada de decisiones: algunos problemas de los contratos algorítmicos concluidos con asistente digital", *Cuadernos de Derecho Privado*, núm. 9, págs. 154-155.
[144] En el mismo se recogen los Principios del Instituto Europeo de Derecho (European Law Institute, ELI), sobre tecnología Blockchain, smart contracts y protección de consumidores.

asistente digital independiente, entre otros. En cuanto a los principios ELI, destaca en principio 2, en el que se indica que será de aplicación la legislación sobre consumidores a los contratos algorítmicos. Por tanto, el contrato algorítmico celebrado a través de un asistente digital entre consumidor y comerciante entra en el ámbito de aplicación de la legislación de la UE en materia de Derecho de Consumo, de forma que el comerciante no podrá evitar su responsabilidad por las acciones derivadas de su asistente digital, infringiendo derechos de la persona consumidora basándose que fue resultado de las decisiones tomadas por un asistente digital[145]. También destaca el principio 3, en el que se recogen obligaciones de información precontractual, de forma que la obligación de proporcionar información previa al contrato por parte de quien comercia es un deber general que debe persistir, independientemente de que la persona consumidora se sirva de un asistente digital. También se destaca la importancia en esta materia de la Directiva (UE) 2019/770[146], así como la Directiva (UE) 2019/771[147], que constituyen una sólida base para la persona consumidora que busque solución en aquellos supuestos en los que un asistente digital actúa de una manera diferente a la razonablemente esperada, y ello conlleve una falta de conformidad. La doctrina considera que esa falta de conformidad debería solventarse atendiendo a las soluciones que contemplan las dos Directivas, en atención a los artículos 7 y 8 de la Directiva de compraventa de bienes, y artículos 6 y 7 de la Directiva de servicios digitales, lo que se traduce en la reparación, sustitución, reducción de precio o incluso la resolución del contrato, incluso pudiendo añadirse el derecho a una indemnización de daños y perjuicios para compensar las posibles pérdidas ocasionadas por la falta de conformidad derivada de la actuación de un asistente digital[148].

En quinto lugar, la evaluación de solvencia realizada al consumidor. Actualmente, es común que se realice la comprobación de la solvencia de determinados usuarios mediante sistemas automatizados, gracias al uso de la IA. Esto se traduce en el riesgo de generar nuevas formas de discriminación a determinados grupos o personas, o de perpetuar patrones históricos de discriminación por motivos de origen racial o étnico, género, discapacidad, edad u orientación sexual, tal y como se establece en el Considerando 58 del AI Act. Además, en este instrumento normativo se definen los sistemas automatizados de la valoración de solvencia como sistemas de alto riesgo, tal y como se recoge en el anexo III, apartado 5.b) del AI Act. Tal y como se establece en los artículos 9, 10 y 17 del AI Act, esto se traduce en la debida adopción *ex ante* de medidas de gestión de riesgo, un plan adecuado de gobernanza de los datos, un sistema de gestión de calidad, y una verificación previa del impacto sobre los derechos fundamentales que, en su caso, complementaría a la que se deba llevar a cabo en virtud de lo establecido en el artículo 35 del RGPD.

Como ejemplo de entidades que deberán llevar a cabo este debido cumplimiento, nos encontramos con las empresas de puntuación de crédito (*scoring*), que surgieron con la

[145] Últ. ob. cit., pág. 157.
[146] Directiva (UE) 2019/770, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministros de contenidos y servicios digitales.
[147] Directiva (UE) 2019/771, del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de compraventa de bienes.
[148] PACHECO JIMÉNEZ, M.ª N., ob. cit., pág. 163.

finalidad de valorar la solvencia de personas o entidades en relación con determinadas garantías o instrumentos, al igual que las entidades tanto financieras como de seguros que actúan con fines profesionales, en la medida que utilicen sistemas de IA de alto riesgo, tal y como se establece en los artículos 4.2 y 72.1 del AI Act. En este sentido, destaca la STJUE C-634/21 (SCHUFA), mencionada anteriormente.

Destacan también en este sentido las *FinTech,* que conceden créditos al consumo y que se nutren fundamentalmente de datos alternativos para evaluar el mérito crediticio de consumidores que no disponen de datos económicos o financieros. Algunos de estos datos son recogidos directamente por los prestamistas de los consumidores, pero otros se adquieren de bases de datos de terceros, como pueden ser Acxiom y Experian[149]. En este sentido, es preciso señalar que la Directiva (UE) 2023/2225 prohíbe el uso de los datos no estructurados para inferir la capacidad de pago del consumidor. También es interesante lo establecido en su artículo 18, puesto que, a diferencia de lo establecido en el artículo 22 del RGPD, simplemente se refiere al "uso" de tratamientos automatizados de datos por parte del prestamista, y también se da importancia en la misma a la valoración de solvencia realizada por las agencias de *scoring* a petición de los bancos, siendo indiferente que el prestamista acepte y asuma el resultado o que la decisión sobre el crédito se asiente sobre la base de nuevos datos[150].

Puesto que este sistema es uno de los considerados de alto riesgo, en la normativa europea se recogen una serie de derechos para proteger a los consumidores. En primer lugar, teniendo en cuenta los artículos 13.2 f), 14.2 g) y 15.1 h) RGPD, el interesado debe poder obtener del responsable del tratamiento de datos información significativa sobre la lógica aplicada por el algoritmo, así como acerca de la importancia que pueda tener dicho tratamiento. También destaca en este sentido, el artículo 18.8 de la Directiva (UE) 2023/2225, que consagra el derecho del solicitante del crédito con tratamiento automatizado de datos a obtener una explicación clara y comprensible de la evaluación de solvencia. Destaca en este ámbito la sentencia de la Sala Primera del Tribunal de Justicia de la Unión Europea, de 7 de diciembre de 2023, asunto C-634/21, como primera sentencia sobre decisiones automatizadas y sus implicaciones jurídicas para la protección de datos y el Reglamento de IA. La misma adapto un enfoque garantista expandiendo el alcance del artículo 22 del RGPD más allá del responsable formal de la decisión, abarcando a terceros que procesen datos.

La parte demandada, SCHUFA, es una empresa que proporciona información sobre la solvencia de consumidores basada en procedimientos matemáticos y estadísticos, realizándose una clasificación de la persona atendiendo a su comportamiento. El demandante alega que su solicitud de préstamo fue denegada sobre la base de la información proporcionada por SCHUFA, así como que ejercitó de derecho de acceso de protección de datos. El principal problema fue que la empresa proporcionó contenido genérico, sin mostrar al demandante los datos sobre sí mismo, y sin explicar la ponderación que de esos datos se había realizado en valores de probabilidad. Además, la

[149] ARROYO ARAYUELAS, E., "Inteligencia artificial y evaluación de la solvencia", *Revista Justicia y Derecho*, vol. 8, 2025, pág. 3.
[150] Últ. ob. cit., pág. 5.

empresa alegó que ella no era la responsable de la denegación del crédito, sino sus socios contractuales, a quienes les facilitada la información de solvencia. La sentencia realiza una interpretación garantista, al considerar que la generación del valor de probabilidad por parte de SCHUFA no es un mero acto preparatorio, por lo que cae en el ámbito de aplicación del artículo 22 del RGPD[151].

En segundo lugar, destaca el derecho a obtener una revisión de la decisión u oponerse a ella, de forma que el consumidor cuya solicitud de crédito haya sido objeto de un tratamiento automatizado puede expresar su punto de vista al prestamista, recogido en el artículo 18.8 de la citada Directiva, así como prevé el artículo 22.3 del RGPD, para el caso de que una decisión se haya tomado lícitamente de forma exclusiva o preponderadamente automatizada.

En tercer lugar, destaca el derecho a la evaluación humana de la solvencia, en virtud de los establecido en los artículos 18.8 y 18.9 de la Directiva (UE) 2023/2225. Se establece que solo se puede solicitar una evaluación humana en caso de que la respuesta a la solicitud haya sido negativa. Esto es posible que confirme que cualquier otra intervención humana a la que tenga derecho el consumidor no incluye el abandono por parte del prestamista del tratamiento automatizado de datos que previamente haya utilizado[152].

IV. PROCEDIMIENTOS DE RECLAMACIÓN: SIMPLIFICACIÓN Y PROTOCOLOS PARA OMICS.

Una vez examinados cuáles son los derechos de los consumidores ante diversas consecuencias derivadas del uso incorrecto, o los fallos por parte de sistemas de IA, a continuación, vamos a explicar cuál sería el proceder oportuno para reclamar un determinado daño que haya podido ser causado.

En primer lugar, es importante recopilar toda la documentación relacionada con el conflicto, entre la que se encuentran contratos, facturas, correos con la empresa, términos de uso, registro de logs, histórico de precios, capturas de pantalla cotejadas, logs de actividad, resultados generados por la IA, términos de uso o políticas de privacidad, etc. Además, es preciso identificar cuál ha sido la vulneración, si se ha incumplido la TRLGDCU, si hay un tratamiento de datos personales no autorizados, en virtud de lo establecido en el RGPD, o si se ha tomado una decisión automática sin intervención humana.

En segundo lugar, antes de acudir a la OMIC, es obligatorio haber intentado resolver el conflicto directamente con la empresa, ya sea a través del servicio de atención al cliente, o mediante una reclamación escrita. Se pueden hacer uso de formulario de reclamaciones o canales oficiales, se puede exigir que intervenga una persona en los casos de decisiones automatizadas o se puede solicitar una rectificación, compensación o incluso explicación. De este primer intento de conciliación, el consumidor debe guardar una copia de forma que quede constancia de este.

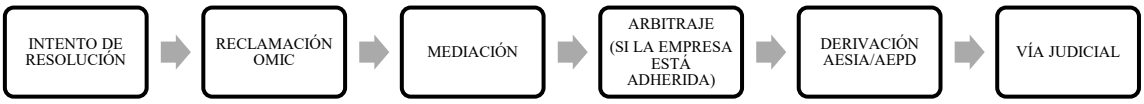
[151] En este sentido, véase PACHECO JIMÉNEZ, M.ª N., ob. cit., pág. 166.
[152] ARROYO ARAYUELAS, E., ob. cit., pág. 9.

Habiendo realizado ese primer intento sin respuesta positiva, se puede presentar la reclamación ante la OMIC más cercana (la ciudad donde vivas), o de forma telemática, si esa opción está disponible en el municipio. Deben incluirse datos personales, datos de la empresa, indicar que el problema es con un sistema automatizado y describir el sistema de IA (error, sesgo, daño, falta de transparencia, etc.), explicación clara de los hechos, así como la petición concreta que se solicita.

Posteriormente, la OMIC traslada la reclamación a la empresa, intenta una mediación amistosa, y si no se alcanza un acuerdo, se puede comenzar un arbitraje de consumo o incluso iniciar una acción judicial. Dependiendo del caso, se deberá solicitar a la OMIC que derive el caso a la Delegación de Protección de Datos, al Arbitraje de Consumo, si la empresa está adherida, o incluso a la Agencia Española de Supervisión de Inteligencia Artificial. En caso de que la empresa no responde o niegue responsabilidad alguna, deberá plantearse interponer, en su caso, una denuncia ante la Agencia Española de Protección de Datos (en adelante, AEPD), acudir a asociaciones de consumidores o incluso valorar la vía judicial, si ha existido daño económico o moral[153]. Es importante destacar que, por motivos de competencia, la OMIC no debe solicitar el código fuente, sino que pedirá explicaciones significativas y evidencias, como parámetros, logs, etc. Posteriormente, se coordinará con la AEPD o la AESIA.

Adjuntamos un modelo de esta solicitud en el apartado de Anexos.

1. Diagrama de flujo del procedimiento



[153] En este sentido, es fundamental destacar que la nueva Directiva 2024/2853 en materia de productos defectuosos, considera al software como producto, siendo a partir de su aprobación completamente posible reclamar los daños derivados de este tipo de productos, pese a los problemas de prueba que pueden surgir. Ahora bien, el contenido informativo no se considera como producto. En este sentido se ha planteado un gran debate en torno a la información emitida por sistemas de IA generativa, a la hora de reconocer la responsabilidad de los proveedores de dichos sistemas. Es por esto por lo que la doctrina, como destaca EVANGELIO LORCA, R., Responsabilidad civil e inteligencia artificial en el ámbito sanitario, MORENO MARTÍNEZ, J.A. FEMENÍA LÓPEZ, P.J. (coords.), *Inteligencia artificial y derecho de daños: cuestiones actuales. Acorde al Reglamento (UE) 2024/1689*, ed. Dykinson, Madrid, 2024, pág. 176 consideran que las aplicaciones como Chat GPT deben quedar excluidas de la aplicación de la Directiva 2024/2853.
De otro lado, y como novedad introducida, también es posible la indemnización del daño psicológico.; y también es destable los mecanismos de facilidad probatoria introducidos. También se mantiene la cláusula de exoneración por riesgos del desarrollo, de forma que el proveedor del producto podrá quedarse exonerado si demuestra que, en el momento en el que se ponen en circulación los productos, el estado de la ciencia y de la técnica no le permitía advertir ese defecto, no responderá. Sin embargo, la doctrina entiende que esta cláusula deberá entenderse a la luz de la nueva era digital, destacando al respecto autores como Guilles Grau o Celeste Danesí.

2. Guías rápidas para consumidores: qué reclamar y cómo

En primer lugar, el consumidor tiene derecho a la transparencia, de forma que debe saber que está interactuando con un sistema de IA, cuál es el propósito del sistema, y cómo influye en la toma de decisiones, todo ello con base legal en los artículos 13 a 15 del RGPD y el AI Act. El derecho del consumidor a la transparencia en su interacción con sistemas de IA se recoge expresamente en el artículo 50 AI Act, que establece que los proveedores[154] deben garantizar que, cuando los sistemas de IA interactúen directamente con personas físicas, estas sean informadas de que están interactuando con un sistema de IA, salvo que ello resulte evidente para una persona razonablemente informada. Además, el artículo exige que se proporcione información sobre el carácter artificial de los contenidos generados o manipulados (texto, imagen, audio o vídeo). Por su parte, el artículo 86, refuerza esa transparencia con una exigencia *ex post* en situaciones de mayor impacto: cuando la decisión adoptada con apoyo en un sistema de alto riesgo le produce efectos jurídicos o le afecta significativamente, de forma que en estos casos el consumidor tiene derecho a recibir una explicación clara y significativa del papel desempeñado por la IA en la decisión y de los elementos principales que la sustentan. De este modo, ambos artículos se complementan: el primero asegura un derecho a la identificación y comprensión del sistema con el que se interactúa, y el segundo garantiza un derecho a la explicación sustantiva de la decisión cuando ésta afecta de manera relevante a la esfera jurídica o a los derechos fundamentales de la persona. Respecto a cómo reclamarlo, puede exigir por escrito que se identifique claramente el sistema de IA o solicitar una explicación clara y comprensible de su funcionamiento y criterios.

En segundo lugar, tiene derecho a no ser objeto de decisiones automatizadas (excepto si se cumplen las excepciones del artículo 22 relacionadas con el tratamiento necesario para determinados contractos, si existe consentimiento, etc.) de forma que si una IA toma decisiones que afectan significativamente al consumidor (por ejemplo, devengar un crédito, fijar el precio, etc.), el usuario tiene derecho a que en esta decisión intervenga una persona humana, a que se le proporcione una explicación clara e incluso a impugnar la decisión, en base a lo establecido en el artículo 22 RGPD, así como en la Carta de Derechos Digitales, adoptada el 14 de julio de 2021. Para reclamarlo, puede enviar una solicitud a la empresa exigiendo la revisión humana de la decisión, y en caso de respuesta negativa, acudir a la OMIC o a la AEPD.

En tercer lugar, tiene derecho a la protección de datos personales, de forma que, si el sistema de IA usa datos personales del consumidor como pueden ser el nombre, el historial de navegación, la ubicación, etc., el consumidor tiene derecho a saber qué datos se usan, rectificarlos o borrarlos o incluso a oponerse a su uso automatizado, en base al RGPD, así como a la LOPDGDD. Para reclamarlo, puede solicitar el acceso, rectificación

[154] Es preciso aclarar que cuando nos referimos al "proveedor" (*provider*) se hace referencia a (según se establece en el AI Act): "una persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente".

u oposición a ese tratamiento, que son los conocidos como derechos ARCO, y en caso de que la empresa no responsa, puede reclamar ante la AEPD.

En cuarto lugar, el consumidor tiene derecho a un trato justo y no discriminatorio, de forma que una IA no puede tomar decisiones basadas en sesgos injustos por razón de género, raza, orientación, etc., en base a los establecido en el AI Act, y diversas normas de carácter nacional y europeo. En cuanto a la reclamación, se debe documentar el trato injusto recibido y denunciar ante la empresa, OMIC o AEPD. En casos muy graves, se deben tomar acciones judiciales. Por ejemplo, el artículo 10.2 AI Act, que establece que los conjuntos de datos de entrenamiento, validación y prueba se someterán a prácticas de gobernanza y gestión de datos adecuadas para la finalidad prevista del sistema de IA de alto riesgo. Dichas prácticas se centrarán, en particular, en lo siguiente: el examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones.

V. CONCLUSIONES

Tal y como ha quedado reflejado a través de lo indicado en apartados anteriores, los riesgos que se derivan de las actuaciones en las que intervienen sistemas de IA son muy diversos, y los consumidores no se encuentran todavía lo suficientemente preparados en relación con el alcance de estos sistemas, ni tampoco tienen el conocimiento suficiente de los derechos que son poseedores en lo que a la relación con los sistemas de IA se refiere.

En este sentido, múltiples de derechos se pueden ver afectados como son el derecho a la privacidad, a la toma de decisiones automatizadas siempre que exista conocimiento, al tratamiento de datos personales con conocimiento, a ser atendido por una persona física, a la no discriminación por raza, edad, sexo, etc. Es por esto por lo que es preciso que las autoridades pertinentes fomenten el conocimiento de todos los riesgos que puede conllevar el uso de este tipo de sistemas.

Para ello, una de las recomendaciones principales a seguir es la creación de un nuevo órgano consultivo al que puedan dirigirse por parte de los consumidores todas las dudas en materia de IA, que pueda convertirse en un apoyo para los ciudadanos en esta nueva era en la que nos ha tocado vivir.

En segundo lugar, sería recomendable proporcionar un nuevo cauce administrativo al que puedan dirigirse todas las quejas que presenten los consumidores cuando en sus diversas relaciones con los comercios u otros establecimientos hayan intervenido este tipo de sistemas.

VI. CUADRO DE ACCIÓN ADMINISTRATIVA

Problema detectado	Normativa aplicable	Recomendación concreta	Nivel de competencia (UE/Estado/CCAA)
Falta de información al consumidor sobre el uso de IA	AI Act	Creación de una Unidad Técnica sobre IA y Consumo	Plena competencia (Estatuto Autonomía 31.1.22, para legislar y ejecutar políticas públicas)
Decisiones automatizadas sin intervención humana	RGPD	Actualizar protocolos de la OMIC	Competencia ejecutiva para inspección, sanción y mediación en conflictos de consumo
Sesgos algorítmicos	RIA, Directiva 2024/2853	Campañas informativas a consumidores	Competencia plena para desarrollar programas, campañas y formación ciudadana.
Tratamiento de datos personales sin consentimiento ni transparencia	LOPDGDD	Supervisión de tecnologías digitales	Competencia limitada, subordinada al marco estatal y europeo, pero puede actuar en materia de información, prevención y protección.
Falta de vías efectivas de reclamación	Estatuto del Consumidor de CLM	Desarrollo de un Observatorio Autonómico sobre IA y Derechos del Consumidor	Plena competencia (Estatuto Autonomía 31.1.22, para legislar políticas públicas)

VIII. CASO PRÁCTICO Nº 4: SITUACIÓN DE DISCRIMINACIÓN ALGORÍTMICA DESFAVORABLE POR NO CONCESIÓN DE CRÉDITO

Elemento	Detalle
Situación real	Una familia solicita una hipoteca al banco donde acude habitualmente, considerando que podría serle concedido, en atención a los requisitos observados. Sin embargo, cuando solicitan el préstamo se procede a la denegación automática de la misma. A través de la solicitud de información, son conocedores de que han sido objeto de una decisión automatizada a la hora de tratar sus datos y ofrecer la respuesta denegatoria. La aplicación no tenía almacenados datos de las personas que vivían en entornos rurales.
Problema detectado	Situación de discriminación algorítmica por falta de representatividad de los datos.
Normativa aplicable	RIA, RGPD, LOPDGDD, Directiva 2853/2024
Impacto en consumidores	Riesgo de discriminación, falta de accesibilidad, pérdida de oportunidades, sesgos algorítmicos indeseados, tratamiento de datos automatizados, falta de personal humano.
Propuesta autonómica	Crear un observatorio a través del cual se controlen y vigilen este tipo de actuaciones, de forma que puedan tener conocimiento de las ayudas en las que se utilizan estos tipos de sistemas y poder paliar los efectos indeseados del uso de estos cuando este tipo de fallos se producen.
Prioridad	Corto / Medio plazo.

CAPÍTULO V. CASOS DE USO EN SECTORES CLAVE (CON EJEMPLOS CONCRETOS)

I. AGROALIMENTACIÓN: TRAZABILIDAD DIGITAL, LOGÍSTICA

La adopción de sistemas de IA en la agricultura permite optimizar insumos y procesos (riego, plagas, fertilización). Estudios experimentales y evaluaciones sectoriales muestran reducciones significativas del uso de fertilizantes en determinadas explotaciones (el porcentaje varía por cultivo y metodología[155]). En este sentido, hay estudios que revelan que la mejora de la eficiencia energética en el conjunto de sistemas de producción es una de las claves para poder producir más alimentos con menor aplicación de fertilizantes[156]. Como ejemplos concretos, en Italia, xFarm[157], con una plataforma que recorre en segundos los datos que llegan de satélites, sensores de suelo etc., los convierte en consejos diarios que llegan a más de 200.000 agricultores en toda Europa[158].

En un mundo como en el de la agroalimentación, la automatización y las tecnologías de la información son esenciales para incrementar la productividad, mejorar la calidad e incluso alcanzar una mayor eficiencia en la industria alimentaria, e incluso destacan algunos autores que la principal justificación para adoptar la automatización radica en la mejora de los productos[159]. Gracias al uso de estas tecnologías se consigue la reducción de tiempos improductivos en las líneas de producción, menor tiempos de preparación, entregas más rápidas, reducción de costes, mayor flexibilidad de producción y mayor productividad[160].

Respecto a sectores concretos, la automatización reduce el consumo de energía y optimiza procesos en industrias azucareras, mejorando la eficiencia en la pre-molienda. En la industria pesquera la automatización ha demostrado mejoras significativas en la velocidad de procesamiento y rendimiento.

1. Importancia del uso de sistemas de inteligencia artificial en agroalimentación

La agricultura ha experimentado un gran cambio en los últimos años, impulsado por los avances tecnológicos que buscan optimizar la producción y promover la sostenibilidad. La IA se ha convertido en una herramienta crucial que es capaz de abordar desafíos complejos como son el cambio climático, la escasez de recursos, y el aumento de la

[155] En este sentido, es de especial relevancia el estudio realizado por AZTI, referente a la tecnología utilizada para una pesca sostenible. Fuente: https://www.azti.es/productos/memoria-tecnologia-para-una-pesca-sostenible/. Última fecha de consulta: 3 de octubre de 2025.
[156] QUEMADA, M., GABRIEL, J.L., Impacto de los fertilizantes y la energía en la producción de alimentos, 2023. Acceso al documento: https://www.upa.es/Anuario2023/020-Anuario-2023-Quemada-Gabriel.pdf.
[157] La empresa xFarm Tecnologies, que es una plataforma que integra datos satélites y sensores, con presencia en Europa. Fuente: XFarm. Consultado en: https://xfarm.ag/es/empresa. Última fecha de consulta: 3 de octubre de 2025.
[158] LARRAZABAL, M., El impacto de la Inteligencia Artificial en la Agricultura: Potencia y oportunidades (I), *Agricultura Digital*, pág. 72.
[159] DAMIÁN MORAN G.J., et. al., "Industria 4.0 y su relación con la automatización en la industria Alimentaria: una revisión sistemática y bibliométrica", *Manglar,* núm. 22, vol. 2, 2025, pág. 230. Doi: http://doi.org/10.57188/manglar.2025.025
[160] Ídem.

demanda de alimentos a nivel mundial. En este sentido se ha procurado la optimización de aspectos cruciales como la gestión del riego, el manejo de plagas y la preservación del suelo, mejorando la productividad y promoviendo prácticas que son fundamentales para la sostenibilidad agrícola. Para ello, utiliza una tecnología de información a través de la cual recopila todos los datos necesarios, los analizada, y toma decisiones basadas en información detallada y específica sobre las condiciones del suelo, cultivos, clima y recursos hídricos con la intención de adecuar el cuidado de los suelos y cultivos a la variabilidad presente[161].

Es preciso destacar que la IA para la agricultura se presenta en dos conceptos que parecen de forma diferenciadas en las investigaciones que se ha realizado sobre el tema: la agricultura de precisión y la agricultura inteligente. Ambas buscan optimizar el rendimiento agrícola mediante el uso de tecnología y datos, pero mientras que la agricultura de precisión está relacionada con el saber utilizar los recursos en el lugar y momento adecuados, la agricultura inteligente represente un paso más allá, pues es la que integra tecnologías emergentes como la IA, la robótica, etc.[162].

Gracias al uso de la IA en la agricultura inteligente es posible analizar grandes cantidades de datos rápidos, en los que se detectan signos de enfermedades específicas en los productos sembrados, o incluso en los nutrientes de la tierra. Gracias a estos avances se consiguen grandes soluciones para un correcto aprovechamiento en la utilización de pesticidas, así como una disminución considerable de los mismos. En este sentido, se han realizado varios estudios relacionados con la IA en agricultura, destacando: el estudio y desarrollo de soluciones mecanizadas automatizadas mediante la aplicación de sensores y nuevas tecnologías para la producción de cítricos, o la detección de enfermedades en cultivos de país mediante imágenes con visión artificial [163].

Dentro de las herramientas utilizadas encontramos sensores de humedad del suelo, drones para la aplicación de pesticidas y fertilizantes, sistemas de riego automatizados y software de gestión de datos agrícolas[164]. También se han utilizado drones para sobrevolar y analizar cultivos de patatas, de manera que la Universidad de Pamplona realizó un proyecto con el objetivo de detección temprana de problemas, para el cual se emplearon cámaras RGB y NIR (Near-Infrared)[165], de forma que se pudiesen obtener los respectivos ortofotomosaicos y así identificar zonas con mayor o menor actividad fotosintética. En

[161] MÉNDEZ-PALOS E. E., "La Inteligencia Artificial en la producción agrícola: estudio exploratorio", Red Internacional de Investigadores en Competitividad, XVIII Congreso, pág. 1947.
[162] Últ. ob. cit., pág. 1499.
[163] Últ. ob. cit., pág. 1500.
[164] HERNÁNDEZ-SALAZAR, C.A., GONZÁLEZ ESTRADA, O.A., GONZÁLEZ-SILVA, G., "Integración de la inteligencia artificial y la agricultura de precisión en cultivos de café", *Revista UIS Ingenierías,* núm. 23, vol. 4, 2024, pág.145. Doi: https://hal.science/hal-04815497v1
[165] Una cámara NIR es un dispositivo que detecta y procesa luz en el rango del infrarrojo cercano (NIR), típicamente entre 700 y 1000 nm. A diferencia de las cámaras visibles, estas cámaras son sensibles a la luz no visible y se utilizan en aplicaciones como la vigilancia, la astronomía, la industria de semiconductores, la agricultura y el control de calidad de alimentos, ya que pueden revelar detalles no detectables a simple vista. Fuente: Labiser. Consultado en: https://labiser.es/tecnica-nir/#:~:text=La%20espectroscop%C3%ADa%20NIR%20(Near%20Infrared,grasa%20o%20prote%C3%ADna%20sin%20reactivos. Última fecha de consulta: 25 de noviembre de 2025.

este proyecto se tuvieron en cuenta otras variables como área cubierta, duración de batería, resolución de fotografías, estabilidad, coste, impacto del ambiente, etc.[166].

2. Casos de uso

En primer lugar, en el sector cafetero, el uso de IA ha mostrado grandes beneficios. Para ello, se utilizan tecnologías como redes de sensores inalámbricos, computación en la nube, que permiten a los productores de café hacer frente a las variaciones climáticas y mejorar la calidad del producto. También destaca la visión por computadora, que permite el análisis de imágenes digitales para reconocer objetos, medir dimensiones, detectar anomalías o estimar variables de interés, lo que es fundamental para identificar anomalías nutricionales u otras deficiencias[167].

En segundo lugar, empresas como Covap también están haciendo uso de estos sistemas, afirmando públicamente que ya están utilizando la misma en sus procesos a través del análisis de datos, automatización de tareas, mejora de rendimientos y toma de decisiones. Este tipo de empresas familiares se atreven a dar el salto, pero reiteran que no quieren perder su identidad ni su esencia como agricultores[168]. El Grupo Operativo Celegand, liderado por COVAP (Cooperativa Ganadera del Valle de los Pedroches), junto con la participación de Cooperativas Agroalimentarias de Andalucía, entre otras, han presentado nuevas variades de trigo y triticale que han resultado ser más productivas que las utilizadas anteriormente[169]. En este sentido, también destaca Zoomagri, que destaca por su compromiso con la transformación digital de la agricultura. A través del uso de IA, logran desarrollar soluciones a lo largo de la cadena agroindustrial, desde los semilleros hasta los puertos e industrias[170].

En tercer lugar, respecto al sector pesquero, el centro tecnológico vasco Azti ha analizado las potenciales aplicaciones de las técnicas de IA, desde el procesamiento de muestras biológicas hasta la mejora de la eficiencia energética de los buques pesqueros[171].

En cuarto lugar, en el sector ovino, resulta reseñable Gradiant, que está utilizando la IA junto con la tecnología NIR (esta tecnología es una técnica analítica no destructiva que usa la luz infrarroja para medir la composición química de una muestra) para la monitorización del estado de la fertilidad de las ovejas. Este proyecto lo está ejecutando

---

[166] LEÓN-RODRÍGUEZ, M. E., et. al., "Drones en la agricultura", *Revista Ingeniería Solidaria*, núm. 2, vol. 19, 2023, pág. 6. Doi: https://doi.org/10.16925/2357-6014.2023.02.05.
[167] Últ. ob. cit., pág. 149.
[168] Fuente: Hoyaldía.com. Consultado en: https://www.hoyaldia.com/tag/covap/. Última fecha de consulta: 16 de septiembre de 2025.
[169] Fuente: Somos Futuro, núm. 59, julio-septiembre 2023, pág. 24. Consultado en: https://celegand.grupooperativo.es.
[170] Fuente: Revista Alimentaria, Servicios Start Up. Consultado en: https://revistaalimentaria.es/tag/start-up. Ultima fecha de consulta: 16 de septiembre de 2025.
[171] Fuente: Europapress. Consultado en: https://www.europapress.es/euskadi/noticia-azti-coordina-herramienta-promueve-desarrollo-sostenible-sectores-maritimos-conservacion-20250204110706.html. Ultima fecha de consulta: 16 de septiembre de 2025.

el equipo de Calidad y Seguridad Alimentaria 4.0 de CNTA y cuenta con financiación del Ministerio de Agricultura, Alimentación y Pesca (MAPA)[172].

Por último, destaca el "Proyecto Agraria: inteligencia artificial aplicada a la cadena de valor de la producción agraria 2050", relativo a la Convocatoria para la concesión de ayudas para financiar proyectos del "Programa Misiones de I+D en Inteligencia Artificial 2021"[173], que nace con el objetivo de investigar la aplicabilidad y viabilidad de la IA junto con otras tecnologías relacionadas con la industria 4.0 en soluciones reales para definir nuevos métodos de producción agraria que redunden en que el futuro del sector agroalimentario sea más tecnológico, innovador, sostenible y comprometido con la eficiencia energética y la disminución de la huella de carbono. De especial importancia también el Grupo de Investigación BISITE, de la Universidad de Salamanca, que lidera la aplicación de algoritmos de IA para potenciar el sector agrícola[174].

3. Desafíos aparentes

Pese a los innumerables beneficios del uso de la IA en la agricultura, también debemos destacar algunos de sus riesgos e inconvenientes. En primer lugar, la aplicación de la IA representa un cambio drástico en los procesos de producción de forma que se necesita una adaptación gradual a todas estas herramientas. De otro lado, destacan los altos costes iniciales, así como la necesidad de capacitación. En áreas rurales, con infraestructuras limitas, es preciso desarrollar políticas y estrategias que promueven una adopción fácil y segura de este tipo de sistemas[175]. Los consumidores pueden verse realmente afectados en relación con el precio que tengan que asumir, si no es posible la reducción a corto plazo de estos costes. Así como la posible presencia de la brecha digital y la necesidad de desarrollar políticas de capacitación.

4. Normativa

En cuanto la regulación aplicable a escala europea el Reglamento (UE) 2024/1689 (RIA) que, aunque es una normativa de carácter trasversal, establece obligaciones que podrían ser aplicables a sistemas de IA empleados en la agricultura (clasificación por riesgo, obligaciones de transparencia, evaluación de impacto, etc.). A escala autonómica existen libros blancos y estrategias de impulso sectorial (p. ej. CIDAI en Cataluña para la agroalimentación. Destaca los sand-box propuestos, el concepto de datos interoperables, así como la intención de colaboración público-privada)[176]. Lo que interesa ahora es traducir esas obligaciones generales a reglas sectoriales operativas (certificación, entornos de ensayo, repositorios de datos interoperables). Este Libro Blanco sobre la IA

[172] Fuente: CNTA. Consultado en: https://www.cnta.es/gestion-de-datos-e-inteligencia-artificial-oportunidad-para-el-desarrollo-del-sector-agroalimentario/. Ultima fecha de consulta: 16 de septiembre de 2025.
[173] Fuente: Portal Ayudas Digital. Consultado en: https://portalayudas.digital.gob.es/misiones-ia-2021/Paginas/Index.aspx. Última fecha de consulta: 3 de octubre de 2025.
[174] Fuente: Bisite. Consultado en: https://bisite.usal.es/es. Ultima fecha de consulta: 16 de septiembre de 2025.
[175] MÉNDEZ-PALOS E. E., ob. cit., pág. 1497.
[176] Fuente: Cidai. Consultado en: https://cidai.eu/es/eventos/presentacion-del-libro-blanco-sobre-la-inteligencia-artificial-aplicada-al-sector-agroalimentario/. Ultima fecha de consulta: 3 de octubre de 2025.

aplicada a la Agroalimentación surge con la intención de facilitar y acelerar la adopción de la UA en el ámbito de agroalimentación, convirtiéndose en un instrumento clave para el aumento de la eficiencia en los procesos productivos. Dentro del mismo se incluyen actuaciones para impulsar la aplicación de la IA, así como la disponibilidad y gobernanza de datos, la creación de entornos de pruebas, así como la necesidad de la colaboración público-privada. Destaca también el Reglamento 178/2002 sobre seguridad alimentaria[177].

4.1. Perspectiva comparada de la regulación de inteligencia artificial en agroalimentación

A nivel internacional, destaca también el uso de la IA en el sector agroalimentario. RootAI, por ejemplo, es una empresa de investigación con sede en EE. UU., que se encuentra desarrollando IA y robótica, para fortalecer el sector de la agricultura de interior que se encuentra operativa actualmente. O la startup Taranis, que tiene sede en Israel, que ha desarrollado un motor científico que analiza datos de campo relacionados con el ciclo de producción de cultivos y el clima e indica el momento y lugares más adecuados para usar agroquímicos. También destaca Connecterra, en Países Bajos, que utiliza IDA (*Itelligent Daity Farmers Assistant*), un servicio impulsado por inteligencia artificial que utiliza datos recopilados de vacas para detectar problemas de salud[178].

Pues bien, en materia regulatoria destacan, en primer lugar, los Países Bajos. En este sentido, cuentan con una estrategia nacional denominada *"Strategic Action Plan for Artificial Intelligence*"[179], que incluye prioridades en agricultura. La estrategia nacional apoya proyectos de IA para *smart farming*, gestión de datos en agricultura, sistemas autónomos agrícolas.

En segundo lugar, destaca Brasil, que cuenta con la Estrategia Brasileña de Inteligencia Artificial (EIBA)[180]. El principal objetivo de esta es orientar las acciones del Estado brasileño a favor del desarrollo de acciones, en sus diversas vertientes, que estimulen la investigación, la innovación y el desarrollo de soluciones en Inteligencia Artificial, así como su uso consciente, ético y a favor de un futuro mejor. La agricultura está incluida dentro de los ejes estratégicos. La estrategia podría favorecer tanto la adopción de IA como la creación de regulaciones específicas, o de soft law, para casos de uso agropecuario.

En tercer lugar, destacan otros países latinoamericanos, como Colombia o Costa Rica, que cuentan con políticas nacionales en materia de IA, tal y como se refleja del Informe

[177] Reglamento (CE) nº 178/2002 del Parlamento Europeo y del Consejo, de 28 de enero de 2002, por el que se establecen los principios y los requisitos generales de la legislación alimentaria, se crea la Autoridad Europea de Seguridad Alimentaria y se fijan procedimientos relativos a la seguridad alimentaria. DOCE núm. 31, de 1 de febrero de 2001.

[178] Consultado en: Informe de tecnologías emergentes y desarrollo de negocio. Sector agroalimentario global y europeo.

[179] Acceso al documento: https://wp.oecd.ai/app/uploads/2021/12/Netherlands_Strategic_Action_Plan_for_Artificial_Intelligence.pdf

[180] Consultado en: https://opsaa.iica.int/frame-3194.

de la CCIA (*Computer and Communications Industry Association*)[181]. Aunque no haya regulación específica en muchos de estos países, las políticas de IA nacionales pueden favorecer proyectos de IA agrícola (por ejemplo, en materia de datos rurales o agricultura digital). En este sentido, las estrategias nacionales podrían servir como marco para financiar, monitorear o regular proyectos de IA en agricultura, especialmente en temas de sostenibilidad y digitalización rural.

Por último, destaca China. Su enfoque respecto a la regulación de la IA es particular y exclusivo, puesto que se centra en la seguridad nacional, el desarrollo económico, así como la estabilidad social. En cuanto a estrategias, el Plan de Desarrollo de la IA de Nueva Generación[182] de este país fue una de las iniciativas pioneras en establecer el objetivo primordial de liderar el mundo en IA para 2030. En materia agroalimentaria, ha lanzado un plan quinquenal (2024-2028)[183] para "smart-farming", que busca impulsar la IA, el big data y la maquinaria agrícola digital. También destaca el etiquetado de contenido de IA (Measures for Labeling of AI-Generated Synthetic Content)[184]. Incluso las redes sociales chinas han incorporado una serie de etiquetas para identificar el contenido generado con IA[185], en aras a cumplir con la nueva ley nacional, denominada "Medidas para la identificación del contenido sintético generado por la IA", que entró en vigor el 1 de septiembre de 2025.

En conclusión, son muchas las estrategias nacionales que tienen puesto el foco en la IA, con diferentes proyectos ya impulsados, pero no se cuenta en el panorama internacional actualmente con normas vinculantes sectoriales. Además, si bien es cierto que las estrategias desarrolladas promueven diversas medidas que facilitan una mayor producción, menor tiempo, y con un gran coste de recursos, no todas las medidas se traducen efectivamente en un beneficio directo al consumidor. Es por esto por lo que se proponen las siguientes medidas autonómicas.

5. Solución autonómica

En primer lugar, sería recomendable desarrollar un Libro Blanco que recopile las reglas, estándares y directrices para un uso seguro de la IA en agroalimentación, que se ocupe de las principales deficiencias existentes en materia de responsabilidad, ética o seguridad. En este sentido, podrían traducirse las obligaciones generales que se encuentran en el AI Act a reglas operativas en materia de gobernanza de datos, evaluación de impacto o trazabilidad, en forma de guías autonómicas.

---

[181] Consultado en: https://ccianet.org/wp-content/uploads/2025/04/CCIA_Global-Round-Up-National-AI-Policies_Whitepaper.pdf

[182] En este sentido, véase en Informe de la CCIA recientemente citado.

[183] Fuente: Modern Diplomacy. Consultado en: https://moderndiplomacy.eu/2025/01/29/chinas-agricultural-priorities-in-2025/. Ultima fecha de consulta: 20 de noviembre de 2025.

[184] Entre otras, destaca la norma obligatoria GB 45438-2025, que define los métodos para identificar contenido sintético producido por IA

[185] Fuente: Europapress. Consultado en: https://www.europapress.es/portaltic/socialmedia/noticia-redes-sociales-chinas-incorporan-etiquetas-identificar-contenido-generado-ia-20250902120100.html#google_vignette. Ultima fecha de consulta: 25 de noviembre de 2025.

En segundo lugar, deberían establecer condiciones de licencias para proveedores de IA que operen en la región, como pueden ser certificados de cumplimiento ético, de transparencia, pruebas previas en entornos reales controlados, etc.

En tercer lugar, sería interesante promover espacios regionales de experimentación donde se testeen tecnologías de IA en agroalimentación, con medición de impactos reales, incluido una asesoría regulatoria.

En cuarto lugar, es preciso fomentar la creación de repositorios de datos agroalimentarios regionales, con estándares interoperables, que estén abiertos cuando sea posible, para garantizar la privacidad; así como asegurar la trazabilidad desde la producción.

Por último, es preciso que todo ello repercute grosso modo en un beneficio para los consumidores, ya sea en la reducción del precio o en el incremento de la calidad de la producción, puesto que no puede admitirse una mejora sustancial de todo el proceso productivo sin una mayor satisfacción del consumidor con el producto. En este sentido, sería interesante que se promoviese por parte de las autoridades estatales algún tipo de incentivo para las empresas que desarrollasen algunas de estas estrategias, siempre y cuando se repercuta en los derechos de los consumidores.

II. PUBLICIDAD SEGMENTADA Y MENORES

1. El origen de la publicidad segmentada

Actualmente se ha producido una segmentación de mercado, de forma que se ha dividido en grupos más compactos y homogéneos de clientes y consumidores, tendiendo en cuenta sus características o comportamientos similares. Pueden tenerse en cuenta diferentes criterios, como pueden ser variables de información demográfica, geográfica o conductual. Esta segmentación es posible a través de la información obtenida mediante el Big Data, que es lo que permite a los analistas identificar subdivisiones en tiempo real, favoreciendo a las estrategias de marketing y permitiendo una personalización amplia[186].

Esta segmentación del mercado también ha conllevado una segmentación de la publicidad, destacado plataformas como Meta Ads, Google Ads, TikTikAds, Amazon Marketing Cloud, que permiten llegar a los usuarios en el momento exacto en el que buscan productos específicos. También destaca el uso de Machine Learning que aplica modelos predictivos o redes neuronales para anticipar la probabilidad de compra y personalizar ofertad de forma automática. En este sentido, destaca el enfoque Dara-Driven, conocido como "viaje del cliente", que ha revolucionado la forma en que las empresas comprenden e influyen en el comportamiento del consumidor[187].

De esta forma, el rastro de datos que los usuarios han ido dejando al utilizar diversos sitios web y aplicaciones se ha ido aprovechando a lo largo del tiempo para perfeccionar las estrategias de marketing. Estos avances permiten una mayor precisión y personalización

[186] BALSECA-MEJÍA, C. J., "Big Data aplicada a la segmentación publicitaria (Meta Ads) y su impacto gerencial: caso Electrohogar", *Revista Sociedad & Tecnología*, núm. 8, 2025, pág. 383.
[187] Últ. ob. cit., pág. 385.

en la comunicación con los consumidores[188]. Muy interesante la percepción que tienen los consumidores de este tipo de publicidad, resultando cuatro tipo de consumidores: (i) *control paradox*, quienes son conscientes de los algoritmos y los consideran apropiados; (ii*) fatigued*, que también son conscientes de ellos, pero los encuentran inapropiados y se sienten incapaces de lidiar con ellos; (iii) *uniformed but critical,* que son más vulnerables debido a su falta de conocimiento y habilidades; y (iv) *skilled and critical,* que son conscientes y críticos de la persuasión algorítmica y tienen habilidades para manejarla. Los estudios destacan la necesidad de adaptación a cada grupo[189].

2. La publicidad dirigida a menores

Los menores podrían encontrarse dentro del tercer grupo de la clasificación mencionada anteriormente, pues son uno de los objetivos de la mayoría de los anuncios y, en la mayoría de las ocasiones, no son conscientes de ellos. Pese a que algunos autores consideren que la IA se puede convertir en una aliada en la supervisión de contenidos comerciales perjudiciales para menores en Internet, pues puede gestionar el gran volumen de datos que se genera actualmente, analizando y entendiendo cómo se comportar las personas y qué contenidos consumen en Internet[190], también pueden convertirse en su peor enemiga pues se utiliza para perfilar a los mismos e incluir en su opinión a través de las redes sociales, anuncios en televisión, etc.

Son varias las estrategias seguidas por las marcas para atraer la atención de los menores: (i) estrategia multicanal, a través de la cual alcanzar a los niños en diferentes plataformas simultáneas, como pueden ser la televisión, Youtube, sitios web, plataformas de streaming…; (ii) *branded content*, que ha ganado relevancia, al permitir que las marcas lleguen a los niños sin que perciban el contenido como un anuncio, como pueden ser vlogs con publicidad incluida; (iii) estrategias de influencers, que se ha convertido en una de las más poderosas, debido a la cercanía que sienten los niños con los creadores de contenido; (iv) *generated content,* que consiste en usar el contenido generado por los propios usuarios; (v) publicidad en plataformas de video online, etc. Respecto a su impacto en los últimos años, es cierto que tal y como afirman diversos estudios, en los últimos años se ha reforzado la protección de menores de 0 a 7 años para evitar mensajes engañosos y promocionar productos adecuados a su edad, y se han establecido directrices para identificar claramente la publicidad y evitar confusiones entre contenido comercial y entretenimiento[191]. Sin embargo, otros retos están todavía pendientes de solventarse, como la recopilación de datos personales de los menores, que no siempre se adecúa a lo establecido en el Reglamento General de Protección de Datos, o la globalización de las

[188] BLANCO SANGUINETI, R. G., CÁRDENAS CÓRDOVA, C. D., TORPOCO BALTAZAR, A., "La inteligencia artificial en la publicidad: una visión sistemática de la década 2020-2024", *Journal of the Academy*, núm. 11, 2024, pág. 74.
[189] Últ. ob. cit., pág. 75.
[190] RANGEL, C., "Inteligencia Artificial como aliada en la supervisión de contenidos comerciales perjudiciales para menores en Internet", *Revista Mediterránea de Comunicación,* núm. 13, vol. 1, pág. 18.
[191] STEFANOVA YORDANOVA, *Los niños conectados y la publicidad del siglo XXI: Un análisis de la evolución de las estrategias publicitarias dirigidas a los menores en España*, 2025, pág. 35.

plataformas digitales, que dificulta la aplicación de normativas nacionales, como la Ley General de Publicidad en España, que se analizará posteriormente.

3. Casos de uso

Un caso de uso especialmente relevante en la materia es el conocido como *"Meta Multistate Complaint"*. Esta demanda fue planteada por la mayoría de los Estados Unidos frente a Meta, acusando a la compañía de causar un daño mental a menores de edad, como consecuencia de prácticas manipulativas. Fueron más de 40 estados en EE. UU. Los que demandaron en octubre del 2023 a Meta por engaño público sobre los riesgos asociados al uso de las redes sociales y contribuir a una crisis de salud mental entre los jóvenes. La demanda describe varias técnicas basadas en el perfilado de usuario y la manipulación del tiempo en las plataformas de Meta, destacando las siguientes: algoritmos de recomendación personalizados, secuencias de recompensa variable, *feeds* basados en la vinculación o compromiso, *scrolling* infinito, contenido efímero, notificaciones audiovisuales y hápticas que impulsan un mayor compromiso con las plataformas y un contenido de vídeo de formato corto, como el *reel*[192]. En la demanda señala que entre 2009 y 2019 los distritos escolares vieron un aumento del 30 por ciento en el número de estudiantes que decían sentirse "tan tristes o desesperados casi todos los días que dejaron de hacer algunas actividades habituales". Y añade: "La mala conducta de los demandados ha sido un factor importante en desencadenar la actual crisis de salud mental, con porcentajes en aumento de depresión, trastornos alimentarios, soledad, pensamientos de autolesión e ideación suicida en menores de edad"[193].

Respecto a las infracciones cometidas, la parte demandante considera que se ha recopilado información personal de niños sin consentimiento parental verificable, que existe falta de notificación directa a los padres, así como falta de aviso adecuado en las plataformas sobre la información que se recopilaba de los niños, y conocimiento real de que menores de 13 años usaban la plataforma sin tomar las medidas precisas. En cuanto a la manipulación llevada a cabo a través de redes sociales, existen diferentes procedimientos: (i) la personalización a través de algoritmos, de forma que analizan grandes cantidades de datos de usuarios para ofrecer contenido personalizado y aumentar la participación; (ii) explotación de vulnerabilidades económicas, con campañas que recopilan información sobre el estado de ánimo y emociones, (iii) el "*framing*", o en cuadre, a través del cual se incluye en la dinámica social de la redes sociales y se refuerza la presión social al resaltar información específica en las noticias de usuarios, etc.[194]. Realmente, nos encontramos ante de numerosas prácticas como *scroll infinito, variable reward,* etc., que son patrones de *engagemen*t y que se utilizan habitualmente por los usuarios y no son ilegales *per se.* Ahora bien, lo que se alude en el presente caso es que

[192] MARTÍNEZ MARTÍNEZ, R., FERNÁNDEZ HERNÁNDEZ, C., "Publicidad digital y menores: una visión integrada de la Ley de Servicios Digitales y el Reglamento de Inteligencia Artificial (manipulaciones y conductas prohibidas, riesgos sistémicos en grandes modelos de lenguaje)", *LA LEY Derecho de familia*, núm. 44, octubre de 2024, Editorial LA LEY, pág. 4.

[193] Fuente: ABC. Consultado en: https://www.abc.es/xlsemanal/a-fondo/el-cerebro-de-los-ninos-y-el-movil-del-crimen-redes-salud-mental.html. Ultima fecha de consulta: 25 de noviembre de 2025.

[194] Últ. ob. cit., pág. 5.

los algoritmos proporcionan contenido personaliza para que los usuarios lo consuman hasta el agotamiento, lo que distorsiona la percepción del tiempo de los jóvenes.

4. Riesgos: los sesgos algorítmicos

Uno de los principales desafíos emergentes es la presencia de sesgos en los sistemas de IA, siendo recomendable para mitigar ese sesgo que las empresas implementen auditorías algorítmicas periódicas, diversifiquen sus fuentes de datos y promuevan la inclusión desde el diseño de sus modelos de segmentación. En segundo lugar, destaca la transparencia algorítmica y el consentimiento informado, pues son las empresas las que deben de comunicar de manera clara sus políticas de privacidad, explicando el propósito de la recolección de datos y garantizando que el consentimiento sea voluntario, específico y revocable[195]. Con el fin de garantizar que las experiencias publicitarias sean equitativas para todos los usuarios, la empresa Levi Strauss & Co se asoció con Lalaland.ai. Su estudio de moda digital que crea modelos personalizados generados por inteligencia artificial ha revolucionado el mundo de la moda al crear modelos personalizados generados por IA para aumentar la diversidad en su publicidad[196].

5. Normativa

A nivel autonómico, hemos de mencionar la Ley 10/2007, de 29 de marzo, de Medios Audiovisuales de Castilla-La Mancha[197], en la que se destaca la necesidad de adoptar las medidas necesarias para garantizar la protección de las y los menores ante los contenidos emitidos en los respectivos canales. En España, las prácticas publicitarias se rigen por la Ley General de Publicidad[198]. Entre el diverso articulado, es preciso mencionar el artículo 3, en el que se considera publicidad ilícita "la publicidad que atente contra la dignidad de la persona", y merece especial atención que se refiere especialmente al artículo 20, apartado 4 (entre otros), referente a la protección de la juventud y la infancia. En este mismo artículo indica que se considera ilícita la publicidad "dirigida a menores que les incite a la compra de un bien o servicio, explotando su inexperiencia o credulidad". De otro lado, muy interesante también lo recogido en la Ley de Competencia Desleal[199], que en su artículo 5 considera engañosas las omisiones que supongan la "ocultación de la información necesaria para que el destinatario adopte o pueda adoptar una decisión relativa a su comportamiento económico con el debido conocimiento de causa".

A nivel europeo, en primer lugar, es preciso aclarar que el DSA prohíbe la publicidad basada en el perfilado digital dirigido a menores por VLOP (así establecidos en el artículo 28), y que hay una serie de obligaciones de sistemas de verificación en relación con su edad.

Además, puesto que en estos casos se hace uso de sistemas de IA, hemos de atender a lo recogido en el AI Act. Recordemos que, entre las prácticas prohibidas, se encuentran

[195] BALSECA-MEJÍA, C. J., ob. cit., pág. 389.
[196] TORIBIO, O., "Irrupción e impacto de la inteligencia artificial (IA) en la publicidad", *Revista INARTES*, núm. 1, vol. 1., junio-noviembre de 2024, pág. 8.
[197] DOCM núm. 82, de 19 de abril de 2007.
[198] Ley 34/1988, de 11 de noviembre, General de Publicidad. BOE núm. 274, de 15 de noviembre de 1988.
[199] Ley 3/1991, de 10 de enero, de Competencia Desleal. BOE núm. 10, de 11 de enero de 1991.

aquellas destinadas a manipular y perjudicar a individuos o grupos, prestando especial atención a las personas vulnerables. En el artículo 5 apartado 1 se prohíbe lo siguiente: "la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas (…)". Es preciso centrar el enfoque es ese "perjuicio sustancial"[200] (en relación con el artículo 5 RIA). Por tanto, tal y como afirma la doctrina[201], este apartado se vincula con dos tipos de prácticas publicitarias ilícitas: la subliminal y la engañosa. Ahora bien, debe destacarse que en la ley de publicidad no exige que se haya producido un perjuicio ni que se haya producido intercambio comercial alguno para que se de esa ilicitud, mientras que la regulación del AI Act requiere que se altere la capacidad de toma de decisiones y además que sea potencialmente causante de algún tipo de perjuicio considerable[202].

Sea como fuere, deben respetarse las obligaciones establecidas en el AI Act, como la del artículo 50, en la que se indica el deber de informar a los usuarios, especialmente consumidores, cuando estén interactuando con sistemas de IA que está generando contenidos, respondiendo a preguntas o tomando decisiones. Cuando se trate de sistemas de IA generativa, es necesario marcar sus contenidos, en especial las ultrafalsificaciones o *deepfakes*. De otro lado, cuando los responsables del despliegue sean administraciones públicas, se deberán registrar los sistemas de IA que estén utilizando en la base de datos europea y realizar una evaluación de impacto cuando afecten a servicios esenciales. Muy reseñable será el papel de la Agencia de Supervisión de la Inteligencia Artificial, (AESIA) que será la encargada de controlar la utilización de sistemas de IA en España.

5.1. Perspectiva comparada de la regulación de inteligencia artificial en publicidad segmentada y menores

A nivel internacional, se cuenta con diversos pronunciamientos legislativos, así como recomendaciones respecto a esta materia. En primer lugar, en Reino Unido la ICO (Information Commissioner's Office) ha publicado guías sobre IA y protección de datos[203] en aras a asegurar la equidad y transparencia en sistemas automatizados. En este sentido, en muchos casos el uso de IA para segmentar publicidad entra en los límites de "perfilado", y requiere evaluaciones de impacto de privacidad. Además, es interesante destacar que se cuenta con un Código de Publicidad[204], que se sigue aplicando, aunque la segmentación del anuncio se haya generado por IA. No hay una regla que obligue a

[200] En este sentido, es preciso hacer alguna comparación con lo establecido en la LCD, pues mientras que en esta normativa no se requiere daño, en el AI Act nos habla del requisito de "alteración sustancial y perjuicio considerable").

[201] VEGA GARCÍA, P., "Efectos de la regulación europea sobre inteligencia artificial en el control de la publicidad ilícita", *Revista E-Mercatoria,* vol. 2. 23-11, junio-diciembre 2024, pág. 218.

[202] En este sentido, véase últ. ob. cit., pág. 219.

[203] Fuente: Página web AEPD. Consultado en: https://www.aepd.es/prensa-y-comunicacion/blog/abordando-conceptos-erroneos-de-la-inteligencia-artificial. Ultima fecha de consulta: 20 de noviembre de 2025.

[204] Acceso al documento: https://www.asa.org.uk/static/8bb5edb9-99b6-4e29-b1c30cbfd2d9886e/9b4a8d2d-7d8b-440b-a25deb04c9e58ed3/The-CAP-Code-Introduction.pdf

revelar que un determinado anuncio se ha hecho con IA, pero se recomienda transparencia cuando el uso de esta pueda confundir a los consumidores.

En cuanto a China, ha aprobado reglas de etiquetado obligatorio para contenido generado por IA, conocidas como "Measures for Labeling of AI-Generated Synthetic Content". Es un sistema de doble pista, puesto que requiere etiquetas visibles para los usuarios, que sean "explícitas", y también marcas ocultas (conocidas como "metadatos"), que identifiquen el contenido generado por IA para la rastreabilidad. Es obligación de la plataforma asegurar de que los usuarios no pueden eliminar estas etiquetas, debiendo los creadores indicar cuándo el contenido es creado por IA[205].

Por último, destaca Estados Unidos, que no cuenta con una ley federal integral que regule de forma específica la IA en la publicidad segmentada, pero ha avanzado en materia estatal. Por ejemplo, en nueva York destaca la ley "*Algorithmic Pricing Disclosure Act*"[206], que obliga a mostrar un aviso claro si el precio ofrecido se ha calculado por un algoritmo que usa datos personales. De otro lado, destaca iniciativas como *AdChoices*[207], que permiten a los usuarios saber cuándo se está usando "interest-based advertising" (publicidad basada en intereses) y da la opción de salirse de la página. También se cuentan con guías, elaboradas por la Comisión Federal de Comercio (*The Federal Trade Commission*, FTC), sobre cómo las empresas deben representar el uso de la IA, sobre todo cuando utilizan la personalización en la publicidad[208].

6. Solución autonómica

En primer lugar, que se promueva la formación y sensibilización de los agentes, de forma que anunciantes, agencias, plataformas digitales, etc. sean conocedores de los riesgos de la publicidad segmentada y la diversa regulación que existe a nivel nacional y europeo.

En segundo lugar, que se colabore con las autoridades competentes como la AESIA o la AEPD (Agencia Española de Protección de Datos) en aras al cumplimiento normativo.

En tercer lugar, que exista vigilancia por parte de los organismos autonómicos del cumplimiento de la normativa y que se contemplen sanciones para caso de incumplimiento en caso de que otra normativa de mayor rango no las prevea.

---

[205] Nuevas normas de etiquetado de contenido de IA en China: ¿Qué son y cómo se comparan con la Ley de IA de la UE?, *Bird&Bird*, 20 de mayo de 2025.

[206] Pese a que haya suscitado algo de controversia, se ha confirmado la constitucionalidad de esta Ley de Divulgación de Precios Algorítmicos. En este sentido, véase https://www.troutmanprivacy.com/2025/10/new-york-algorithmic-pricing-disclosure-act-upheld-as-constitutional/. Última fecha de consulta: 20 de noviembre de 2025.

[207] Es un programa de autorregulación de la *Digital Advertising Alliance* (DAA) para la publicidad dirigida en línea en Estados Unidos. Ofrece a los consumidores control sobre cómo se utilizan sus datos para mostrar sus anuncios basados en sus intereses, y permite activar o desactivar la publicidad dirigida. Véase: https://youradchoices.com/?language=es, última fecha de consulta: 20 de noviembre de 2025.

[208] Fuente: FTC. Consultado en: https://www.ftc.gov/es/business-guidance/resources. Última fecha de consulta: 20 de noviembre de 2025.

III. SALUD DIGITAL Y APPS MÉDICAS

1. La inteligencia artificial en sanidad

No podemos obviar que, en muchos lugares del mundo, la IA está cambiando de forma gradual la manera en que se presta la atención sanitaria. En este sentido, existen cuatro sectores en los que su uso está siendo predominante: (i) la gestión de servicios sanitarios, que incluye el apoyo a la gestión integral de los centros sanitarios, la coordinación de herramientas de información para pacientes, etc.; (ii) la medicina predictiva, que entre sus objetivos destaca respaldar los resultados de diagnóstico, tratamiento y predicción que se producen en muchas situaciones médicas; (iii) la toma de decisiones, que persiguen ayudar a médicos y gestores en la toma de decisiones clínicas en una gran variedad de funcionales específicas; (iv) los datos del paciente y diagnóstico, que permite recolectar una gran cantidad de datos de diferentes fuentes, permitiendo gestionar datos generador a partir de actividades clínicas como la detección, el diagnóstico y la asignación de tratamientos[209].

Tal y como explican los criterios de Eggers et al.[210], existen cuatro enfoques principales para la automatización de la IA a los clínicos: aliviar, separar, reemplazar y aumentar. La IA permite aliviar la carga de trabajo en las disciplinas como el diagnóstico por la imagen, los algoritmos también pueden emplearse para reducir los ingresos hospitalarios evitando los innecesarios antes de que ocurran, algunas de las tareas de los profesionales sanitarios podrían ser desempañadas directamente por la IA (aunque sea éticamente cuestionable), y gracias al uso de la tecnología se podría reducir el número de errores humanos, así como la sobrecarga de trabajo y el estrés.

En este sentido, algunos estudios concluyen que la IA pueden mejorar la prestación de servicios sanitarios, y reflejan impactos financieros positivos, mostrando la posible reducción de costes en escenarios específicos. También se ha advertido que puede tener un impacto social positivo, al mejorar la calidad, la eficiencia y la accesibilidad de los servicios de salud, contribuyendo al aumento de la esperanza y calidad de vida de las personas[211].

2. El concepto de salud digital

El término *e-Health* hace referencia al uso de las TIC en el área de la salud, con el fin de optimizar la atención médica. La salud digital está formada por siete modalidades: (i) telemedicina, a través de atención remota; (ii) automatización de procesos y servicios, mediante la digitalización de recursos; (iii) *mHealth,* que son las aplicaciones móviles sobre las que incidiremos posteriormente; (iv) *wearables,* que son dispositivos y/o accesorios electrónicos; (v) realidad virtual, mediante la realización de simulaciones de

[209] DIÍEZ, J., Aplicaciones médico-sanitarias de la inteligencia artificial: una visión desde la práctica clínica, *Anales de la Real Academia de Doctores de España*, vol. 8, núm. 4, 2023, págs. 884-885.
[210] EGGERS WD, SCHATSKY D, VIECHNICKI P. *AI-augmented government: Using cognitive technologies to redesign public sector work A report from the Deloitte Center for Government Insights*, 2017, citado en DÍEZ, J., ob. cit., pág. 885.
[211] ESTRELLA PÉREZ, P., ESCOBEDO, N., "La inteligencia artificial en el sector salud: aplicaciones e impacto", *Revista Informática + Salud,* Especial Inteligencia Artificial Generativa, febrero 2024, pág. 23.

intervención; (vi) realidad aumentada, a través de operaciones en remoto; y (vii) *big data* e IA, en relación con las gran cantidad de datos utilizados y el uso de técnicas avanzadas para alcanzar una mejor calidad en los sistemas de salud[212].

Destaca la doctrina que uno de los principales beneficios de la *e-Health* es la comodidad, habiéndose dado cuenta de ello un grupo de investigadores de Filadelfia, quienes utilizaron la telesalud para el control de pacientes oncológicos durante la pandemia por COVID-19. Indican que los pacientes están más cómodos, tienen sus necesidades emocionales satisfechas, no se realizan viajes innecesarios, e incluso ahorran tiempo. También consideran que facilita la toma de decisiones del equipo de salud, reduce el estrés e incluso se percibe una aptitud positiva por parte de los pacientes, que se muestran permisivos con el uso de estas tecnologías[213]. En atención primaria en España, la salud digital se ha tradujo en consultas eficiencias, sin tantas aglomeraciones y listas de espera, disminuyendo la carga de trabajo, la reducción de costes y limitando las consultan presenciales a las que fuesen estrictamente necesarias. En salud mental favorece la relación terapéutica y facilita el acceso a pacientes con problemas, y se convierte en un trabajo más flexible e incluso más beneficioso para pacientes con ansiedad social, o con diversas dificultades como movilidad limitada, estigma social o que viven en hogares situados en lugares remotos[214].

3. Aplicaciones médicas: casos de uso

El uso de aplicaciones móviles con finalidades en salud se puede traducir en grandes beneficios para múltiples usuarios, pues facilitan un reporte casi automático de nuestro estado de salud. Además, acerca la atención médica a zonas remotas, facilitando la comunicación y ofreciendo una atención inicial en lugar con limitada cobertura asistencial, garantizando la continuidad y calidad asistencial. En cuanto a la salud mental, se muestra como un recurso prometedor especialmente entre los más jóvenes[215].

Hay todo tipo de aplicaciones, desde las que ofrecen terapias de conversación y técnicas de relajación que ayudan a maneras el estrés, la ansiedad y mejorar el estado de ánimo; hasta las que pueden ofrecer planes de alimentación personalizados, programas de ejercicios y seguimiento del sueño, que se adaptan a las necesidades y preferencias del usuario y ofrecen recomendaciones basadas en datos objetivos[216]. En cuanto a ejemplos de estas aplicaciones mencionamos los siguientes. La compañía *HealthBlock* ha lanzado una aplicación basada en la tecnología de cadena de bloques que ayuda a los usuarios a

[212] ARIAS, A. C. et al., "Sistematización teórica de salud digital", *Revista Científica Sapientiae*, vol. 8, núm. 16, enero-junio 2025, pág. 129.
[213] HUAIQUIÁN SILVA, J., ESPINOZA VENEGAS, M., RÍOS BOLAÑOS, M., "Salud digital en el control de pacientes crónicos durante la pandemia: la mirada del equipo de salud", *Revista Ciencia y Enfermería,* 2022, pág. 8.
[214] Últ. ob. cit., pág. 9.
[215] PANADÉS ZAFRA, R. et al., "Análisis de retos y dilemas que deberá afrontar la bioética del siglo XXI, en la era de la salud digital", *Atención Primaria*, núm. 56, 2024, pág. 3.
[216] SERRANO ACITORES, A., "El impacto de la inteligencia artificial en el sector sanitario: retos éticos y legales", *LA LEY mercantil,* núm. 120, enero de 2025, Editorial LA LEY, pág. 9.

mantenerse activos y sanos[217]. También podemos mencionar *SleepTime*, para proporcionar sueños de calidad a los usuarios; *LumoRun*, que monitorizan los parámetros biométricos cuando se realiza ejercicio físico; *iConnecta*, que ha sido desarrollada por el Instituto de Oncología de Cataluña, promoviendo un método escalonado de atención psicosanitaria del cáncer de mama; o *Social Diabetes*, para gestionar la diabetes de forma sencilla sin tener que revisar los parámetros constantemente, entre otras.

Respecto a este último tipo, destacó el uso de la aplicación móvil *OneTouch Reveal*, pero no de forma positiva, pues se pudo comprobar que dicha aplicación había estado proporcionando instrucciones incorrectas sobre la cantidad de insulina que se debía proporcionar. Fueron los dos riesgos jurídicos aparentes: (i) la seguridad y la calidad de las apps sanitarias (con la necesidad de que se certifiquen como producto sanitario) y (ii) la responsabilidad por recomendaciones clínicas automatizadas Tal fue la gravedad, que la AEMPS emitió una alerta informativa[218] para advertir a los usuarios sobre la posibilidad de que la aplicación proporcionase recomendaciones de dosis de insulinas inadecuadas[219]. De esta manera, pese a que estas herramientas puedan resultar de gran utilidad, también conllevan diversos riesgos.

En cuanto a la posible responsabilidad derivada de este tipo de aplicaciones sanitarias, ha habido una variedad de pronunciamientos en cuanto a si es posible o no el reconocimiento de responsabilidad a los desarrolladores de estas aplicaciones, cuando los consejos que se dan pueden ser realmente dañinos para la persona afectada.

En primer lugar, hemos de analizar si pueden considerarse estas aplicaciones como productos sanitarios. La doctrina entiende que es fundamental comprender que la calificación de programa informático, bien como producto sanitario o como accesoria, es independiente de la ubicación del programa informático y del tipo de interconexión entre el programa informático y el producto. Sí que se trata de un matiz importante en referencia al uso específico que se hace del programa informático, ya que es ese uso el que determinará que un determinado dispositivo sea considerado o no como producto sanitario, lo que puede resultar complejo[220]. En este sentido, resulta de especial importancia las guías publicadas por la Unión Europea para facilitar a los desarrolladores y a las agencias reguladoras la clasificación de productos sanitarios en general, y de este tipo de tecnologías en particular[221]. Para poder avanzar en cuanto a la consideración de estas aplicaciones como un producto sanitario, diversos autores entienden que cuando una

---

[217] HULSEN, T., "Aplicaciones del metaverso en medicina y atención sanitaria", *Adv Lab Med,* vol. 5, núm. 2, pág. 168.

[218] Fuente: Página del Gobierno Español. Consultado en. https://www.aemps.gob.es/informa/informacion-sobre-la-posibilidad-de-obtener-recomendaciones-de-dosis-de-insulina-incorrectas-al-utilizar-la-funcion-mentor-de-insulina-de-la-aplicacion-movil-onetouchreveal/?lang=gl. Última fecha de consulta: 3 de octubre de 2025. Referencia: 28/2022, publicada el 8 de agosto de 2022.

[219] En este sentido, véase ZABALLOS ZURILLA, M. Responsabilidad, *mHealth* y productos defectuosos en la asistencia sanitaria: cuestiones clásicas y "futuras", en BELLO JANEIRO, D. (coord.), *Los nuevos tiempos del Derecho Sanitario: profesionales y pacientes como protagonistas*, ed. Reus, 2023 págs. 176-177.

[220] Últ. ob. cit., pág. 157.

[221] Guidance on Qualification and Classification of medical devices, October 2021.

aplicación esté destinada a alguno de los fines previsto en el Reglamento de Productos Sanitarios[222] será considerada como producto sanitario. Atendiendo a los riesgos potenciales que puedan derivarse de su utilización, se le asignará a una categoría entre I, IIa, IIb y III, de mayor a menor riesgos[223].

En segundo lugar, hemos de estudiar si pueden tratase como productos defectuosos. Si bien es cierto que se ha reiterado en múltiples ocasiones que la información proporcionada por este tipo de herramientas no convierte en defectuosa a la aplicación de forma automática, parece que con las aplicaciones de salud ocurre algo diferente. La doctrina no mantiene una posición unánime respecto al carácter de la información de salida, y de si entra en el ámbito de aplicación de la Directiva en materia de productos defectuosos[224], o no. Es una cuestión controvertida, pero se ha planteado que en este caso la aplicación proporciona una información que no tiene carácter genérico, sino que está vinculada directamente con cuestiones médicas, por lo que entiende que podría generar una expectativa razonable en el usuario de que la información será fiable y precisa, "aumentado la conexión entre la información errónea con el daño"[225]. Otra parte de la doctrina entiende que estaríamos hablando de un *software no integrado.* Si una aplicación determinada causa un daño, habría que resolver si ello convierte al teléfono en defectuoso. En virtud del principio de elementos intrínsecos mencionado anteriormente, algunos autores entiendan que la respuesta debería ser negativa. La razón se basa en que dichas aplicaciones no se refieren ni al uso ni a la presentación del producto en el que se instalan, de manera que no le proporcionan funcionalidad alguna[226]. Sin embargo, actualmente con la aprobación de la Directiva 2024/2853 tal y como se indica en el expositivo 13 de la misma, el software se considera un producto a los efectos de la aplicación del régimen de responsabilidad objetiva[227].

---

[222] Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n. 178/2002 y el Reglamento (CE) n. o 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo. DOUE, 5 de mayo de 2017.

[223] ZABALLOS ZURRILLA, M., ob. cit., pág. 159.

[224] Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. DOUE, núm. 2853, de 18 de noviembre de 2024.

[225] MARTÍN FABA, J.M., "La inteligencia artificial", cit., pp. 17-18.

[226] GARCÍA-MICÓ, T.G., *Robótica quirúrgica y derecho de daños*, ed. Marcial Pons, Madrid, 2024, pág. 79.

[227] "*Los productos en la era digital pueden ser tangibles o intangibles. Los programas informáticos, como los sistemas operativos, las microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. Los programas informáticos pueden introducirse en el mercado como productos autónomos o, posteriormente, pueden integrarse en otros productos como componentes, y pueden causar daños al ejecutarse. En aras de la seguridad jurídica, debe aclararse en esta Directiva que los programas informáticos son un producto a efectos de la aplicación de la responsabilidad objetiva, independientemente de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo, se accede a él a través de una red de comunicaciones o tecnologías en la nube o se suministra a través de un modelo de programa informático como servicio. Sin embargo, la información no debe considerarse un producto, por lo que las normas sobre responsabilidad por productos defectuosos no deben aplicarse al contenido de los archivos digitales, como*

4. Riesgos e inconvenientes

En primer lugar, como con todos los sistemas de IA, nos encontramos ante sistemas poco transparentes, de forma que cuando ofrecen un resultado determinado, es poco probable obtener la trazabilidad de todo el proceso. En segundo lugar, en caso de errores, como el que hemos comentado antes, puede ser realmente difícil determinar quién es el responsable de este, si el desarrollador del algoritmo, el proveedor del servicio, etc.[228]. En tercer lugar, despierta cierta preocupación la protección de los datos, pues estos sistemas precisan alimentarse de multitud de ellos, y en este caso son datos de carácter sensible, que pueden poner el riesgo la privacidad de los pacientes. En quinto lugar, preocupa una falta de alienación con la realidad, de manera que los algoritmos se entrenen con datos no representativos de la población en general, de forma que sean incompletos o que sean diseñados de manera incorrecta. Este problema se puede dividir en cuatro categorías: relevancia y contexto, errores de registro; diversidad en los estándares y errores de preparación de datos[229]. También destacan dos situaciones producidas: el *overfitting* o sobreajuste, que se produce cuando el algoritmo utiliza demasiadas variables en el conjunto de datos de entrenamiento y predice relaciones inadecuados y resultados inseguros; o el *data leakage*, o fuga de datos, que es otro problema relacionado con el desarrollo tecnológico[230]. Por último, también destacan las desventajas referentes a la implementación clínica de la tecnología, puesto que existen dudas sobre la calidad de las investigaciones y la forma de integrar los métodos de IA en el flujo de trabajo médico[231].

los archivos multimedia o los libros electrónicos o el mero código fuente de los programas informáticos. Un desarrollador o productor de programas informáticos, incluidos los proveedores de sistemas de IA en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo (5), debe ser tratado como un fabricante.

[228] En este sentido, la doctrina ha advertido que podríamos encontrarnos ante un producto sanitario, siempre y cuando cumpla las funciones que se encuentran recogidas en el Reglamento de Productos Sanitarios para considerarlos como tal. Algo diferente es cuando nos entremos ante una aplicación médica, de forma que lo único que debe considerar defectuosa es la información. Esto es algo más controvertido. La información podrá convertir al producto final que constituye su soporte en defectuoso si, en aplicación del principio de los elementos intrínsecos, se puede considerar que esta se refiere al uso o a la presentación del bien, y si provee al último de funcionalidad. Incluso algunos autores consideran que se podría defender también su consideración como producto (no como servicio) si estuviese integrado en el hardware. En este sentido, véase: GARCÍA-MICÓ, T.G., Robótica Quirúrgica y derecho de daños, ed. Marcial Pons, Madrid, 2024. Destaca también la prueba, de forma que principal problema es que encontramos con sistemas de baja trazabilidad o "black box". Se incluyen en la misma mecanismos de facilidad probatoria, puesto que se incluye tanto una exoneración de la defectuosidad del producto, como del nexo causal, por lo que se introduce una inversión parcial de la carga probatoria (atendiendo a una serie de requisitos). De otro lado, sigue siendo aplicable la exoneración por riesgos del desarrollo, que puede convertirse en un obstáculo a la hora de resarcir a las víctimas.

[229] REDONDO, M., ALONSO SUERO, E., La inteligencia artificia como herramienta para mejorar la salud pública: desafíos éticos y legales, *Revista Informática + Salud,* Especial Inteligencia Artificial Generativa, febrero 2024, pág. 31

[230] DIÍEZ, J., ob. cit., pág. 887.

[231] Últ. ob. cit., pág. 888.

4. Normativa

En primer lugar, a nivel europeo, es reseñable el Reglamento 2025/327[232] (conocido como REEDS), que surge con la intención de proporcionar las salvaguardias suficientes para garantizar un nivel elevado de protección, seguridad, confidencialidad y uso ético de los datos de salud. Es preciso alinear esta normativa con el Anteproyecto de Ley de Salud Digital[233]. Respecto a las aplicaciones de bienestar, que han sido referidas anteriormente, en su Considerando número 49 indica que los usuarios de estas deben ser informados de la capacidad de dichas aplicaciones para conectar y suministrar datos a los sistemas HCE[234].

A nivel nacional, destaca la LOPDGDD, ya mencionada, en cuyos artículos se especifica cómo deben tratarse los datos de salud, siendo obligaciones generales del responsable y encargado del tratamiento. En este sentido, destaca también la Carta de Derechos Digitales, que incluye "el derecho a la protección de la salud en el entorno digital", incluyendo el acceso seguro a servicios digitales, confidencialidad, derecho a la no discriminación, ética en la IA etc. Hemos de destacar que en España no existe una Ley Estatal que regule de forma global la salud digital, pero sí contamos con instrumentos que promueven la transformación del Sistema Nacional de Salud de España. En este sentido, destaca la Estrategia de Salud Digital, vigente de 2021 a 2026, que busca modernizar la salud pública a través de tecnologías digitales. Dentro de sus objetivos, se encuentra los siguientes: capacitar a las personas en el cuidado de su salud, optimizar el sistema sanitario y gestionar los datos de salud de forma ineficaz e interoperable, mejorando de esta manera la atención prestada al ciudadano. Además, se incluye dentro de los objetivos fortalecer la interoperabilidad, lograr un alineamiento a futuro con el Espacio Europeo de Datos de Salud, estudiado anteriormente.

De otro lado, destaca el Proyecto de Ley de Salud Digital, de forma que el Ministerio de Sanidad ha abierto una consulta pública para esta futura ley[235], que pretende regular la historia clínica digital interoperable, tanto a nivel nacional como europeo, que pueda adaptarse al REEDS. Además, abordará el uso de la IA, la biometría y otro tipo de

---

[232] Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847. DOUE, núm. 1689, de 12 de julio de 2024. Fecha de entrada en vigor: 25 de marzo de 2025.

[233] Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

[234] Sistema de Historia Clínica Electrónica, que es un repositorio digital y unificado que contiene toda la información médica y de salud de un paciente, como su historial médico, diagnósticos, medicamentos, resultados de laboratorio e imágenes

[235] Consulta Pública previa sobre el Anteproyecto de Ley de Salud Digital por el que se adapta al ordenamiento nacional el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/284 y se regula la historia clínica digital interoperable nacional y el uso de tecnologías digitales en la asistencia sanitaria.

tecnologías en salud, incluyendo las garantías específicas para pacientes y profesionales. El objetivo principal es estructurar un modelo de gobernanza para el uso primario de los datos de salud (atención sanitaria) y para el uso secundario (investigación, salud pública).

A nivel autonómico, destaca el Libro Blanco sobre la Inteligencia Artificial aplicada a la salud[236]: la IA para dar respuesta a los retos del sector de la Salud en Cataluña, que incluye una serie de recomendaciones para fomentar la adopción de la IA en el ecosistema de salud en Cataluña, entre las que se encuentran la creación de entornos de pruebas, facilitar la innovación público-privada, combatir la resistencia al cambio en las organizaciones, entre otras. Dentro de las diferentes cuestiones que se analizan en el mismo, destaca el apartado 5.4.6., donde se manifiesta la falta de transparencia y la gran dificultad con la que nos encontramos para garantizar el comportamiento ético de los modelos de IA y la seguridad legal para la práctica clínica. En este sentido, destaca que la gran complejidad, característica común de los sistemas de IA, se traduce en una falta de confianza en el resultado, unida a la presencia de posibles sesgos poco éticos. También destaca que el marcado CE no es suficiente para dar solución a este tipo de inconvenientes, puesto sólo garantiza que la herramienta funciona para un determinado propósito, pero realmente ese marcado no entra a validad si las prestaciones se están realizando con la suficiente calidad. Como último punto a destacar, realiza especial hincapié en la formación de los profesionales que, durante el desarrollo de su profesión, hagan uso de este tipo de sistemas. De esta forma, la carencia de un número suficiente de profesionales que conozcan cómo trabajar con equipos dotados de inteligencia artificial influirá de forma negativa en la capacidad de garantizar a medio plazo la incorporación de la IA en las organizaciones de salud.

También destaca el Anteproyecto de ley presentado por Cantabria para regular la salud digital a nivel autonómico. Es un texto realmente innovador, que aborda neurotecnologías, derechos digitales, teleasistencia, y aporta cierta seguridad jurídica a los profesionales sanitarios. Destaca en concreto el artículo 23 del texto legal, referente al uso de IA en salud, que dicta: "*1. Los sistemas de inteligencia artificial podrán emplearse, entre otras, para funciones de diagnóstico, apoyo a decisiones clínicas, gestión sanitaria, investigación, innovación o predicción epidemiológica, bajo condiciones de transparencia, explicabilidad y control humano. 2. El empleo de sistemas digitales de asistencia al diagnóstico y, en particular, de sistemas basados en inteligencia artificial no limitará el derecho a la libertad diagnóstica del profesional sanitario."* De esta manera, se deja entrever cierta limitación respecto al uso de los sistemas de IA en medicina, de forma que siempre se respete el margen de decisión de los profesionales sanitarios. Este instrumento puede convertirse en un punto de partida de cara al desarrollo de una futura ley nacional.

4.1. Perspectiva comparada de la regulación de inteligencia artificial en sanidad

Respecto a la normativa existente en el resto de países vecinos, Alemania es uno de los países más avanzado en la materia. En cuanto a legislación clave, destaca la *Digital*

[236] Acceso al documento: https://storage.cdn.eurecat.org/CIDAI/WhitePapers/WP-IA-Salut.pdf

Healthcare[237], del año 2019, que permite recetar aplicaciones médicas, siendo financiadas por el seguro público. De otro lado, destaca la iniciativa *Hospital Future Act*, del año 2020[238], que es un proyecto que tienen como objetivo financiar la digitalización hospitalaria, priorizando un modelo regulatorio muy claro para aplicaciones médicas, promoviendo el uso de la IA, así como la presencia de la telemedicina.

En cuanto a Francia, se convirtió en uno de los países pioneros en impulsar estrategias en materia de salud digital, como fue *Ma Santé* 2022[239], que propuso una gran reforma para digitalizar el sistema. En primer lugar, trataba de paliar las desigualdades de acceso a la atención sanitaria, teniendo en cuenta que el aumento de población dificultaba el acceso a las consultas. También reflejaba altas aspiraciones respecto a la mejora de la cooperación entre los diferentes profesionales sanitarios, pudiendo disponer de más tiempo para atender a sus pacientes, y que pudiesen contar con diversas oportunidades de formación. Actualmente la reforma casi integral del sistema sanitario no se ha logrado por completo, teniendo en cuenta que algunos de los objetivos previamente mencionados todavía no han podido cumplirse, pero sí que se ha progresado en otras cuestiones. Dentro de los principales desafíos con los que se han topado es las desigualdades en el acceso a la atención y la sostenibilidad financiera del sistema, pero ha habido avances en áreas como la digitalización de los servicios de salud y la mejora de la atención primaria. De otro lado, cuenta con una estricta regulación de datos sanitarios que se gestiona a través del *Health Data Hub*[240], de forma que cuenta con un marco sólido en telemedicina. Cuentan con una organización formada por 56 partes interesadas, destacando de entre ellas la Agencia Nacional de Salud, y se encargan de implementar las principales directrices estratégicas del Sistema Nacional de Datos Sanitarios (SNDS)[241]. Además, se creó un Comité Estratégico de Datos Sanitarios en el año 2021, que tiene como objetico apoyar el desarrollo del SNDS, formulando recomendaciones concretas para mejorar la recopilación, el intercambio y el uso de datos sanitarios en beneficio del interés público.

En cuanto a Reino Unido, diferentes iniciativas llevadas a cabo en IA clínica, como es la creación del NHS Digital[242], que es un organismo público ejecutivo no departamental,

---

[237] Digital Healthcare Act – DVG, aprobada el 7 de noviembre de 2019 por el Bundestag (Parlamento alemán) y adoptada el 7 de noviembre de 2019 por el Bundesrat (Consejo Federal).

[238] Fuente: Medinfo. Consultado en: https://medinfo.charite.de/en/digital_healthcare_cmio/hospital_future_act. Última fecha de consulta: 20 de noviembre de 2025.

[239] Fuente: Página del Gobierno Francés. Consultado en: https://sante.gouv.fr/archives/masante2022/. Última fecha de consulta: 20 de noviembre de 2025.

[240] Fuente: Heath Data Hub. Consultado en: https://www.health-data-hub.fr/. Última fecha de consulta: 20 de noviembre de 2025.

[241] Este sistema es una gran base de datos que recopila información sanitaria de la población francesa (casi el 99%). Está compuesto por diversas fuentes como los datos del seguro de enfermedad, los datos hospitalarios y los registros de defunciones, y su objetivo es servir como herramienta para la investigación, especialmente en farmacoepidemiología, así como para el sistema de salud en general. Fuente: "Uso del Sistema Nacional de Datos Sanitarios (SNDS) francés en farmacoepidemiología: una revisión sistemática en su fase de maduración", *Terapias,* vol. 79, núm. 6, noviembre-diciembre 2024, págs. 659-669.

[242] Fuente: Página del Gobierno de Reino Unido. Consultado en: https://www.gov.uk/government/organisations/nhs-digital. Última fecha de consulta: 20 de noviembre de 2025.

patrocinado por el Departamento de Salud y Asistencia Social. Dentro de los servicios que ofrece, destacan diversos proyectos para mejorar la atención médica en Inglaterra, incluyendo el desarrollo y la gestión de sistemas de tecnologías de la información tradicionales, la infraestructura de datos, la ciberseguridad y el soporte adecuado para el intercambio seguro de información. De otro lado, destaca la MHRA, que es la agencia responsable de la regulación de medicamentos y productos sanitarios[243], que publicó una guía sobre cuándo considerar al software médico como dispositivo médico[244]. Dentro de esta guía, se incluye un diagrama de flujo de decisiones del dispositivo, de forma que, dependiendo de si el dispositivo cumple o no con esas funciones, podrá considerarse tener esa consideración médica, o, al contrario. Por ejemplo: sí será considerado dispositivo médico si tiene uno o más de estas funciones: prevención de enfermedades, seguimiento de enfermedades, lesiones o discapacidades, control de la gestación etc. Sin embargo, si sus funciones son otras, como la educación médica del paciente, o almacenar o transmitir datos, entre otras, podrá entenderse que no tiene fines médicos. En el caso de una aplicación médica que proporciona simplemente nuestra frecuencia cardíaca no podría calificarse como un dispositivo médico, pero sí tendrá tal consideración cuando aconseje qué hacer, por ejemplo, en caso de que esa frecuencia sea demasiado alta.

Respecto a Estados Unidos, también cuenta con una regulación liderada por la FDA (Food and Drug Administration), destacando una guía en la que se recoge el software como dispositivo médico (*Software as Medical Device*)[245], aclarando cuando se considera que el software es un dispositivo médico. En este sentido, se define *como "software destinado a ser utilizado para uno o más fines médicos que realizan estos fines sin formar parte de un dispositivo médico de hardware".* Dentro de las funciones médicas, se encuentran: diagnóstico, prevención, seguimiento, tratamiento o alivio de enfermedades; que sustenta o mantiene tiene la vida, desinfección de dispositivos médicos, etc. Es muy interesante porque se encuentran también recogidas algunas notas respecto al fabricante de estos dispositivos, indicando lo siguiente: "*esta persona física o jurídica tiene la responsabilidad legal final de asegurar el cumplimiento de todos los requisitos reglamentarios aplicables al dispositivo médico en los países o jurisdicciones donde se pretende que esté disponible o se venda, a menos que esta responsabilidad sea impuesta específicamente a otra persona por la Autoridad Reguladora dentro de esa jurisdicción"*. De otro lado destaca la creación de un marco legislativo que regula la IA adaptativa, que se encuentra en proceso. En este sentido, en el mes de agosto de 2023 Joe Biden firmó un borrador de regulación de la IA para reducir los riesgos de caer en perjuicios y violaciones de los derechos civiles. Este decreto presidencial exigía a los creadores de sistemas de IA que entrañase riesgos para la economía o la salud pública que compartiesen

[243] https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency. Última fecha de consulta: 20 de noviembre de 2025.

[244] Acceso al documento: https://assets.publishing.service.gov.uk/media/64a7d22d7a4c230013bba33c/Medical_device_stand-alone_software_including_apps__including_IVDMDs_.pdf

[245] Acceso al documento: https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf

con el Gobierno los resultados de los test de seguridad antes de su difusión masiva[246]. Respecto a la telemedicina, está regulada por cada Estado de forma independiente. Cada estado tiene la opción de decidir si la telesalud está cubierta o no, qué tipos de telesalud están cubiertas, qué tipos de atención o servicios cubrir, y dónde en el estado puede estar disponible la telesalud. Por último, cuenta con una normativa de privacidad muy estricta para la salud, como es la HIPAA (Health Insurance Portability and Accountability Act), que es la Ley de Portabilidad y Responsabilidad de Seguros de Salud en Estados Unidos). La misma recoge el deber de los profesionales de salud de tomar medidas razonables para preservar la confidencialidad de la información médica personal, teniendo en cuenta las preferencias del paciente, de forma que a toda persona reconoce el derecho de confidencialidad, a no ser que autorice al médico que relevar información. También destaca que toda persona debe poder ver y obtener copias de su historial médico y pedir que se corrijan los errores que pueda contener.

Una noticia para destacar dentro de las iniciativas llevadas a cabo en este país es la de que el 24 de septiembre de 2024 el senador Edward Markey presentó en el Senado de los Estados Unidos la Propuesta de Ley para la protección de derechos individuales en relación con los algoritmos computacionales y para otras finalidades, también llamada "la Ley de Derechos Civiles de la Inteligencia Artificial 2024" (Artificial Intelligence Civil Rights Act of 2024). Esta norma representa un intento legislativo significativo para abordar los desafíos y riesgos asociados al uso de algoritmos computacionales por los ciudadanos estadounidenses, protegiendo los derechos individuales y abordando cuestiones como la discriminación, la transparencia y los sesgos[247].

En cuanto a Japón, presenta una estrategia digital nacional bastante robusta. Respecto a la telemedicina, se encuentra liberalizada desde 2020. Es uno de los países en los la que la IA está transformando la práctica médica. En el ámbito citológico, la combinación de Citología de Base Líquida (conocida como CBL) mezclada con algoritmos de aprendizaje profundo, ofrece nuevas soluciones para el tamizaje de cáncer cervicouterino[248]. Respecto a su regulación, no cuenta con normativa sectorial en materia médica, pero en mayo de 2025 se aprobó la primera legislación del país en materia de desarrollo y uso de inteligencia artificial para abordar los peligros que entraña el empleo inadecuado de esta tecnología. En virtud de los establecido en la normativa, el Gobierno puede abrir una investigación en caso de que se produzca un problema derivado del uso de la IA e incluso ofrece asesoramiento a las empresas, así como el público. Sin embargo, no se recoge ningún tipo de sanción y si existen sospechas de la comisión de algún delito, deberá recurrirse a normas especiales como el Código Penal.

Por tanto, a nivel global hemos visto que contamos con diferentes que promueven el uso ético de la inteligencia artificial en el ámbito sanitario, así como diferentes instrumentos

[246] Fuente: Revista Pesquisa. Consultado en: https://revistapesquisa.fapesp.br/es/normativa-sobre-inteligencia-artificial-en-ee-uu/. Última fecha de consulta: 20 de noviembre de 2025.
[247] Fuente: Cuatrecasas. Consultado en: https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/propuesta-regulacion-federal-ia-ee-uu. Última fecha de consulta: 20 de noviembre de 2025.
[248] Fuente: Citorushtc. Consultado eh: https://www.citorushtc.com/post/9-ctc-inteligencia-artificial-y-citologia-liquida-estudio-en-el-pa%C3%ADs-japon. Última fecha de consulta: 20 de noviembre de 2025.

normativos en los que se aclara qué requisitos es preciso que tenga un software que se utilizan en sanidad para ser considerado un dispositivo médico (o producto sanitario). Esto es realmente un avance, pero en materia legislativa todavía nos encontramos anclados en la creación de instrumentos de soft law, no vinculantes, que a la hora de exigir una reclamación de responsabilidad civil por un daño derivado de un sistema de inteligencia artificial que se utilice en el ámbito sanitario, no tendrán eficacia alguna, siendo precisa una regulación de carácter sectorial. A nivel europeo, es cierto que estas lagunas se pueden suplir con la aplicación de la normativa en materia de producto defectuoso mencionada anteriormente, la Directiva 2024/2853, pero cuenta con una exoneración por riesgos del desarrollo que puede dificultar el resarcimiento de la víctima, al poder ampararse el fabricante en que en el momento en el que se introduce el producto en el mercado, el estado de la ciencia y de la técnica del momento, no le permitieron advertir el defecto que presentaba el producto, y por ende, el daño que se podría ocasionar.

5. Solución autonómica

En primer lugar, habiendo advertido los principales desafíos con los que nos encontramos, en crucial que se promueve el desarrollo de algoritmos de IA que sean transparentes y explicables, estableciendo una serie de mecanismos que permitan evaluar y monitorear su rendimiento y precisión.

En segundo lugar, es preciso que se promuevan los *sandbox*, siguiendo las directrices recogidas en el AI Act y a través de estos se podrán validar clínicamente estas apps antes de sacarlas al mercado, así como será precisa su certificación conforme a la normativa de productos sanitarios[249].

En tercer lugar, en cuanto a la privacidad y protección de datos, se debe gestionar el anonimato o pseudonimización de los mismos siempre que sea posible, en aras a fomentar la privacidad de los usuarios y la protección de datos de carácter sensible.

En cuarto lugar, se convierte en un elemento primordial invertir en la educación digital de los usuarios, a través de campañas informativas de carácter público para explicar qué es la IA, sus usos en sanidad y cuáles son los riesgos que plantea.

En quinto lugar, se debe advertir a los proveedores de estos sistemas de la necesidad de información en caso de que se produzca una determinada actualización, así como de expresar cualquier advertencia a través de un lenguaje claro y accesible para personas sin formación técnicas, incluyendo el etiquetado de "contenido generado por IA", que corresponde según la normativa[250].

Por último, se debe promover una normativa regulatoria de carácter sectorial, que se convierte en el escudo protector de aquellos pacientes que sufran daños causados por sistemas de IA en el ámbito sanitario, donde ya se han empezado a hacer uso de

[249] En este sentido, véase la medida estratégica prevista en el capítulo VIII, referente a un sandbox autonómica IA-consumo.

[250] [250] En este sentido, véase la ficha normativa 12 prevista en el capítulo VIII, relativa al etiquetado de contenidos generados por IA.

dispositivos como Da Vinci, o el robot Star, siendo esta último completamente autónomo, utilizado en cirugía laparoscópica.

Hay que tener en cuenta que el Derecho sanitario no es propiamente Derecho de Consumo (vid. manual consumo p. 41-42).

III. COCHES AUTÓNOMOS

La IA también ha aparecido en el mundo del motor, permitiendo una conducción aparentemente mucho más eficaz y relejada, al no tener que ser el propio humano el que tenga el control del vehículo, pudiendo dejar artículo de ese trabajo en manos del vehículo, que ha sido diseñado especialmente para esta función. En este sentido, un informe reciente de la DGT asegura que más del 90% de los accidentes de tráfico se deben en alguna medida a errores humanos. Se entiendo que la conducción automatizada reducirá en gran medida los errores humanos en la conducción, ayudando a que disminuya el número de víctimas mortales en carretera[251]. Ahora bien, como veremos, surgen algunas cuestiones controvertidas para el consumidor, sobre todo en materia de ciberseguridad y falta de normativa específica en caso de que se produzca un accidente en este tipo de vehículos.

En cuanto al uso de coches autónomos en España, resulta especialmente interesante destacar que ya en el año 2018 el 43,5% de la población lo consideraba bastante útil, y el 44,8 % consideraban que esta nueva modalidad de vehículos era muy viable[252]. Es de especial relevancia destacar que, a través de la primera convocatoria del Perte del Vehículo Eléctrico y Conectado (VEC), cuya resolución se conoció en 2021, se han podido financiar tres proyectos enfocados en la conducción autónoma y la movilidad conectada, liderados por: Renault Group, Ficosa y Avanza Zaragoza. Esto les permite a los fabricantes poder realizar pruebas constantes de las tecnologías que permiten avanzar en la conectividad del vehículo con su entorno[253].

De otro lado, la Unión Europea pretende que haya 30 millones de coches eléctricos en Europa en 2038, aunque esa meta genera cierto escepticismo en el sector de la industria del motor debido a problemas técnicos. También se considera que la implantación de un coche autónomo podría reducir las ratios de mortalidad de tráfico si va acompañado de mejoras en las infraestructuras, como puede ser un carril exclusivo para la circulación de vehículos eléctricos que se propone en Reino unido. En este sentido, destaca un informe del Ministerio de Transportes británico del 2022, que recomienda *instalar Automated Lane Keeping Systems*, o sistemas automatizados de mantenimiento de carril, y defiende

---

[251] Fuente: Dirección General de Tráfico. Consultado en: https://www.dgt.es/muevete-con-seguridad/vehiculos-seguros/conduccion-automatizada/vehiculos-de-conduccion-automatizada/. Última fecha de consulta: 21 de octubre de 2025.

[252] En este sentido, es de especial relevancia el "Estudio sobre la opinión del vehículo autónomo", informe de enero de 2018, creado por Confederación Nacional de Autoescuelas, Universitat de València, Institut de Trànsit i Seguretat Viària.

[253] Fuente: el Economista. Consultado en: https://www.eleconomista.es/motor/noticias/13503386/08/25/espana-acelera-en-la-carrera-por-el-coche-autonomo-a-la-espera-de-cambios-en-la-normativa.html. Última fecha de consulta: 21 de octubre de 2025.

que los coches autónomos o los robots taxis harán más segura la carretera porque la IA reducirá el número de errores humanos y rebajará los accidentes y colisiones[254].

1. Concepto y tipología

En primer lugar, hemos de diferenciarlos según el grado de automatización, encontrándonos con vehículos autónomos y semiautónomos. En relación con el primer grupo, tal y como indica la Dirección General de Tráfico, *será aquel vehículo con capacidad motriz equipado con tecnología que permita su manejo o conducción sin preciar la forma activa de control o supervisión de su conductor, tanto si dicha tecnología autónoma estuviera activada o desactivada, de forma permanente o temporal*[255]. De esta manera, conformarían el segundo grupo aquellos vehículos en los que sería necesaria la intervención humana.

De otro lado, contamos con otras clasificaciones del nivel de automatización de vehículos, como la impulsada por la Sociedad de Ingenieros de Automoción (SAE), que clasifica el nivel de automatización en función del nivel de atención e intervención del humano en la conducción. En este estándar se recogen seis niveles de automatización: (i) nivel 0: *coche manual*, de forma que es el conductor el que se encarga de todas las tareas relativas a la conducción del vehículo, sin ningún sistema de ayuda; (ii) nivel 1, *conducción asistida*, de forma que un sistema de asistencia a la conducción se encarga de controlar la dirección o la aceleración, pero nunca los dos a la vez, y el conductor continua realizando el resto de tareas relativas a la conducción; (iii) nivel 2, *automatización parcial*, en el que uno o varios sistemas de asistencia a la conducción se encargan de la dirección y la aceleración o desaceleración; (iv) nivel 3, *automatización condicionada*, de forma que un sistema de conducción automatizada realiza todas las tareas de conducción, pero con ciertas limitaciones y el conductor debe responder a cualquier solicitud de intervención; (v) nivel 4, *automatización alta*, en el que un sistema de conducción automatizada realiza todas las tareas de conducción, incluso si el conductor humano no responde adecuadamente a una solicitud de intervención; y (vi) nivel 5, *driverless*, en el que un sistema de conducción automatizada realiza todas las tareas de conducción en todas las condiciones posibles, de forma que el vehículo puede prescindir completamente de la figura del conductor, del volante y de los pedales[256].

También entienden otros autores que el factor diferenciador se encuentra en quién monitoriza el entorno, sea el sistema de conducción automatizada o el conductor, pues el automóvil automático es un tipo de automóvil capaz de detectar su entorno y navegar sin ningún tipo de intervención humana[257]. Dependiendo del tipo de calificación, el sistema

---

[254] VÁZQUEZ PITA, E. Responsabilidad en vehículos autónomos y soluciones jurídicas de la Ley de Inteligencia Artificial (AI ACT), *Anuario da Facultade de Dereito da Universidade da Coruña* Vol. 28, 2024, pág. 67.

[255] NAVAS NAVARRO, S., et al, *Inteligencia artificial: tecnología y derecho*, Ed. Tirant lo Blanch, Valencia, 2017, pág. 101.

[256] Fuente: Dirección General de Tráfico. Consultado en: https://www.dgt.es/muevete-con-seguridad/vehiculos-seguros/conduccion-automatizada/vehiculos-de-conduccion-automatizada/. Última fecha de consulta: 21 de octubre de 2025.

[257] BARONA VILAR, S., *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice,* Ed. Tirant Lo Blanch, Valencia, 2021, pág. 99.

jurídico aplicable varía[258]. Ante la aparición de este tipo de vehículos, gran parte de las investigaciones sobre la toma de decisiones morales por parte de estos sistemas de inteligencia artificial, se centran en dilemas de sacrificio en el contexto de los coches autónomos. En el *Moral Machine Experiment*[259], llevado a cabo con millones de participantes de 233 países, se plantearon escenarios sobre un accidente inevitable variando los siguientes factores: (i) salvar personas frente a mascotas, (ii) salvar más vidas frente a menos vidas, (iii) salvar pasajeros frente a peatones, (iv) salvar a hombres frente a mujeres, etc., y las mayores diferentes se encontraron a favor de salvar personas antes que animales, salvar el mayor número de vidas y salvar preferentemente a personas jóvenes (aunque destacaron diferencias notables en contra de criminales, personas con sobrepeso, de bajo status social, hombres y pasajeros). Lo que sugiere este estudio es que las decisiones de los usuarios puedan ser tenidas en cuenta para programar la inteligencia artificial de los coches autónomos. Sin embargo, sus conclusiones han sido muy criticadas porque se base en criterios utilitaristas exclusivamente y porque no es permisible que sean los conductores quienes decidan los criterios de toma de decisiones de un coche autónomo[260].

2. Casos de uso

2.1. Sentencia Caso Tesla

Es ampliamente conocido que el gran desarrollo de los sistemas de inteligencia artificial se traduce en una mejora de la vida de los seres humanos, así como una comodidad inmensurable en el desarrollo de sus tareas diarias. Sin embargo, cuando la confianza en estos sistemas tiene carácter pleno, se pueden producir graves accidentes.

Esta reflexión no dista en demasía de lo que ya ha ocurrido en el mundo real. El día 29 de diciembre de 2019 un Tesla *Model S* que circulaba de modo usual salió de la autopista y se saltó un semáforo en rojo en una zona residencial. El vehículo colisionó contra un Honda Civil en una intersección, ocasionando el fallecimiento de dos de sus ocupantes. El fallo, según afirma el conductor es que no saltó el piloto automático, mientras que los funcionarios de las autoridades que investigaron el accidente determinaron que estaba activado en el momento del choque[261]. Aunque no suelen ser habituales, este tipo de

[258] Actualmente no se permite la circulación de vehículos autónomos en vías abiertas al tráfico en general en España, con excepción de aquellos que obtengan la autorización del Subdirector General de Gestión de la movilidad. Es el 1 de diciembre de 2021 el día en que se introdujo una enmienda al texto refundido de la Ley de Tráfico, a través del artículo 11 bis, referente a las obligaciones del conductor de un vehículo automatizado, y que indica lo siguiente: "*el titular del sistema de conducción automatizado de un vehículo deberá comunicar al Registro de Vehículos del organismo autónomo Jefatura Central de Tráfico las capacidades o funcionalidades del sistema de conducción automatizada, así como su dominio de diseño operativo, en el momento de la matriculación, y con posterioridad, siempre que se produzca cualquier actualización del sistema a lo largo de la vida útil del vehículo*."

[259] AWAD, E., DSOUZA, S., KIM, R., SCHULZ, J. et al., "The Moral Machine Experiment", *Nature*, 563 (7729), 2018, págs. 59-64., citado en ESPINOSA P., CLEMENTE M., La percepción de la toma de decisiones a través de inteligencia artificial cuando se produce daño a las personas, *Estudios Penales y Criminológicos.*, 44 (ext.), 2023, págs. 4-5. ISSN-e: 2340-0080.

[260] ESPINOSA P., CLEMENTE M., ob. cit., pág. 7.

[261] Periódico El Confidencial, artículo redactado por Omar Kardoudi, el 16 de marzo de 2022.

accidentes se deben a ese exceso de confianza de los humanos en las respuestas "seguras" de los coches automáticos. En 2020, una conductora fue acusada de homicidio debido al accidente que se produjo mientras supervisaba el volante tras las pruebas de un Uber todoterreno totalmente autónomo en la vía pública. Los funcionarios concluyeron que la conductora iba distraída viendo su teléfono unos segundos antes del choque y la policía aseguró que el accidente se podría haber evitado si el conductor hubiera estado atento.

2.2. Accidentes reiterados

Entre los meses de julio del año 2021 y mayo de 2022, se produjeron casi 400 accidentes de tráfico con vehículos que utilizaban este tipo de tecnología. Como resultado de los accidentes, seis personas perdieron la vida y cinco resultaron heridas de gravedad, y otros 41 sufrieron lesiones moderados o leves. Destaca en este sentido el informe de la NHTSA (La Administración Nacional de Seguridad del Tráfico en las Carreteras, que es una agencia dependiente del gobierno de los Estados Unidos) en relación con la fiabilidad de los vehículos autónomos y la opción de piloto automático. Es cierto que muchos de estos accidentes también se produjeron con vehículos autónomos Tesla, pero también debe valorar que existen 830.000 modelos de esta marca californiana en EE. UU. equipados con la función de piloto automático, encontrándose una gran diferencia con Ford, General Motors, o BMW que, aunque cuenten con una tecnología similar, disponen de muchas menos unidades circulando por carreteras estadounidenses[262].

Ya hay jurisprudencia que condena a un usuario que supervisaba la conducción autónoma en un test de entrenamiento, y al no estar atento puesto que estaba visualizando un vídeo, atropelló a un ciclista que la máquina tardó en reconocer. Así como el caso de un Volvo XC90 autónomo de Uber que circulada por la localidad de Tempe (Arizona), que atropelló a una mujer que cruzaba la calzada por una zona sin señalización, de coche y con su bicicleta. Tanto volvo como Uber reconocieron que en el momento exacto del suceso el vehículo estaba siendo objeto de pruebas en conducción autónoma, de forma que el conductor no pudo adoptar una medida preventiva para evitar el impacto. El principal problema fue que la mujer decidió cruzar la carretera sin darse cuenta de que un automóvil circulaba a pocos metros, y no se pudo hacer uso del sistema *City Safety* (circulaba a una velocidad aproximada de 65 km/h)[263]. La familia de la víctima entabló una demanda contra Uber y finalmente se llegó a un acuerdo extrajudicial. Es muy interesante destacar que los proveedores de sistemas de IA de estos vehículos decidieron no reconocer su responsabilidad, destacando varios argumentos: *Aptiv*, que era proveedor del *City Safety*, reconoció que en ese momento el sistema estaba desconectado. *Nvidia*, colaborador tecnológico de Uber indicó que este estaba utilizando su propia tecnología autónoma y no la de *Nvidia*. A partir de ese suceso Uber y *Nvidia* paralizaron sus pruebas de conducción autónoma por el país.

---

[262] Fuente: El Mundo. Consultado en: https://www.elmundo.es/motor/2022/06/19/62aeba79fdddff4c408b4588.html. Última fecha de consulta: 21 de octubre de 2025.

[263] Fuente: Diario de transporte. Consultado en: https://www.diariodetransporte.com/historico/sociedad/primer-atropello-mortal-un-coche-autonomo-sin-conductor-uber/. Última fecha de consulta: 25 de noviembre de 2025.

3. Riesgos e inconvenientes

Los principales riesgos que aparecen en el panorama actual son: la falta de seguridad, la responsabilidad, la privacidad, la ciberseguridad y la influencia en la industria. En este sentido, los coches autónomos que funcionan mediante sistemas de inteligencia artificial son ciertamente inseguros, y presentan ciertas lagunas legales puesto que destaca la existencia de algoritmos opacos. Otro factor determinante es el análisis masivo de datos por parte de plataformas y grandes redes interconectadas. En este sentido, la Unión Europea se ha pronunciado al respecto indicando que *"la opacidad, la complejidad, la imprevisibilidad y un comportamiento parcialmente autónomo, pueden haber difícil comprobar el cumplimiento de la legislación vigente de la UE sobre protección de derechos fundamentales, e impedir su cumplimiento efectivo"*[264].

Para evitar a priori este tipo de situaciones, una de las estrategias más efectivas ha sido exigir más test a los fabricantes y desarrollar los llamados "crash algorithms" (algoritmos de colisión). A través de ellos se predicen todos los escenarios posibles, de forma que el vehículo autónomo puede ser entrenado para saber cómo debe reaccionar en cada momento[265].

4. Normativa aplicable

En primer lugar, a nivel europeo, se aprobó en 2022 el Reglamento (UE) 2022/1426[266], que establece las bases para homologar vehículos automatizados de nivel 4, en el que se recoge todos los requisitos que son precisos para la posible circulación de estos vehículos. Merece especial mención la validación del concepto de seguridad por parte del fabricante, estableciéndose lo siguiente: *"el fabricante presentará una declaración en la que afirme que el ADS no entraña riesgos excesivos para los ocupantes del vehículo y para otros usuarios de la vía pública".*

En cuanto a normativa aplicable a nivel nacional, destaca el Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. Ahora bien, no podemos afirmar que este instrumento legislativo sea adecuado teniendo en cuenta la sofisticación con la que cuentan hoy en día los vehículos. En este sentido, se está tramitando la aprobación de un Real Decreto para vehículos totalmente automatizados[267], cuya aprobación se encuentra en curso. Alguna de las cuestiones que se quieren modificar son las siguientes: *"en el artículo primero se modificaría el Reglamento General de Circulación, incorporando dos nuevos artículos, el 4bis y el 18 bis, a través de los cuales se establecerían las condiciones*

[264] VÁZQUEZ PITA, E., ob. cit., pág. 71.
[265] Últ. ob. cit., pág. 80.
[266] Reglamento de Ejecución (UE) 2022/1426 de la Comisión de 5 de agosto de 2022 por el que se establecen normas para la aplicación del Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo en cuanto a los procedimientos uniformes y las especificaciones técnicas para la homologación de tipo del sistema de conducción automatizada (ADS) de los vehículos totalmente automatizados. DOUE, núm. 21, de 26 de agosto de 2022.
[267] Propuesta Real Decreto, por el que se modifiquen el Reglamento General de Circulación, aprobado por Real Decreto 1428/2003, de 21 de noviembre y el Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, en materia de conducción automatizada.

y los requisitos básicos para la circulación de estos vehículos, así como las obligaciones derivadas de su puesta en circulación. Adicionalmente, se añade un nuevo anexo V sobre normas y condiciones particulares de circulación de los vehículos dotados de un sistema de conducción automatizada, compuesto, a su vez, por dos secciones. La primera, relativa a las condiciones generales de circulación que deben satisfacer los vehículos totalmente automatizados, la segunda, disponiendo la creación del Manual de Circulación Segura en el que, en términos generales, se establecerán las condiciones para la circulación segura de estos vehículos cuando circulen por las vías públicas". También destaca el Real Decreto 465/2025[268], que tiene el objetivo de actualizar la señalización teniendo en cuenta los cambios sociales y tecnológicos producidos en materia de movilidad.

En cuanto a las instrucciones existentes a la hora de realizar las diversas pruebas, la DGT publicó la Instrucción 07/2025[269], para regular cómo elaborar las pruebas o ensayos de investigación con vehículos automatizados. Además, existen "Centros de Reconocimiento Tecnológico", que se encargan de certificar que los vehículos cumplen ciertos requisitos para realizar las pruebas. De otro lado, se está preparando una normativa especializada que regule los niveles más avanzados de conducción autónoma, como son esos niveles 4 y 5. La misma contará con obligaciones para los ocupantes, reglas específicas de circulación (como puede ser la inclusión de un manual de conducción segura) y una serie de parámetros exigibles sobre datos del sistema (entre los que destaca el software, las actualizaciones, el diseño operativo, etc.). De esta manera, en España se permite una conducción ordinaria hasta el nivel SAE 2, pero es preciso una autorización de prueba para niveles superiores.

En cuanto a la responsabilidad civil exigible en materia de daños derivados de un accidente de circulación, se abre una posibilidad más a la hora de reclamar daños causados por un accidente producidos por un coche autónomo debido a la nueva regulación. De esta manera, encontramos diferentes alternativas. De un lado, aparece la Directiva 2024/2853[270], que al considerar el software y el resto de los elementos digitales como "producto" propiamente dicho, facilita una indemnización por daños en aras a resarcir a la víctima. En este sentido, aludimos a las obligaciones establecidas para con el programador informático, que debe, además de poner en marcha un algoritmo funcional y seguro, en intentar evitar que su diseño del algoritmo genero sesgos o discriminaciones que puedan perjudicar a otros usuarios, obligación recogida en el artículo 9 del AI Act. En este sentido, los expertos en la materia sugieren que los ingenieros, matemáticos y aquellos que trabajan en la generación de algoritmos realicen un juramento hipocrático para comprometerse a no hacer daño o guiarse por unos protocolos éticos o negarse a

[268] Real Decreto 465/2025, de 10 de junio, por el que se modifica el Reglamento General de Circulación, aprobado por Real Decreto 1428/2003, de 21 de noviembre, en materia de señalización de tráfico.
[269] INSTRUCCIÓN VEH 2025/07. Asunto: Programa Marco de Evaluación de la Seguridad y Tecnología de Vehículos Automatizados (Programa ES-AV). Autorización de pruebas de vehículos automatizados en vías abiertas al tráfico en general.
[270] Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. DOUE núm. 2853, de 18 de noviembre de 2024.

realizar un trabajo que contradiga su código deontológico[271]. Así como en el artículo 25 del AI Act, que se traduce en una obligación de cumplimiento de este.

La responsabilidad civil se articulará a través de regímenes nacionales, como es la normativa de vehículos a motor, y más después de las modificaciones que se introducirán si finalmente esta propuesta normativa que ha sido comentada anteriormente sale adelante[272].

Respecto a la nueva normativa aprobada en materia de IA, algunos autores consideran que la atribución de responsabilidades civiles de los automóviles en caso de accidente se ha resuelto a través de la aprobación del AI Act[273]. En este sentido, el artículo 25 del AI Act atribuye expresamente la responsabilidad al fabricante, que se convierte en un potencial responsable de que el sistema de IA cumpla las obligaciones recogidas en el Reglamento, al formar parte de la cadena de valor. El principal problema a la hora de exigir responsabilidad sea cualquier fuere la vía elegida, será la de afrontar la carga probatoria, pues como hemos indicado anteriormente, se trata de sistemas de caja negra o "black box", que no siempre cumplen las obligaciones en materia de trazabilidad que se exigen.

De cualquier manera, en caso de que se quisiera desarrollar una regulación de carácter sectorial, se considera que cualquier regulación de los coches autónomos debería cumplir los siete requisitos esenciales expuestos en el Libro Blanco de Inteligencia Artificial de la UE[274]: (i) acción y supervisión humana, (ii) solidez técnica y seguridad; (iii) gestión de la privacidad y de los datos; (iv) transparencia, diversidad; (v) no discriminación y equidad; (vi) bienestar social y medioambiental y (vii) rendición de cuentas.

Otros autores plantean la posibilidad de que se apliquen determinadas leyes por analogía. Destaca en este sentido la autora francesa Marie-Julie Loyer-Lemercier, que plantea la posibilidad de aplicar la Ley Badinter[275] a los accidentes de tráfico en los que esté implicado un vehículo autónomo, entendiendo que no debe plantear graves problemas,

---

[271] VÁZQUEZ PITA, E., ob. cit., pág. 83.

[272] ATIENZA NAVARRO, María Luisa, *Daños causados por inteligencia artificial y responsabilidad civil*, Atelier Libros Jurídicos, Barcelona, 2022.

[273] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). DOUE núm. 1689, de 12 de julio de 2024. En este sentido, véase VÁZQUEZ PITA, E., ob. cit., pág. 68.

[274] Libro Blanco sobre la inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza. Bruselas, 19 de febrero de 2020.

[275] En Francia, la Ley 85-677 del 5 de Julio de 1985, llamada *Badinter,* es la "prima hermana" de nuestra Ley 30/1995. Se aplica a cualquier vehículo de motor que está involucrado en un accidente de tráfico. Una ley que, focalizada en la búsqueda, no tanto de un responsable, sino más en un deudor de una obligación de compensación de las lesiones corporales causadas, que no es otro que la compañía de seguros del conductor, excluye, deliberadamente, el razonamiento clásico de la responsabilidad civil, sobre la base, en particular, de la causalidad. Excluyendo claro está la fuerza mayor y el hecho de tercero como exoneración de la responsabilidad. Fuente: https://www.abogacia.es/actualidad/noticias/nuevo-sistema-de-valoracion-de-danos-en-accidentes-de-trafico-el-ejemplo-frances/.

siempre que un ser humano conserve la posibilidad de reconducir la dirección del volante, pisar el freno, etc. Ahora bien, en aquellos casos en los que el ser humano no tenga acceso al pedal ni al volante, la cuestión se torna mucho más delicada[276].

Ya hay países que han elaborado determinadas propuestas muy interesantes en materia de ciberseguridad, como la del Gobierno británico, que ha lanzado una guía no-estatutaria respecto al chequeo de las carreteras públicas y la relación de este tipo de vehículos con la ciberseguridad. En este sentido, un senador llegó a plantear la obligación de que el coche autónomo detectase y reportase los ciberataques o intentos de toma de control, protegiendo así los datos almacenados por el coche ya estuviese estacionado o en movimiento. Esto se realizó como objeto del proyecto de ley *SPY Car Act*, y aunque no se convirtió en ley, se traduce en un antecedente de gran importancia. Respecto a la normativa europea, destaca el Reglamento de Ciberresiliencia[277], en concreto su Considerando 34, que señala lo siguiente: *"Al integrar componentes procedentes de terceros en productos con elementos digitales durante la fase de diseño y desarrollo, los fabricantes, a fin de garantizar que los productos se diseñen, desarrollen y produzcan de conformidad con los requisitos esenciales de ciberseguridad establecidos en el presente Reglamento, deben ejercer la diligencia debida con respecto a dichos componentes, incluidos los componentes de programas informáticos libres y de código abierto que no se hayan comercializado".*

4.1. Perspectiva comparada de la regulación de inteligencia artificial en vehículos autónomos

Como hemos indicado, a nivel nacional, nos encontramos actualmente con un marco normativo que se encuentra en desarrollo. Se permite la conducción autónoma, pero sólo hasta el nivel SAE 2 en circulación ordinaria. En cuanto a las pruebas de niveles superiores, se permiten, pero solo bajo permisos especiales de la DGT. Existe un proyecto de Real Decreto para introducir niveles avanzados (niveles 4 y 5). Como hemos indicado, no existe un régimen completo de responsabilidad civil específico.

Respecto a la regulación de los países aledaños, en el caso de Alemania, es uno de los países más avanzado en materia regulatoria en el ámbito de la conducción autónoma en el ámbito de la Unión Europea. Respecto a las leyes más importantes, destaca la Ley de Conducción Autónoma en el año 2021[278], que permite la conducción de los vehículos de los niveles SAE 4 en rutas definidas. La misma cuenta con un marco completo de responsabilidad y requisitos técnicos, así como recoge una serie de rutas urbanas de pruebas autorizada. También se regula el manejo de los datos necesario para el funcionamiento, e incluso se define el término de "supervisor técnico", que es la persona

[276] LOYER-LEMERCIER M. J., *L'assurance des voitures inteligentes, de lássurance d'un human à l'assurance d'un robot,* Cerveau (x) ed Droit. Neurodroit, algorithmes, intelligence artifielle, objets connectés, centres de decisión, ed. LGDJ, Paris, 2023, pág. 301.

[277] Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) nº 168/2013 y el Reglamento (UE) 2019/1020 y la Directiva (UE) 2020/1828 (Reglamento de Ciberresiliencia). DOUE, núm. 2847, de 20 de noviembre de 2024.

[278] Acceso al documento: https://dserver.bundestag.de/btd/19/274/1927439.pdf

física que pueda desactivar o liberar las maniobras de conducción del vehículo de motor con función de conducción autónoma desde el exterior en casos individuales. También es interesante destacar que es preciso contar con un seguro de responsabilidad para la supervisión técnica.

Respecto a Francia, cuenta con autorizaciones para vehículos nivel SAE 3 y 4 en condiciones específicas. De otro lado, cuenta con una Ley de Movilidad[279] que incluye conducción autónoma, así como un marco robusto para la realización de pruebas. Se recoge en el Capítulo 2, y si bien no define el marco legal en el que debe producirse la circulación de vehículos autónomos, abre la posibilidad de circulación de estos vehículos, y establece cómo debe realizarse su regulación.

En cuanto a Reino Unido, desde el año 2021 permite niveles avanzados de automatización en la conducción bajo autorización. Actualmente, está en desarrollo el *Automated Vehicles Act*[280], en la que se encuentra definido el término de "responsabilidad del operador del sistema", en vez del conductor. Es muy interesante destacar lo establecido en el Capítulo 5, donde se incluyen sanciones civiles contra organismos regulados. Por ejemplo, establece que el secretario de Estado podrá emitir una notificación de sanción monetaria a una entidad autorizada de conducción autónoma si está convencido de que un vehículo automatizado autorizado ha cometido una infracción de tráfico, mientras la entidad era responsable del mismo.

En relación con Estados Unidos, no cuentan con una ley federal única, sino que cada Estado cuenta con una regulación propia. Dentro de los Estados punteros destacan California, Nevada, Arizona y Texas. En cuanto a los vehículos autónomos sin conductor, operan comercialmente en ciertas ciudades, como son Waymo y Cruise. Actualmente, el Departamento de Transportes ha anunciado que las empresas estadounidenses que desarrollen coches autónomos quedarán exentas de ciertas normas federales de seguridad[281], lo que se convierten en un incentivo para la innovación tecnológica, pero se convierte en un obstáculo a la hora de exigir responsabilidad en caso de que se cause un accidente.

Por último, destaca Japón, que es uno de los países más avanzados, puesto que desde el año 2023 cuenta con vehículos que son autónomos en su totalidad, y la circulación está autorizada para sistemas SAE 4, en determinadas zonas. Eiheiji fue la primera zona en la que se lanzó el primer servicio de transporte con conducción completamente automatizada, sin conductor.[282] Destaca la completa integración de estos vehículos en la ciudad, incluida la planificación urbana y el transporte público. En cuanto a la regulación, se está desarrollando una legislación para abordar la responsabilidad en caso de accidentes. También se está preparando la infraestructura necesaria para desplegar carriles

[279] Ley sobre Orientación de la Movilidad de Francia (Loi n° 2019-1428 d'orientation des mobilités).
[280] Acceso al documento: https://www.legislation.gov.uk/ukpga/2024/10/contents.
[281] Fuente: euronews. Consultado en: https://es.euronews.com/business/2025/04/27/estados-unidos-relaja-la-normativa-para-favorecer-la-llegada-de-los-coches-autonomos. Última fecha de consulta: 20 de noviembre de 2025.
[282] Fuente: Nippon. Consultado en: https://www.nippon.com/es/in-depth/d00917/. Última fecha de consulta: 20 de noviembre de 2025.

exclusivos para el transporte autónomo. En este sentido, Nissan tiene como objetivo lanzar un servicio de taxis de condición autónoma en abril de 2027[283], esperemos que la normativa llegue antes de este hecho, para lograr una protección real y efectiva.

En conclusión, los líderes mundiales en la materia son Estados Unidos, Alemania, Japón y Reino Unido. En España, como hemos visto, se cuenta con un marco sólido para las pruebas y se está preparando una normativa para regular la conducción cien por cien autónoma, incluyendo los niveles 4 y 5. Se considera que, una vez aprobada la normativa que se está tramitando actualmente, se equipararán las obligaciones del sistema autónomo con las que el conductor tiene actualmente[284].

5. Solución autonómica

En primer lugar, de cara a minimizar los posibles daños que puedan producirse, y siguiendo el ejemplo de Reino Unido, una acción para realizar a largo plazo puede ser construir vías especiales, que estén dotadas de sensores y comunicación entre vehículos, y con las señales de la carretera, sin cruces, o sin interacción con los peatones), de forma que los vehículos automáticos puedan circular con total seguridad[285].

En segundo lugar, otra medida que podría llevarse a cabo para fomentar un entorno más seguro en relación con el uso de vehículos autónomos podría ser solicitar la colaboración estatal para poder establecer un sistema de registro específico que incluya nivel de autonomía, fabricante, software utilizado y actualizaciones, facilitando de esta manera la trazabilidad en caso de siniestros[286].

En tercer lugar, en materia de prevención de riesgos, sería interesante elaborar protocolos de verificación técnica periódica, así como implantar inspecciones técnicas específicas para vehículos autónomos, que incluya revisión de sensores, algoritmos de decisión y conectividad. Una segunda acción en materia de prevención podría ser realizar campañas de concienciación ciudadana, en aras a informar a la población sobre cómo interactuar con este tipo de vehículos en la vía pública y qué hacer en caso de tener un accidente.

Por último, podría ser realmente interesante crear una unidad técnica a través de la cual se pueda monitorizar el comportamiento de los vehículos autónomos en tiempo real, que sea capaz de detectar anomalías, así como de coordinar respuestas rápidas. También sería aconsejable fomentar convenios para el desarrollo de sistemas predictivos de riesgo, simuladores de accidente y mejoras en la inteligencia artificial aplicada a la movilidad.

En conclusión, es reseñable que a nivel nacional hay una gran cantidad de trabajo en proceso, pero actualmente no contamos con una regulación completamente asentada. Es importante destacar que la tecnología avanza más rápido que la legislación, lo que puede

[283] Fuente: Swissinfo. Consultado en: https://www.swissinfo.ch/spa/nissan-planea-lanzar-un-servicio-de-taxis-de-conducci%C3%B3n-aut%C3%B3noma-en-jap%C3%B3n/73132652. Última fecha de consulta: 20 de noviembre de 2025.

[284] Fuente: El Mercantil. Consultado en: https://elmercantil.com/2024/11/23/veremos-a-kitt-por-las-carreteras-espanolas/. Última fecha de consulta: 20 de noviembre de 2025.

[285] En este sentido, cabe mencionar la acción realizada por China, donde desde el año 2018 se han habilitado circuitos de pruebas en entornos reales. Véase VÁZQUEZ PITA, E., ob. cit., pág. 78.

[286] En este sentido, véase la ficha normativa 3 prevista en el capítulo VIII, referencia al registro CLMIA.

traducirse en un sentimiento de inseguridad jurídica generalizado. En materia de protección de datos, es preciso garantizar la confidencialidad, puesto que la mayoría de los sistemas de IA se nutren de datos, y no en todas las ocasiones los consumidores conocen cuándo y, sobre todo, para qué fines, están cediendo esos datos. Respecto a la responsabilidad civil, es necesaria la realización de pruebas controladas y un régimen regulatorio de la responsabilidad algo más fuerte, de forma que, de aprobarse el uso extendido de este tipo de sistemas completamente autónomos, por ejemplo, las potenciales víctimas pueden verse resarcidas en caso de sufrir un daño.

CAPÍTULO VI. FORMACIÓN Y EMPODERAMIENTO CIUDADANO

1. Introducción

La IA ha llegado para quedarse, y para convertirse en una verdadera aliada. Para que eso pueda ser posible, es indispensable procurar una formación adecuada sobre IA a todos los consumidores y todo el personal que trabajan con ella. Por tanto, las personas encargadas de enseñar al conjunto poblacional como

En este sentido, a lo largo de este capítulo esbozaremos diferentes alternativas, que pueden complementarse entre sí, cuyo objetivo fundamental es conseguir que la población en general se encuentre lo suficientemente formada como para poder hacer un uso responsable de la IA, siendo consciente de las diversas ventajas, pero también riesgos y desavenencias que pueden surgir cuando presenta algún fallo.

En primer lugar, proponemos un plan formativo dirigido a inspectores, técnicos municipales, así como personal de las OMICs, que sirve como un instrumento útil de consulta cuando quieran tenerse presente conocimientos básicos sobre IA. También puede convertirse en una herramienta para promover el emprendimiento ciudadano en torno a la IA, con un enfoque ético primordial.

En segundo lugar, se plasma una guía de uso digital, para consumidores y pymes, a través de la cual se ofrezcan las principales utilidades de diversas herramientas desarrolladas gracias a la IA, y se recomienda cuál debe ser el uso debido de las mismas, teniendo en cuenta cuestiones fundamentales como la protección de datos.

En tercer lugar, también mencionaremos diversas campañas de sensibilización que promuevan una IA segura para toda la comunidad ciudadana que ya son una realidad en diferentes partes del mundo e incluso propondremos algunas que podrían ser llevadas a cabo por la administración autonómica.

Por último, destacaremos el papel fundamental de las asociaciones y redes ciudadanas en este ámbito.

2. Plan formativo para inspectores, OMICs y técnicos

Esta propuesta de plan formativo tiene el nombre de*: "Formación en nuevas tecnologías e Inteligencia Artificial para la protección de la Ciudadanía".* Los objetivos generales del mismo serían proporcionar conocimientos básicos sobre la IA, analizar sus principales riesgos éticos, legales y su afección a los consumidores, capacitar a los técnicos en la evaluación, prevención y control de los riesgos que implica el uso de la IA, así como la posibilidad de crear capacidades institucionales para acompañar procesos ciudadanos relacionados con la IA. La duración será de 40 horas. El plan estaría compuesto por seis módulos.

A) Módulo I. Introducción en la inteligencia artificial

En primer lugar, el módulo I está encaminado a la introducción en el concepto de la IA, de forma que se puedan explicar cuáles son sus tipos, cuál ha sido su evolución y cuáles son sus aplicaciones actuales. También se explicaría cuál es la diferencia entre IA débil y

fuerte, generativa o incluso qué quiere decir que algunos sistemas sean autónomos (por ejemplo, dentro de la IA débil encontramos los asistentes virtuales; mientras que podríamos calificar como IA fuerte un robot quirúrgico). Por último, se expondrían casos de uso en consumo dentro de la administración pública, el entorno privado e incluso en el emprendimiento.

Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) comprensión básica de la IA, explicando que es la misma y cómo se diferencia del resto de tecnologías digitales, así como conociendo los diversos conceptos claves, como son algoritmo, aprendizaje automático, sistema de recomendación o modelos generativos; (ii) realizar un primer acercamiento con la normativa en materia de IA que facilite su comprensión.

Los principales criterios de evaluación de este módulo serán los siguientes: (i) comprensión conceptual, (ii) conocimiento normativo; (iii) aplicación práctica; (iv) competencias de mediación; (v) actitud crítica y ética.

B) Módulo II. Riesgos y desafíos de la IA para los consumidores

En segundo lugar, el módulo II estaría orientado a los riesgos y desafíos de la IA para los consumidores, en este sentido se hablaría de casi todos los conceptos mencionados en apartados anteriores: opacidad algorítmica y falta de transparencia; sesgos algorítmicos y falta de transparencia, desinformación, *deepfakes* y manipulación digital; y recolección de datos y vulneración de la privacidad, teniendo en cuenta lo establecido en el artículo 22 RGPD, así como el artículo 5 del AI Act.

Dentro de los riesgos se deberá explicar los diferentes panoramas con los que nos enfrentamos actualmente derivados del uso de sistemas de IA. De un lado, el riesgo algorítmico, que se refiere a la posibilidad de que los algoritmos demuestren sesgos basados en factores dependientes de la persona que los crea; pudiendo manifestarse en decisiones automatizadas que afectan a la vida y derechos de las personas. También el riesgo de privacidad ante la IA, que se refiere a los posibles daños a la privacidad y derechos de los individuos causados por la recopilación, el uso y el procesamiento de datos por sistemas de inteligencia artificial, lo que se puede traducir en una exposición no autorizada de información, la manipulación de datos personales y la falta de control sobre la información que se recopila y utiliza. O el riesgo de manipulación de la IA (en relación con la Directiva 2005/29/UE), que se refiere al uso indebido de los algoritmos y sistemas de IA para influir en los resultados, de manera que benefician a ciertas partes interesadas, en detrimento de otras, lo que puede incluir desde la manipulación de resultados de búsqueda hasta la difusión de noticias falsas. La manipulación se lleva a cabo cuando se ajustan los parámetros del algoritmo para producir un resultado deseado, en vez de uno imparcial (por ejemplo, en plataformas de comercio electrónico es usual que los algoritmos se manipulen para mostrar los productos que más ingresos generados a la empresa, en vez de los que más interés generan al usuario).

Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) identificación de riesgos principales, pudiendo detectar problemas de seguridad y privacidad, riesgo de dependencia tecnológica, etc.; (ii) impacto en derechos básicos de

los consumidores, evaluando los riesgos en contratos digitales, por ejemplo, y relacionando estos riesgos con la normativa aplicable.

Los principales criterios de evaluación de este módulo serán los siguientes: (i) análisis crítico; (ii) aplicación normativa; (iii) competencias de mediación; (iv) dimensión ética y social.

C) Módulo III. Explicación del marco legal y ético de la IA

En tercer lugar, el módulo III debe ir dirigido a la explicación del marco legal y ético tanto a nivel internacional, europeo, nacional y autonómico sobre IA. En este sentido, se deberá abordar las principales consideraciones del AI Act haciendo hincapié en las obligaciones establecidas para proveedores de sistemas de IA de alto riesgo, así como la nueva Directiva 2024/2853 en materia de productos defectuosos, con especial consideración sobre los mecanismos de flexibilidad de carga probatoria introducidos por la misma. también destaca el Convenio de IA del Consejo de Europa. A nivel nacional, destaca la normativa relacionada con protección de datos, como es el RGPD, y a nivel autonómico destaca el Libro Blanco desarrollado por la comunidad de Cataluña, que puede servir como precedente al resto de las comunidades autónomas, pudiendo animarse a promulgar normativa sobre esta materia, en aras a suplir las lagunas que todavía existen en materia regulatoria.

De otro lado, se incluirán talleres de lectura con el objetivo de entender la normativa fundamental en materia de IA, como son: el AI Act, el DSA así como el TRLGDCU. Por ejemplo, se propone el siguiente ciclo de talleres:

- Taller 1: AI Act – Responsabilidad y Transparencia

  • Objetivo: Comprender las obligaciones de los proveedores y usuarios de sistemas de IA.

  • Lectura guiada: Títulos II y III del AI Act (clasificación de riesgos y requisitos de transparencia).

  • Caso práctico: una startup española lanza un sistema de IA para la automatización de la solvencia crediticia. Debate: ¿Está en la categoría de alto riesgo? ¿Qué obligaciones de transparencia debe cumplir?

  • Actividad: Identificar qué documentación técnica y evaluaciones de conformidad serían exigibles.

- Taller 2: DSA – Moderación de contenidos y plataformas

  • Objetivo: Analizar cómo el DSA regula la responsabilidad de las plataformas digitales.

  • Lectura guiada: Capítulos III y IV (obligaciones de proveedores de servicios intermediarios y plataformas muy grandes).

  • Caso práctico: una red social elimina comentarios críticos sobre un banco. Debate: ¿Se trata de moderación legítima o de censura?

- Actividad: Mapear los derechos de los usuarios (notificación, recurso, transparencia algorítmica).

- Taller 3: TRLGDCU – Protección del consumidor en entornos digitales
  - Objetivo: Revisar cómo se aplican los derechos de información, desistimiento y garantías en el comercio electrónico.
  - Lectura guiada: Libro II, Título II (contratos celebrados a distancia).
  - Caso práctico: un consumidor compra un dispositivo conectado (IoT) que deja de recibir actualizaciones al año. Debate: ¿Se vulnera el derecho a la conformidad del bien digital?
  - Actividad: Redactar un modelo de reclamación aplicando artículos sobre garantías y servicios digitales.
- Taller 4: Relación AI Act – DSA – TRLGDCU
  - Objetivo: Explorar cómo se solapan las tres normativas en escenarios reales.
  - Caso práctico: una plataforma de e-commerce usa IA para recomendar productos, modera reseñas de usuarios y vende bienes digitales.
  - Actividad: identificar obligaciones bajo el AI Act (riesgo del sistema de recomendación), revisar obligaciones de transparencia y notificación del DSA, aplicar derechos de desistimiento y garantía del TRLGDCU. Debate: ¿Qué tensiones aparecen entre innovación y protección del consumidor?

  Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) comprensión del marco normativo, conociendo los elementos esenciales del AI Act y relacionándolos con el resto de normativa; (ii) aplicación práctica del marco legal; (iii) capacitación para la mediación, dotando a los OMICs de herramientas para comunicar el marco legal de forma accesible.

  Los principales criterios de evaluación de este módulo serán los siguientes: (i) comprensión normativa; (ii) aplicación práctica del marco legal; (iii) competencias de mediación; (iv) visión crítica y prospectiva.

D) Módulo IV. Evaluación de competencias prácticas

El cuarto lugar, el módulo IV estaría relacionado con el papel de las OMICs y el resto de los técnicos en esta era de las nuevas tecnologías, en aras a la evaluación de competencias prácticas. Para ello, deben adquirir nuevas competencias respecto a la atención ciudadana. También es de especial importancia la formación de estos para poder evaluar los productos y servicios impulsados por IA, incluida la detección de posibles fraudes, estafas o potenciales vulneraciones de derechos. Por último, debería incluirse un modelo de protocolo de actuación ante reclamaciones relacionadas con daños derivados de sistemas de IA. Debe atenderse a lo recogido en la Guía de la AEPD sobre decisiones automatizadas del año 2022.

Se incorpora un protocolo de triaje para la formación:

1. *Recepción y preparación.*

- Objetivo: Garantizar que cada participante comprende el contexto de la simulación.
- Acciones:

- Explicar brevemente el caso práctico (ej. reclamación por decisión automatizada en crédito).

- Entregar materiales de apoyo (ficha del caso, normativa aplicable).

- Recordar criterios de evaluación (normativa, mediación, ética, comunicación).

2. *Clasificación inicial de competencias*

- Objetivo: Identificar el nivel de preparación antes de la simulación.

- Acciones:

- Breve cuestionario diagnóstico sobre normativa (AI Act, DSA, TRLGDCU).

- Preguntas rápidas sobre principios éticos (equidad, transparencia, responsabilidad).

- Resultado: Clasificación preliminar en tres niveles:

- Nivel 1 (básico): Conocimientos generales, dificultad para aplicar normativa.

- Nivel 2 (intermedio): Reconoce riesgos y derechos, aplica normativa con apoyo.

- Nivel 3 (avanzado): Aplica normativa y ética con autonomía y seguridad.

3. *Simulación de casos*

- Objetivo: Observar competencias prácticas en acción.

- Acciones:

- Role-play de mediación entre consumidor y empresa.

- Resolución escrita de un caso práctico con aplicación normativa.

- Debate grupal sobre dilemas éticos en IA y consumo.

- Observación: Evaluar desempeño en tiempo real según rúbrica.

4. *Triaje de desempeño*

- Objetivo: Clasificar resultados según competencias demostradas.

- Categorías de triaje:

- A – Competencia plena: Aplica normativa y ética con claridad, comunica eficazmente, propone soluciones viables.

- B – Competencia suficiente: Identifica riesgos y derechos, necesita apoyo en mediación o aplicación normativa.

- C – Competencia en desarrollo: Reconoce conceptos básicos, pero presenta dificultades en análisis crítico y comunicación.

- D – Competencia insuficiente: No logra aplicar normativa ni principios éticos en la práctica.

5. *Retroalimentación y seguimiento*

- Objetivo: Asegurar aprendizaje continuo.

- Acciones:

  - Entregar informe individual con fortalezas y áreas de mejora.

  - Recomendar recursos adicionales (lecturas, guías, talleres).

  - Proponer actividades de refuerzo para quienes estén en categorías C y D.

6. *Registro y documentación*

- Objetivo: Garantizar trazabilidad y transparencia en la evaluación.

- Acciones:

  - Registrar resultados en fichas individuales.

  - Archivar materiales producidos (portafolio, fichas de casos).

  - Elaborar informe global del grupo con distribución de niveles.

De otro lado, se introduce también un modelo de solicitud de explicaciones significativas, que se introduce como Anexo 13.

Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) aplicación de la normativa en la práctica, pudiendo demostrar suficiente competencia para aplicar la normativa en materia de IA en reclamaciones reales, identificando incumplimientos normativos y proponiendo soluciones ajustados al marco legal; (ii) competencias de mediación, de forma que resuelvan los conflictos de forma clara y equilibrada y muestren capacidad para comunicar riesgos y derechos de forma accesible y clara; (iii) capacidades técnicas, de forma que puedan manejar herramientas digitales básicas para analizar reclamaciones vinculadas a la IA y al comercio electrónico.

Los principales criterios de evaluación de este módulo serán los siguientes: (i) aplicación de la normativa; (ii) resolución de casos prácticos; (iii) competencias de mediación; (iv) producción de materiales prácticos.

E) Módulo V. Emprendimiento ciudadano y uso responsable de las tecnologías

En quinto lugar, el módulo V estaría relacionado con el emprendimiento ciudadano y el uso responsable de las nuevas tecnologías. En este sentido, será fundamental destacar la

importancia del emprendimiento con IA en el entorno local, haciendo asequible y comprensible para la ciudadanía en general los múltiples beneficios que puede reportar el uso de esta. De otro lado, se deben analizar diversos proyectos ciudadanos relacionados con la materia e incluso plasmar una serie de ejemplos y buenas prácticas. También será importante potenciar un diseño de servicios digitales de carácter ético, promoviendo un uso responsable y eficiente de estas tecnologías, intentando exponer no solo sus ventajas, sino también sus riesgos e inconvenientes. Como ejemplos de proyectos ciudadanos financiados por la UE destacan Horizonte Europea y *Digital Europe*. Por último, será fundamental proporcionar un catálogo de herramientas que sean de fácil uso y accesibles, que ayuden incluso a prototipar proyectos con IA. Todo ello teniendo en cuenta lo establecido en la LOPDGDD.

Dentro del marco de este módulo, sería interesante realizar el seguimiento de la siguiente checklist del RGPD para Pymes:

1. Registro y análisis de datos

- Identificar qué datos personales se recogen (clientes, empleados, proveedores).
- Determinar la finalidad de cada tratamiento.
- Elaborar el registro de actividades de tratamiento (obligatorio).

2. Base legal del tratamiento

- Verificar que cada tratamiento tiene una base legitimadora (consentimiento, contrato, obligación legal, interés legítimo).
- Documentar la justificación de cada base legal.

3. Políticas y documentación

- Redactar y publicar una política de privacidad clara y accesible.
- Incluir cláusulas informativas en formularios, contratos y comunicaciones.
- Formalizar contratos con encargados de tratamiento (ej. gestoría, hosting).

4. Seguridad y protección de datos

- Implementar medidas técnicas y organizativas: contraseñas seguras, cifrado, copias de seguridad.
- Restringir accesos a datos según funciones.
- Revisar periódicamente la seguridad de sistemas y dispositivos.

5. Derechos de los usuarios

- Establecer un procedimiento para atender derechos ARSULIPO (acceso, rectificación, supresión, limitación, portabilidad, oposición).
- Informar a los interesados sobre cómo ejercer sus derechos.

6. Gestión de brechas de seguridad

- Definir un protocolo de detección y notificación de incidentes.
- Notificar a la AEPD y a los afectados en caso de brecha grave en un plazo máximo de 72 horas.

7. Delegado de Protección de Datos (DPO)

- Evaluar si la empresa está obligada a designar un DPO (ej. tratamientos a gran escala o datos sensibles).
- En caso de no ser obligatorio, asignar un responsable interno de cumplimiento.

8. Formación y concienciación

- Formar al personal en buenas prácticas de protección de datos.
- Promover la cultura de privacidad en la organización.

9. Evaluaciones y auditorías

- Realizar análisis de riesgos periódicos.
- Documentar medidas correctivas y mejoras.
- Revisar la adecuación del cumplimiento al menos una vez al año.

También se adjunta un modelo de acuerdo SaaS con cláusula de transparencia en el anexo 14.

Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) fomentar la cultura emprendedora ciudadana, promoviendo la iniciativa y creatividad por parte de los ciudadanos en proyectos digitales y sociales; e identificando oportunidades de emprendimiento vinculadas a la economía digital (ii) desarrollar competencias digitales responsables, reconociendo los beneficios y riesgos asociados al uso de tecnologías emergentes; (iii) capacitar a los OMICS para la innovación con impacto social, incorporando una perspectiva de inclusión digital y accesibilidad.

Los principales criterios de evaluación de este módulo serán los siguientes: (i) comprensión conceptual; (ii) aplicación práctica; (iii) competencias de ciudadanía digital; (iv) creatividad e innovación.

F) Módulo IV. Simulación con casos reales

En sexto lugar, el módulo VI consistirá en un taller práctico que incluya simulación de casos reales. En este sentido, sería muy útil incluir simulaciones de atención a consumidores afectados por decisiones automatizadas, evaluación de productos digitales desarrollados con sistemas de inteligencia artificial, así como el diseño de un plan de acción local sobre IA y ciudadanía. En este sentido, destaca la importancia del artículo 97 bis TRLGDCU sobre transparencia en mercados en línea.

De otro lado, el plan formativo deberá tener una duración aproximada de 40 horas, teniendo cada uno de los módulos entre 6 y 8 horas. Se podría impartir en una modalidad híbrida, adaptándose a las necesidades de las personas que sean receptores de este plan. Se deben incluir dinámicas participativas y debates, e incluso podrían crearse entornos de prueba y simuladores para explorar sistemas de IA en diferentes situaciones para los consumidores. Dentro de los materiales utilizados, sería preciso utilizar un manual del plan en formato digital, así como una guía rápida de detección de riesgos en IA para técnicos municipales. También sería interesante contar con una base de datos con casos de uso y reclamaciones reales y acceso a diversas plataformas.

Un ejemplo de una simulación con documentación debe incluir logs, parámetros, capturas de imágenes e incluso el histórico de precios. Se propone el siguiente ejemplo:

- Escenario: Plataforma de e-commerce con motor de precios dinámicos (IA) para pequeños electrodomésticos.
- Incidencia: Un consumidor detecta incrementos de precio al iniciar sesión y tras añadir el producto al carrito. Sospecha de discriminación algorítmica y "dark patterns"[287].
- Objetivo del ejercicio: verificar si hay segmentación injusta o manipulación, evaluar transparencia, explicaciones significativas y cumplimiento normativo (RIA/DSA/TRLGDCU/RGPD).
- Redactar respuesta de mediación y medidas correctivas.

Se proponen una serie de plantillas de salida que pueden ser útiles para mediación.

- Respuesta al consumidor:
  - Resumen del hallazgo: El precio varió por alta demanda y por una regla vinculada al estado del carrito.
  - Medidas: Se ha desactivado la regla de carrito para evitar variaciones no informadas; se publicará una política de precios dinámicos clara.
  - Compensación: Aplicación del precio más bajo visto durante su sesión y cupón del 5% en próxima compra.
  - Recurso: Puede solicitar revisión adicional y recibir una explicación ampliada del algoritmo usado.
- Informe de cumplimiento:
  - Hallazgos: Transparencia insuficiente en "regla carrito". No se detecta uso de atributos protegidos.
  - Riesgos: Prácticas desleales y presión comercial.

[287] En el Anexo 17 se incluye una checklist de "dark patterns" en interfaces.

- Acciones: Política de precios, UI con explicación, tope de variación, auditoría trimestral del motor de *pricing*.

Los principales objetivos de aprendizaje de este módulo serán los siguientes: (i) aplicar conocimientos normativos en escenarios reales, identificando obligaciones incumplidas por proveedores y plataformas en situaciones simuladas; (ii) desarrollar competencias de mediación, practicando la gestión de reclamación vinculadas a decisiones automatizadas, publicidad engañosa, etc.

Los principales criterios de evaluación de este módulo serán los siguientes: (i) aplicación normativa; (ii) resolución de casos prácticos; (iii) competencias de mediación; (iv) integración legal.

3. Guías digitales para consumidores y PYMES

3.1. Guía digital para consumidores

En primer lugar, en cuanto a la guía digital para consumidores, proponemos la siguiente, que lleva por título: *"Inteligencia Artificial y tú: cómo protegerte y beneficiarte de la inteligencia artificial como consumidor".*

El primer punto fundamental es explicar qué es la IA. Si bien es cierto que no se puede dar un significado exacto, pues se define de múltiples formas, podemos definirla como el conjunto de tecnologías que permiten a las máquinas tomas decisiones, resolver problemas o incluso imitar algunas habilidades humanas como pueden ser el lenguaje o la visión. Como ejemplos de IA, podemos hablar de IA de tipo generativo, como pueden ser asistentes virtuales o recomendadores. Deberá tenerse en cuenta lo establecido en el DSA, artículos 26 a 28 sobre publicidad y sistemas de recomendación.

El segundo punto es hacer ver al consumidor dónde está la IA presente en la vida diaria de los consumidores, como puede ser en las compras online, en las recomendaciones personalizadas, o incluso en los precios dinámicos, que son aquellos que se calculan de forma automatizada en función de diferentes parámetros como puede ser la diversa demanda que exista de un determinado producto en comparación con la oferta propuesta. En las redes sociales también está presente, pues a través del contenido que consume el usuario, las plataformas ofrecen productos relacionados con sus gustos y preferencias, que es lo que se denomina "selección de contenido". En el ámbito de las finanzas, la IA aparece a través de los créditos automatizados, que tienen en cuenta las condiciones económicas y personales del solicitante para adaptarse a las necesidades de este, y el conocido como "*scoring bancario*", que es una puntuación numérica que utilizan las entidades financieras para evaluar la capacidad de pago de un solicitante de crédito. En el ámbito de la salud, destacan las apps de bienestar, utilizadas para calcular diferentes parámetros de salud como son el pulso, la frecuencia cardíaca, la cantidad de insulina en sangre; o relacionados con el deporte, como la cantidad de actividad realizada en un día, el tipo de deporte realizado. También destaca el diagnóstico asistido por sistemas de inteligencia artificial, cuyo uso está cada vez más expandido en todo el mundo. Por último, en el ámbito de la atención al cliente, es preciso que los consumidores sean

conscientes de que en múltiples ocasiones no son atendidos por una persona física, sino por un chatbot automático, que le proporciona las respuestas exactas a sus necesidades.

Como tercer punto fundamental, es preciso destacar los beneficios que puede tener la IA para los consumidores, como son: mejorar la experiencia del usuario, dando respuestas concretas a sus consultas; ofrece servicios personalizados a las necesidades de cada consumidor, teniendo en cuenta múltiples factores; automatiza gestiones rutinarias, de forma que ahorra tiempo de calidad para los trabajadores, que pueden desempeñar en otro tipo de tareas, de forma que permite también ahorrar mucho esfuerzo por parte del personal, que puede ser dedicado a otras funciones.

Como cuarto punto fundamental, es preciso indicar cuáles son los riesgos que plantea el uso de la IA a los consumidores. En primer lugar, destaca la falta de transparencia, pues, como hemos indicado, los encontramos con sistemas de caja negra, de baja trazabilidad. En segundo lugar, con este tipo de decisiones automatizadas está presente el riesgo de discriminación algorítmica, de forma que algunas decisiones tomadas pueden ser injustas, al haberse alimentado los sistemas con datos poco representativos. En tercer lugar, destaca también la importancia de proteger la privacidad, y en este sentido destacan el consentimiento de las denominadas cookies, que en ocasiones son aceptadas de forma automática por todos los usuarios, sin ser realmente conscientes de lo que están haciendo, y la cantidad de información que están cediendo. El cuarto lugar, destaca la dependencia tecnológica, sobre todo en menores de edad, debiendo ser conscientes tanto los menores como los adultos mayores de edad responsables de los mismos de los múltiples problemas que se pueden ocasionar si no se controla de manera debida tanto las acciones realizadas en Internet, las diversas páginas web que se visitan, así como el tiempo que se pasa en las mismas. Por último, es fundamental advertir al consumidor de la cantidad de agentes maliciosos que conforman Internet, estando presentes continuamente la realización de múltiples estafas, como son el *phishing* (a través de un correo electrónico, solicitan que pinches un enlace como remedio a un supuesto problema planteado, como puede ser que nuestro banco va a bloquear nuestra tarjeta por un error del sistema, y para remediarlo, debemos pinchar ese enlace); *vishing* (múltiples estafas a través de llamadas telefónicas, suplantación de identidad por nuestra voz).

En quinto lugar, es fundamental que el ciudadano sepa cómo debe proteger sus derechos. En este sentido, deben conocer que tienen derecho a conocer que están siendo objeto de una decisión automatizada. También deben verificar todo tipo de fuentes que consulten, siendo un indicio de fiabilidad que el comienzo de una página web sea *"https://ss",* con "s" de "*secure*" (seguridad). Si bien es cierto que no es un indicio infalible, sí que es una de las claves para comprobar si nos encontramos con una web segura. De otro lado, es necesario leer las políticas de privacidad recogidas en las páginas web o aplicaciones utilizadas, y más cuando se utiliza en las mismas IA. Los usuarios deben conocer que las aplicaciones se alimentan con sus datos, que se utilizan para hacerlas mejores, y con un mayor conocimiento de todos los intereses del usuario. Además, es importante no compartir datos personas con chatbots sin verificar, y exigir atención humana cuando el usuario lo necesite.

El sexto lugar, es primordial que los usuarios conozcan cuáles son los derechos recogidos en la ley. En cuanto al AI Act, se recogen una serie de artículos en los que se protege a los consumidores frente a los diversos riesgos causados por sistemas de IA; el RGPD les da derecho a no ser objeto de decisiones automatizadas sin intervención humana, solicitar la corrección o revisión de esas decisiones e incluso solicitar el borrado de los datos.

En séptimo lugar, es preciso hacer hincapié en el uso de estos sistemas como complemento, pero no como sustituto del criterio personal de forma completa, pues son sistemas que se van mejorando y actualizando con el paso del tiempo, y no siempre ofrecen respuestas correctas. Además, deben revisar la configuración de privacidad de las aplicaciones que tengan instaladas y las redes sociales, así como desactivar las recomendaciones automáticas si no están conformes. Es de gran utilidad el uso de herramientas de verificación de contenido falso, denominadas *fact-checking.* En caso de tener cualquier problema, el consumidor debe contactar con su OMIC local, habiendo guardado previamente capturas o registros de sus diversas interacciones con los sistemas de IA. En caso de que no se llegue a un acuerdo con la empresa, se debe acudir a organismos de protección de datos u organismos superiores de derecho de consumo.

Por último, la IA reporta grandes beneficios dentro de una empresa, si se utilizada de manera adecuada, pues permite llevar a cabo determinadas tareas de forma automatizada e incluso pudiendo programarlas, permite procesar, analizar y ordenar grandes volúmenes de datos, ayuda a realizar análisis del comportamiento de los clientes, prediciendo tendencias y acciones futuras e incluso favorece los procesos de digitalización de las empresas[288].

3.1.1. Cómo ejercer tus derechos

En primer lugar, se debe reclamar primero ante la empresa o proveedor La acción inicial es presentar reclamación directamente a la empresa (servicio de atención al cliente, formulario web, correo electrónico certificado).

- Contenido mínimo:
    - Identificación del consumidor.
    - Descripción clara del problema (ej. decisión automatizada, publicidad engañosa, uso indebido de datos).
    - Documentación de soporte (capturas, facturas, comunicaciones).
- Plazo de respuesta: La empresa debe contestar en un plazo máximo de 30 días naturales.

En segundo lugar, se debe acudir a la OMIC (Oficina Municipal de Información al Consumidor)

[288] En este sentido, véase el proyecto *AceleraPyme*, impulsado por el Ministerio para la Transformación Digital y de la Función Pública del Gobierno de España.

- Cuando: Si la empresa no responde, rechaza la reclamación o la respuesta es insatisfactoria.
- Acción: Presentar la reclamación en la OMIC de tu municipio.
- Plazo: La OMIC suele iniciar la mediación en un plazo de 15 días hábiles desde la recepción de la reclamación.

En tercer lugar, se puede reclamar ante la AEPD (Agencia Española de Protección de Datos)

- Cuando: Si el problema afecta a datos personales (ej. uso indebido de datos, falta de consentimiento, brechas de seguridad).
- Acción: Presentar reclamación a través de la sede electrónica de la AEPD.
- Plazo de resolución: La AEPD debe admitir a trámite y resolver en un plazo aproximado de 6 meses, aunque puede variar según la complejidad.

O se puede reclamar ante la AESIA (Agencia Española de Supervisión de la Inteligencia Artificial)

- Cuando: Si el problema está vinculado al uso de sistemas de IA que afectan derechos del consumidor (ej. decisiones automatizadas sin explicación, sesgos, falta de transparencia).
- Acción: Presentar reclamación ante la AESIA, que supervisa el cumplimiento del AI Act y la normativa nacional de IA.
- Plazo: La AESIA establecerá plazos de admisión y resolución, generalmente entre 3 y 6 meses según el caso.

Por último, se acudirá a arbitraje de consumo solo si la empresa está adherida al sistema arbitral, se puede solicitar arbitraje gratuito y vinculante. O a la vía judicial: en última instancia, puesto que el consumidor puede acudir a los tribunales ordinarios.

Resumen de pasos y plazos

Paso	**A quién dirigirse**	**Plazo de respuesta**
1. Reclamación inicial	Empresa/proveedor	30 días
2. Mediación	OMIC	15 días hábiles para iniciar
3. Protección de datos	AEPD	~6 meses
4. Supervisión IA	AESIA	3–6 meses
5. Escalado	Arbitraje / Tribunales	Variable

Se añade una lista de verificación, que facilite la reclamación:

- Identificar si hubo automatización
  - Comprobar si la decisión (ej. precio, recomendación, denegación de servicio) fue tomada por un sistema automatizado.
  - Revisar mensajes, políticas de la empresa o condiciones de uso que lo indiquen.
- Solicitar intervención humana
  - Pedir que una persona revise la decisión automatizada.
  - Exigir un canal claro para recurso humano, conforme al RGPD y AI Act.
- Pedir explicación significativa
  - Solicitar información comprensible sobre los criterios utilizados por el sistema.
  - Preguntar qué datos se tuvieron en cuenta y cómo afectaron al resultado.
- Guardar evidencias
  - Conservar capturas de pantalla, correos, facturas y comunicaciones.
  - Registrar fechas, precios o condiciones que hayan cambiado.
  - Guardar número de referencia de reclamaciones o tickets.

3.2. Guía digital para PYMES

En cuanto a la guía digital para PYMES, el título para la misma es *"Inteligencia Artificial para tu Negocio: Oportunidades, Retos, y Buenas Prácticas para PYMES"*. Es fundamental, en primer lugar, conocer qué funcionalidades puede hacer la IA por nuestra pequeña y media empresa, que en ocasiones puede resultar de gran utilidad. En este sentido, permite: automatizar tareas repetitivas, como puede ser la facturación, o atención al cliente; mejorar el marketing digital con segmentación inteligente, de forma que permite acercar la empresa al tipo de cliente para el que realmente será atractiva; también permite optimizar inventarios y funciones logísticas, procurando un gran ahorro del tiempo; analizar datos de clientes y tendencias seguidas en cada momento; así como generar contenido como pueden ser textos, imágenes o vídeos. Ahora bien, respecto a esta última cuestión, es fundamental que se incluya la marca de agua correspondiente, informando al consumidor que son imágenes ficticias, que han sido desarrolladas gracias al uso de IA, pues es fundamental proporcionar la información necesaria para no crear una ilusión óptica, que nunca podrá ser traducida a la realidad completamente.

En segundo lugar, proporcionamos diferentes herramientas desarrolladas gracias a la IA que pueden ser realmente útiles para PYMES. En materia de atención al cliente, algunos chatbots de gran utilidad pueden ser *Tidio*, *Zendesk AI* o *Landbot*. En el sector del marketing, pueden reportar grandes beneficios aplicaciones como *Mailchimp* con IA,

ActiveCampaign, Marketo o *HubSpot*. Para la generación de contenido, destaca el uso de *ChatGPT* o *Jasper*. También destacan CRM (*customer relationship management*) inteligentes, como *Salesforce* o *Zoho*. Para el ámbito de financias y contabilidad, puede reportar gran utilidad aplicaciones como *QuickBooks* o *Holded*. Para el análisis de datos y la toma de decisions, pueden resultar de gran utilidad *Microsoft Power BI* o *Google Looker Studio*. Para la gestión de proyectos, herramientas como *Monday.com* o *Trello* pueden ser de gran utilidad para realizar tareas repetitivas, recordatorios y asignaciones de trabajo, mejorando la eficiencia del equipo. Por último, plataformas *No Code,* que son aquellas que permiten crear aplicaciones y sitios web sin necesidad de programar, facilitando el desarrollo para emprendedores y pequeñas empresas, entre las que destacan *Peltarion* o *Google AutoML.* Ahora bien, conviene advertencia sobre el cumplimiento del RGPD (en concreto, artículos 44 a 49) en transferencias internacionales que se realicen de datos personales la necesidad de TIA (Transfer Impact Assessment).

En tercer lugar, en cuanto a los beneficios, destacan: el ahorro de tiempo y costes, la mejora en la toma de decisiones, el incremento de la productividad, y un aumento del crecimiento y la innovación. En cuanto a los riesgos, se debe prestar especial atención al uso indebido de datos de clientes, la falta de control sobre decisiones automatizadas, la pérdida de contacto humano con el cliente, errores de automatización sin supervisión, así como el evitar una confianza ciega en herramientas gratuitas o poco fiables.

En cuarto lugar, proporcionamos una serie de claves para un uso plenamente responsable y acorde a la legalidad de los sistemas de IA, de forma que deben seguirse las siguientes indicaciones: cumplir con el RGPD cuando se trate de datos de carácter personal, informar a los clientes del uso de IA para la toma de decisiones; no reemplazar la atención humana, sino mejorarla y complementarla con el uso de IA; indicar si un texto, email o imagen ha sido generada con IA; y por último, revisar las respuestas proporcionadas por estas herramientas, no perdiendo el factor crítico característico del ser humano. En este sentido, es indispensable establecer una serie de políticas y procedimientos para monitorear continuamente el cumplimiento de los principios éticos durante todo el ciclo de vida de los sistemas de IA, así como realizar auditorías éticas periódicas por entidades independientes para evaluar algoritmos, datos, procesos y resultados en busca de sesgos, riesgos o diversos incumplimientos[289]. También es interesante crear canales accesibles, como pueden ser comunidades en línea para que empleados, clientes y el público en general puedan reportar inquietudes, sesgos observados u otros impactos éticos. También se aconseja que las PYMEs realicen evaluaciones de impacto algorítmico (AIA) y auditorías éticas cuando corresponda.

En quinto lugar, para empezar a utilizar estas herramientas, es fundamental: identificar cuáles son las tareas repetitivas o ineficientes que se realizan en tu empresa y que considerarías interesante que se realizasen mediante inteligencia artificial; evaluar las herramientas adecuadas en cada caso, y adaptarlas al sector que corresponda; formar al equipo de profesional que conforman la empresa, de forma que se familiaricen con este tipo de herramientas. Respecto a esto último, sería recomendable desarrollar planes de

[289] En este sentido, véase GIRALT HERNÁNDEZ, E., *Hacia una implementación ética e inclusiva de la Inteligencia Artificial en las organizaciones: un marco multidimensional*, abril 2024, pág. 8.

formación continua obligatorios en todos los niveles, combinando conocimientos técnicos de IA con modelos de ética, sesgos, privacidad y derechos humanos[290]. De otro lado, antes de implementar de forma real la IA dentro de la empresa, es recomendable empezar con pequeños proyectos piloto. Un ejemplo de un proyecto piloto puede ser comenzar a usar un chatbot para atención al cliente en nuestra página web, con el objetivo de responder preguntas frecuentes. Por último, es preciso comparar el impacto que tiene el uso de la IA en nuestra empresa, en comparación con los resultados que encontrábamos antes de su uso. Siguiendo el ejemplo del chatbot, podemos ver cómo en un período máximo de seis meses esta herramienta ha mejorado la rapidez de la respuesta y la satisfacción del cliente.

En sexto lugar, sería interesante crear una política de IA interna, configurando roles concretos, como un DPO (Delegado de Protección de Datos), o un responsable de IA. Un segundo elemento que componga la misma sería un registro de sistemas de IA utilizados en consumo. Por último, elaborar un procedimiento de respuesta concreto a reclamaciones de consumo mediante el uso de IA.

Por último, adjuntamos algunas recomendaciones en materia de emprendimiento que ofrecer a las PYMES: en caso de disponer de una tienda online, incluir recomendaciones personalizadas de productos, teniendo en cuenta las características de los potenciales usuarios; contratar servicios legales, financieros o educativos automatizados, que facilitan múltiples gestiones; solicitar los servicios de una consultoría especializada en datos o análisis de mercado utilizando IA; así como o utilizar asistentes virtuales especializados en nuestro sector.

4. Campañas de sensibilización: "IA segura para todos"

Son varias las iniciativas que han sido llevadas a cabo a nivel internacional con el objetivo de concienciar a la población de la necesidad de defender los derechos digitales. En este sentido, destaca la *Algorithmic Justice League* (AJL), ONG fundada por Joy Buolamwini ("Liga de la Justicia algorítmica"), que es una organización sin fines de lucro que utiliza la investigación, el artículo y la promoción de políticas para conciencias a la sociedad sobre el uso de la inteligencia artificial, así como los daños y los sesgos que la misma puede generar. Es realmente reseñable que el fundador de esta asociación colaboró con el especialista en ética de IA, Timnit Gebru, en aras a publicar un estudio en 2018 sobre el sesgo racial y de género en los algoritmos de reconocimiento facial utilizados por los sistemas comerciales de Microsoft, IBM, y Face++.

De otro lado, destacan campañas como la impulsada en América Latina que lleva por nombre "AI para Todos", que conecta tecnología e innovación para simplificar la vida cotidiana de los consumidores. Samsung fue quien lanzó esta campaña de marketing regional con el objetivo de fortalecer su posición como líder en Inteligencia Artificial en América Latina. A través de spots publicitarios, la campaña narra historias reales que muestran cómo la tecnología puede impactar positivamente en la vida diaria de las personas[291].

[290] Ídem.
[291] Fuente: Samsung Newsroom México.

Con un enfoque mucho más protector, algunas editoriales como *The New York Times, The Washington Post, The Guardian* y Vox Media, lanzaron una campaña publicitaria instando al gobierno de EE.UU. a proteger el contenido de la IA. Esta campaña, denominada *Support Responsible AI* (Apoyo a la IA Responsable), que surgió en 2023 y fue liderada por *News/Media Alliance* en EE. UU., incluye un enlace que nos dirige a la página de Apoyo a la IA Responsable, donde invita a los usuarios a conectar a sus representantes locales para exigir a las grandes tecnológicas que compensen justamente a escritores, artistas y periodistas por su trabajo[292]. En febrero, los principales periódicos de Reino Unido lanzaron una campaña similar, cubriendo sus portadas con la frase "*Make ir fair*" (Hazlo justo), como parte de una iniciativa que pedía a los lectores que ayudasen a proteger la IA del entrenamiento en contenido protegido por derechos de autor.

Teniendo como precedentes las diversas iniciativas llevadas a cabo en países vecinos, se propone a la Junta de Comunidades de CLM realizar su propia campaña de sensibilización que tenga por nombre *"IA Segura para Todos",* cuyo objetivo general sea concienciar a la ciudadanía, consumidores y pequeñas empresas sobre el uso responsable, seguro y ético de la IA, promoviendo la protección de sus derechos digitales y fomentando la confianza informada en esta tecnología. Dentro de los objetivos específicos se encuentra difundir información que sea clara, y de tipo accesible sobre la IA y cómo nos afecta la misma, promover buenas prácticas digitales para un uso seguro de la IA, así como estimular el pensamiento crítico frente a contenidos generador por IA.

Respecto al público objetivo, puede ser tanto la ciudadanía general, como consumidores digitales, responsables de menores usuarios de tecnología, PYMES y microempresas, así como técnicos municipales, educadores y agentes sociales. La duración podría ser de tres meses, y podría lanzarse la misma en la Semana de la Ciberseguridad, o la Semana Europea del Consumidor. El mensaje clave debe ser el siguiente: *"La inteligencia artificial y forma parte de tu día a día. Aprende a usarla de forma segura para proteger tus derechos, privacidad y bienestar".* Respecto a los componentes de la campaña, en primer lugar, vemos los materiales visuales y educativos. Dentro de ellos se incluirían guías prácticas, como *"IA para consumidores: lo que debes saber";* o "*IA en tu negocio: riesgos y oportunidades*". También se incluirán vídeos animados, o cápsulas informativas, a través de los cuales se clarifique el concepto de IA, qué ocurre con los datos, o como protegerse frente a fraudes con IA. Por último, también pueden crearse flyers digitales para redes y pantallas públicas que adviertan de los posibles riesgos de la IA, y que pueden llevar por título el siguiente: *"¿Fake o real? Cómo detectar contenidos falsos generados por IA".*

En segundo lugar, es preciso llevar a cabo acciones presenciales y digitales, como charlas ciudadanas en centros cívicos, bibliotecas o escuelas de adultos, así como talleres prácticos para PYMES y consumidores. Incluso pueden crear podcast en formato entrevista con expertos en IA, consumo y derechos digitales.

En tercer lugar, es preciso dar a conocer la campaña tanto en medios como en redes sociales. Para ello, deben crearse hashtags oficiales, como pueden ser

[292] Fuente: The Verge.

#IASeguraParaTodos, o *#TusDatosTuDecisión.* También es recomendable realizar publicaciones en redes como Facebook e Instagram, X (Twitter), LinkedIn, o WhatsApp. Por último, no se debe olvidar la difusión en radios locales y prensa digital que sigue siendo un medio utilizado sobre todo por personas de más avanzada edad.

En quinto lugar, sería interesante llevar a cabo una acción simbólica a través de un evento público, promoviendo un "Día de la IA Consciente", que sea tanto presencial como online, y permita el debate, así como microtalleres. Incluso pueden realizarse pruebas de herramientas de IA con guías, e incluso una firma de tip simbólico del compromiso ciudadano con la IA ética.

Por último, es preciso crear un sitio web de la campaña, con guías y vídeos descargables, recursos legales y de denuncia, mapa de talleres y actividades locales y un espacio para enviar preguntas, o situaciones vividas. Los principales indicadores de éxito de nuestra campaña será la tasa de reclamaciones resueltas por intervención humana, el % de empresas con aviso IA visible, el número de talleres realizados y participación en los mismos, el número de descargas de materiales, el alcance en redes sociales o incluso las encuestas de percepción de la IA antes y después de la campaña. Este tipo de acciones promueven alianzas con las OMICs, las asociaciones de consumidores y usuario, las universidades, los medios de comunicación locales, etc.

Se propone la creación de un protocolo de respuesta a incidentes: canal directo a la UT-IA y a OMICs para casos con componente IA, como el siguiente:

1. Objetivo

- Garantizar una respuesta rápida, coordinada y transparente ante incidentes de consumo relacionados con sistemas de IA.
- Facilitar la trazabilidad de las reclamaciones y la protección efectiva de los derechos de los consumidores.

2. Alcance

Aplica a incidentes en los que:

- Exista una decisión automatizada que afecte a consumidores (ej. precios dinámicos, denegación de servicios, publicidad personalizada).
- Se detecten riesgos de sesgo, discriminación o falta de transparencia en sistemas de IA.
- Se identifiquen brechas de seguridad o uso indebido de datos personales vinculados a IA.

3. Flujo de actuación

Paso 1. Recepción del incidente

- Consumidor → OMIC: presenta reclamación con evidencias (capturas, logs, comunicaciones).

- OMIC: registra el caso en su sistema interno y clasifica si hay componente IA.

Paso 2. Activación del canal directo

- Si se confirma componente IA, la OMIC activa el canal directo con la UT-IA.
- Se envía un informe inicial con:
    - Datos del consumidor (anonimizados si procede).
    - Descripción del incidente.
    - Evidencias aportadas.
    - Riesgos preliminares detectados.

Paso 3. Análisis técnico

- UT-IA: revisa logs, parámetros y documentación técnica del sistema implicado.
- Evalúa:
    - Transparencia y explicaciones significativas.
    - Cumplimiento normativo (AI Act, DSA, TRLGDCU, RGPD).
    - Riesgos éticos (sesgo, manipulación, exclusión digital).

Paso 4. Coordinación y respuesta

- UT-IA y OMIC: intercambian hallazgos y definen medidas correctivas.
- OMIC: comunica al consumidor la respuesta oficial, incluyendo:
    - Explicación clara del incidente.
    - Medidas adoptadas por la empresa/proveedor.
    - Recursos disponibles (revisión humana, compensación, arbitraje).

Paso 5. Escalado

- Si el incidente afecta a datos personales → derivación a AEPD.
- Si el incidente afecta a sistemas de IA de alto riesgo → derivación a AESIA.
- La UT-IA coordina con estas autoridades para asegurar coherencia en la respuesta.

4. Plazos orientativos

- Recepción y clasificación en OMIC: 5 días hábiles.
- Activación del canal UT-IA: inmediato tras confirmación de componente IA.
- Análisis técnico UT-IA: 15 días hábiles.
- Respuesta al consumidor: máximo 30 días naturales desde la reclamación inicial.

5. Roles y responsabilidades

- OMIC: punto de entrada, mediación y comunicación con el consumidor.
- UT-IA: análisis técnico especializado, coordinación con autoridades.
- Empresa/proveedor: entrega de documentación y colaboración en la investigación.
- AEPD/AESIA: supervisión en casos de datos personales o IA de alto riesgo.

6. Registro y trazabilidad

- Cada incidente se documenta en un expediente digital compartido entre OMIC y UT-IA.
- Se incluyen: reclamación inicial, evidencias, análisis técnico, medidas correctivas y comunicación final.
- Conservación mínima: 2 años para auditoría y seguimiento.

5. Papel de asociaciones y redes ciudadanas

Otra cuestión para analizar es la importancia de la figura de diversas asociaciones que luchan diariamente por los derechos de las personas ante la IA, de forma que sea no lesione ninguno de ellos. También destacaremos el papel de asociaciones que promueven la accesibilidad de las tecnologías, de forma que lleguen al mayor número de personas posible, independientemente de dónde vivan o el dinero que tengan.

El primer lugar, destaca la coligación de 17 organizaciones sociales conocida como *IA ciudadana*[293]*,* que exigieron el año pasado al Gobierno que la trasposición al ordenamiento jurídica español del AI Act se llevase a cabo "con más luces que sombras", con el objetivo de garantizar el mayor nivel de protección posible para la ciudadanía. Este reclamo se hizo a través de un acto organizado ante la sede del Ministerio de Transformación Digital y de la Función Pública, de forma que se instalaron enormes cajas transparentes en las que se podría leer "transparencia", "participación" o "supervisión y control"[294].

En segundo lugar, el marzo de 2023 se presentó la asociación *CIVICAI,* cuyo principal objetivo es sensibilidad a la sociedad sobre los impactos sociales y medioambientales de la IA, y hacer que esta tecnología esté al servicio de las personas y de la sociedad de manera equitativa y responsable. Es especialmente interesante que, con el fin de abordar los desafíos y oportunidades de la Revolución 4.0, esta asociación ha aprobado el Protocolo Cívico de Inteligencia Artificial, como marco conceptual y operativo para

[293] Es una coalición de organizaciones que trabajan para defender los derechos humanos en el contexto de las tecnologías digitales. Su objetivo es ampliar los espacios de participación de la sociedad en la regulación y en la gobernanza de la inteligencia artificial y los algoritmos, con el fin de conseguir que estas tecnologías promuevan la justicia social. Fuente: https://iaciudadana.org. Última fecha de consulta: 3 de octubre de 2025.

[294] Fuente: Siglo XXI, Diario digital independiente, plural y abierto.

enfrentar la era de GenAI y el futuro de la Inteligencia Artificial General[295]. En este sentido, destaca el foro *GOVERNAI*, que es un marco de colaboración entre la referida *CIVICAI,* su Consejo Social y las Administraciones públicas con el objetivo de que los planes de acción de todos los gobiernos en materia de IA incluyan también participación ciudadana. Dentro de las acciones planteadas, si incluye colaborar en el diseño de proyectos piloto que integren soluciones de IA.

En tercer lugar, destaca la organización sin fines de lucro *Partnership on AI,* cuyo compromiso está relacionado con el uso responsable de la IA, e investiga buenas prácticas para los sistemas de IA y para educar al público sobre su uso diligente.

Por último, destacamos la fundación Cibervoluntarios, que es una ONG española de referencia internacional, pionera en el voluntariado tecnológico, centrada en impulsar una transición digital inclusiva, y eliminar la brecha digital. Para ello, desde el año 2001 ayuda a las personas a usar y comprender la tecnología en su día a día de forma cercana, práctica y sencilla, realizando una media de 500 actividades de formación y sensibilización gratuitas anuales.

6. Cuadro de acción administrativa

Problema Detectado	**Normativa Aplicable**	**Recomendación Concreta**	**Nivel de Competencia (con artículo)**
Uso de sistemas de IA sin evaluación previa de riesgos éticos, legales y técnicos.	Reglamento (UE) 2022/2065 sobre servicios digitales y AI Act.	Implementar una auditoría interna de impacto algorítmico antes de desplegar cualquier sistema de IA.	Unión Europea – Artículo 114 del Tratado de Funcionamiento de la UE (TFUE), armonización del mercado interior.
Falta de formación específica en riesgos tecnológicos para emprendedores.	Ley 14/2013, de apoyo a los emprendedores y su internacionalización.	Incluir módulos obligatorios sobre riesgos tecnológicos y ciberseguridad en programas de formación para emprendedores.	Estado – Artículo 149.1. 30ª de la Constitución Española, competencia exclusiva en regulación de condiciones básicas de igualdad.
Escasa protección de datos personales en	Reglamento General de Protección de Datos (RGPD) y Ley Orgánica	Designar un Delegado de Protección de Datos	Unión Europea / Estado – Artículo 16 del TFUE

[295] Fuente: Salut. Generalitat de Catalunya.

Problema Detectado	Normativa Aplicable	Recomendación Concreta	Nivel de Competencia (con artículo)
soluciones de IA desarrolladas por startups.	3/2018 de Protección de Datos Personales.	(DPO) en startups que traten datos sensibles o a gran escala.	(protección de datos) y Artículo 149.1.1ª CE (derechos fundamentales).
Ausencia de mecanismos de supervisión regional para proyectos de IA con impacto social.	Estatutos de Autonomía y normativa autonómica sobre innovación y desarrollo tecnológico.	Crear oficinas autonómicas de supervisión ética de la IA para evaluar proyectos financiados con fondos públicos.	Comunidad Autónoma – Artículo 148.1.17ª CE, competencias en investigación científica y técnica.

Caso práctico nº 7

Elemento	Detalle
Situación Real	Startup en Castilla-La Mancha lanza una plataforma de empleo que usa IA para filtrar candidatos automáticamente.
Problema Detectado	Descartes automáticos sin transparencia ni revisión humana. Recogida de datos sensibles sin consentimiento explícito.
Normativa Aplicable	- RGPD (UE) – Artículo 22: decisiones automatizadas - Ley Orgánica 3/2018 – Artículo 20: derechos digitales - AI Act: ARTÍCULO 50. - CE – Artículo 149.1.1ª y 30ª
Impacto en Consumidores	- Discriminación algorítmica - Pérdida de oportunidades laborales - Vulneración de derechos fundamentales - Desconfianza en el uso de IA
Propuesta Autonómica	Crear un registro autonómico de sistemas de IA aplicados al empleo: - Auditorías éticas - Protocolos de transparencia - Formación empresarial - Supervisión por la Consejería competente
Prioridad	**Alta** – Por el impacto directo en derechos fundamentales y el crecimiento acelerado de la IA en el mercado laboral.

CAPÍTULO VII. PROPUESTAS NORMATIVAS Y PLAN DE ACTUACIÓN

1. Introducción y diagnóstico

La incorporación acelerada de sistemas de IA en los mercados de consumo genera riesgos específicos: opacidad en la fijación dinámica de precios, personalización comercial sin información adecuada, uso de modelos que toman decisiones automatizadas sin revisión humana efectiva, y proliferación de contenidos generados por IA que dificultan la identificación de publicidad.

En Castilla-La Mancha, las reclamaciones detectadas en sectores como comercio electrónico, turismo y servicios financieros muestran patrones recurrentes:
– falta de transparencia en algoritmos que determinan precios y rankings,
– dificultades para obtener una revisión humana de decisiones automatizadas,
– publicidad personalizada dirigida a menores,
– opacidad en *marketplaces* respecto a criterios de clasificación.

Sobre esta base, el presente capítulo estructura medidas priorizadas, diferenciando claramente entre:
a) Actuaciones normativas (modificación de la Ley 3/2019 y desarrollo reglamentario), y
b) Actuaciones organizativas de la Dirección General de Consumo.

El plan respeta las competencias autonómicas (información al consumidor, inspección y sanción en materia de consumo), evitando invadir ámbitos reservados al Estado (bases de protección de datos, supervisión de IA de alto riesgo o scoring crediticio) o a la futura AESIA.

2. Fichas normativas priorizadas

A continuación, se incluyen únicamente las obligaciones compatibles con competencias autonómicas y que aportan un valor efectivo al control de mercado.

Ficha 1. Transparencia en el uso de IA

Obligación: Informar cuando precios, recomendaciones, rankings o decisiones se basen total o parcialmente en IA. Procurar la accesibilidad para los consumidores vulnerables, en relación con el artículo 20 TRLGDCU.
Contenido mínimo: finalidad del sistema, factores generales, posibilidad de revisión humana.
Fundamento: artículo 97 bis TRLGDCU (información en *marketplaces*), artículo 50 AI Act (transparencia de sistemas). Control: inspección autonómica.

Ficha 2. Evaluaciones de Impacto Algorítmico (EIA/DIC) en el ámbito autonómico

Obligación: Las empresas que utilicen sistemas algorítmicos en sectores regulados por la Comunidad Autónoma (energía, transporte, vivienda, comercio minorista regulado, entre

otros) deben remitir a la Dirección General de Consumo un Documento de Información al Consumidor (DIC). Este documento es preceptivo cuando el sistema afecta a precios, rankings, recomendaciones o condiciones de acceso, en la medida en que dichas prácticas inciden directamente en la elección del consumidor.

Alcance limitado:

- El DIC no constituye una auditoría externa ni una Evaluación de Impacto Algorítmico en el sentido del AI Act (competencia estatal y europea).
- Se trata de un instrumento autonómico de transparencia, diseñado para reforzar la información al consumidor y permitir la supervisión administrativa de prácticas comerciales locales.
- Su finalidad es prevenir opacidad y manipulación en mercados regulados, garantizando que el consumidor disponga de datos básicos para comprender cómo se generan precios o recomendaciones.

Contenido mínimo del DIC:

1. Descripción del sistema algorítmico: finalidad, ámbito de aplicación y tipo de decisiones que influye.
2. Datos utilizados: categorías de datos, fuentes y criterios de tratamiento.
3. Riesgos identificados: posibles efectos adversos para los consumidores (discriminación, falta de transparencia, manipulación de elección).
4. Medidas internas de mitigación: controles humanos, mecanismos de revisión, protocolos de corrección de sesgos o errores.
5. Información accesible al consumidor: explicación clara y comprensible de cómo el sistema afecta a precios, rankings o recomendaciones.

Fundamento jurídico: La obligación se apoya en la competencia autonómica en materia de transparencia e información al consumidor, recogida en la Ley 3/2019, de Estatuto de las Personas Consumidoras de Castilla-La Mancha (arts. 8 y ss.). El objetivo es reforzar la protección preventiva en mercados donde la Comunidad Autónoma ostenta potestad reguladora.

Utilidad práctica:

- Transparencia preventiva: obliga a las empresas a documentar y comunicar cómo operan sus algoritmos en sectores sensibles.
- Supervisión administrativa: permite a la DG de Consumo detectar patrones de riesgo y requerir correcciones antes de que se produzcan daños.
- Empoderamiento del consumidor: facilita que los usuarios comprendan el impacto de la IA en precios y recomendaciones, evitando asimetrías de información.

- Complementariedad: no sustituye las obligaciones del AI Act ni del RGPD, pero añade un nivel autonómico de control en materia de consumo.

Ficha 3. Registro Autonómico de Sistemas de IA con impacto en consumo (CLM-IA)

Naturaleza: Registro meramente declarativo e informativo (sin efectos jurídicos vinculantes).
Finalidad: disponer de un censo de sistemas utilizados en comercio, turismo y servicios locales que incidan en precios o recomendaciones.
Documento exigible: ficha sencilla con proveedor, uso y medidas de transparencia adoptadas.
Compatibilidad: no se exige documentación del AI Act ni supervisión técnica.

Ficha 4. Derecho efectivo a la revisión humana

Obligación: Establecer un procedimiento que permita a la persona consumidora solicitar intervención humana, en relación con el artículo 16 quinques de la Directiva 2023/2673.
Fundamento: artículo 22 RGPD (decisiones automatizadas), artículo 86 AI Act (explicación).
Competencia autonómica: garantizar los derechos de información y atención al consumidor.
Facultad de la DG: ordenar la restitución de la situación jurídica a efectos contractuales o administrativos propios de consumo.

Ficha 5. Prohibición de targeting a menores y transparencia en precios personalizados

Obligación: Evitar campañas dirigidas a menores en sectores sensibles.
Fundamento: artículo 28.2 DSA (prohibición de targeting a menores), artículo 25 DSA (prácticas engañosas).
Transparencia: advertencia cuando el precio sea personalizado.

Ficha 6. Transparencia en marketplaces

Obligación: Información clara sobre ranking, remuneración por posicionamiento y parámetros principales. Fundamento: artículo 97 bis TRLGDCU.
Control: inspección autonómica.

Ficha 7. Etiquetado de contenidos generados por IA

Obligación: Identificar de forma visible los contenidos comerciales generados mediante IA. Fundamento: artículo 50 AI Act. Finalidad: prevenir engaño y reforzar la confianza.

Ficha 8. Apoyo a pymes

Medidas: guías de cumplimiento, plantillas de transparencia, asistencia técnica básica y servicio de resolución de dudas. Justificación: evita cargas desproporcionadas y facilita cumplimiento homogéneo. Debe tenerse en cuenta lo establecido en las guías de la AEPD y la AESIA.

Ficha 9. Régimen sancionador específico

Objeto: tipificar infracciones en materia de falta de información sobre sistemas de IA, publicidad personalizada ilícita y ausencia de revisión humana cuando sea obligatoria. Cobertura: Ley 3/2019 de CLM.

3. Proyecto de reforma normativa

3.1. Modificación de la Ley 3/2019 (Parte A)

Únicamente se incluyen preceptos estrictamente necesarios:

Artículo X bis. Información sobre el uso de IA en diversos sectores Obligaciones de transparencia en precios, rankings y decisiones automatizadas.

Artículo X ter. Derechos de las personas consumidoras frente a sistemas de IA Revisión humana, información reforzada, etiquetado.

Artículo X quater. Infracciones específicas en materia de normativa de consumo. Incumplimiento de transparencia, targeting a menores, ausencia de revisión humana, etiquetado incorrecto.

Disposición adicional sobre coordinación con AESIA.

Disposición adicional. Creación del Registro CLM-IA.

3.2. Proyecto de Decreto (Parte B)

Objeto: regular funcionamiento del Registro CLM-IA y definir procedimientos de remisión documental. Ámbito: sistemas que incidan en precios, recomendaciones o contenidos informativos. Naturaleza: puramente declarativa; no requiere documentación técnica del AI Act. Coherencia: evita duplicidad con AESIA o autoridades estatales. Además, el Registro CLM IA debe interoperar con bases de datos nacionales/europeas cuando sea posible.

4. Actuaciones estrictamente organizativas

Estas medidas no son derecho positivo, sino gestión administrativa interna:

– Formularios de triaje en OMIC para identificar casos con IA.
– Checklists para inspección (criterios de transparencia, información previa, etiquetas visibles).
– Guías de lenguaje claro y fichas informativas a consumidores.
– Formación inicial para personal inspector y OMIC.
– Registro interno de incidencias IA-consumo (no confundir con el registro oficial), y obligación de informes anuales de inspección autonómica.

5. Estrategia y cooperación institucional

Cooperación obligatoria:
– AEPD (por artículo 22 RGPD).
– AESIA (supervisión de sistemas de alto riesgo).
– CNMC (prácticas desleales o colusorias basadas en algoritmos).

Coordinación con autoridades de competencia autonómicas y con el Consejo de Consumidores y Usuarios.

Instrumentos: protocolos de remisión de información, coordinación en inspecciones y mecanismos de consulta.

6. Principio de proporcionalidad y evaluación de cargas

Las obligaciones autonómicas en materia de inteligencia artificial aplicada al consumo se diseñan bajo el principio de proporcionalidad, limitándose a los ámbitos de información, transparencia y atención al consumidor. Esto significa que las medidas autonómicas no invaden competencias estatales o europeas ni imponen cargas técnicas desproporcionadas. En concreto, se evita:

- Acceso a logs técnicos o trazas internas de los sistemas algorítmicos, cuya supervisión corresponde al AI Act y a autoridades estatales/europeas.
- Exigir auditorías de sistemas de alto riesgo, reservadas al marco europeo de evaluación de conformidad.
- Regular el scoring crediticio o la evaluación automatizada de solvencia, competencia vinculada al RGPD y al AI Act.
- Supervisar datasets de entrenamiento o la gobernanza de datos (art. 10 AI Act), que forman parte del régimen europeo de calidad y gestión de datos.

Alcance real de las obligaciones autonómicas

- Transparencia hacia el consumidor: obligación de remitir documentos de información claros (p. ej., DIC) cuando los algoritmos afecten a precios, rankings o recomendaciones.

- Derecho a atención humana efectiva: garantizar que los consumidores puedan acceder a un canal humano en caso de bloqueo por sistemas automatizados.
- Información comprensible: explicar de forma sencilla cómo los sistemas influyen en la decisión de compra o en la visibilidad de productos/servicios.

Evaluación de cargas

- Las medidas previstas se configuran como obligaciones de información y transparencia, no como auditorías técnicas complejas.
- Se mantiene un nivel bajo de carga administrativa, especialmente para pymes, al centrarse en documentación básica y accesible (descripción del sistema, datos utilizados, riesgos identificados y medidas de mitigación).
- El objetivo es equilibrar protección del consumidor y viabilidad empresarial, evitando costes excesivos y duplicación de controles ya previstos en el marco estatal y europeo.

7. Conclusión

El presente capítulo ofrece un marco realista, jurídicamente sólido y estrictamente competencial, que:

– refuerza la transparencia algorítmica;
– garantiza derechos del consumidor frente a decisiones automatizadas;
– evita duplicidades con el AI Act y la AESIA;
– ofrece instrumentos organizativos ajustados a la realidad autonómica;
– reduce cargas excesivas y clarifica prioridades.

El resultado es una política pública de consumo centrada en riesgos reales, proporcionada y plenamente aplicable.

CAPÍTULO VIII. HOJA DE RUTA Y CRONOGRAMA AUTONÓMICO (2025–2027)

1. Introducción

Este capítulo despliega la hoja de ruta operativa y el cronograma autonómico 2025–2027 para Castilla-La Mancha en materia de protección de las personas consumidoras en entornos digitales y sistemas basados en inteligencia artificial. La propuesta es coherente con los marcos y contenidos desarrollados en el resto del informe (Cap. II–VIII) y con los principios de transparencia, protección de datos, supervisión de algoritmos y garantía de intervención humana que en él se recogen.

La estrategia persigue tres fines estratégicos: (i) proteger derechos de las personas consumidoras, (ii) asegurar supervisión técnica y jurídica de los sistemas automatizados que impactan al consumo, y (iii) favorecer la innovación responsable y la cooperación interinstitucional dentro del marco competencial autonómico y europeo. Las medidas aquí propuestas se articulan respetando el Derecho de la Unión, especialmente las obligaciones sobre protección de datos y reglas sectoriales aplicables (p. ej. RGPD, AI Act, Espacio Europeo de Datos de Salud cuando proceda). Para la identificación y coherencia normativa se remite, a modo de ejemplo, al anteproyecto de Ley de Salud Digital de Cantabria que regula registros autonómicos, sandboxes y gobernanza del dato en el ámbito sanitario, como referencia técnica y de estructura organizativa.

2. Medidas a corto plazo (2025) — Prioridades y criterios de diseño

Las acciones de 2025 priorizan medidas de alto impacto en derechos de transparencia, información reforzada, control humano y mecanismos de respuesta rápida ante incidencias[296]:

a) Creación de la Unidad Técnica de Inteligencia Artificial para Consumo (UTIA-CLM) — Q1 2025

Descripción. Unidad técnica dependiente de la Consejería competente en consumo, compuesta inicialmente por personal técnico multidisciplinar (jurídico-administrativo, estadístico-datos, ingeniero/a de ML y experto/a en inspección). Funciones: (i) apoyo técnico a las actuaciones inspectoras, (ii) supervisión algorítmica de mercados y plataformas, (iii) elaboración de guías técnicas, (iv) coordinación con AESIA y organismos equivalentes en CCAA.
Justificación normativa. La creación de unidades técnicas especializadas responde a la necesidad práctica de traducir obligaciones del AI Act y del RGPD en criterios operativos para la inspección (responsabilidad proactiva, DPIAs, controles de sesgo).

[296] Destaca la Ley 3/2019 como fundamento competencial autonómico.

b) Guías técnicas y guías ciudadanas sobre consumo digital — Q2 2025

Publicación de:

- Guia técnica para inspección de sistemas de fijación dinámica de precios y rankings en marketplaces (criterios de evaluación de sesgos, transparencia de parámetros).
- Guía para consumidores sobre derechos frente a decisiones automatizadas (lenguaje claro, vías de reclamación).

Las guías se alinearán con los estándares europeos sobre "transparencia significativa" y con las mejores prácticas para la comunicación comprensible de decisiones apoyadas en IA. (Referencia conceptual: texto sobre obligaciones de explicabilidad del AI Act, en concreto su artículo 50 y el artículo 97 bis TRLGDCU).

c) Registro Autonómico de Plataformas Digitales con actividad en CLM — Q3 2025

Registro público (complementario a registros estatales o sectoriales, declarativo y complementario, sin efectos jurídicos vinculantes), con objeto de facilitar la supervisión, la cooperación interadministrativa y la trazabilidad de incidentes. Se diseñará interoperable con registros nacionales/sectoriales y con los mecanismos de la AESIA. (Coherencia con registros sectoriales previstos en anteproyectos autonómicos como el de Cantabria).

d) Protocolo OMIC de derivación y triaje de casos con IA — Q2 2025

Protocolo operable para las Oficinas Municipales de Información al Consumidor (OMIC): criterios de identificación de decisiones automatizadas; priorización de casos por riesgo (consumidores vulnerables, precios discriminatorios, publicidad engañosa programática); rutas de derivación a UTIA-CLM, AESIA o Fiscalía si hay indicios de delito. El protocolo se integrará en las fichas de empoderamiento ciudadanas y debe ser accesible, de forma que pueda ser comprendido por el consumidor vulnerable. (Procedimiento inspirado en esquemas de gobernanza y oficina de acceso recogidos en el anteproyecto de Cantabria).

e) Inspecciones conjuntas piloto con AESIA y CNMC — Q4 2025

Pilotos sectoriales (e-commerce, servicios financieros digitales, plataformas de alojamiento) con metodología común: definiciones de muestra, métricas de auditoría algorítmica (sesgo, variabilidad de precios, trazabilidad de decisiones) y emisión de actas técnicas. Coordinación con la AESIA y la CNMC para evitar solapamientos, teniendo en cuenta las competencias de la AESIA (la cooperación con AESIA es conforme al papel de dicha agencia en supervisión nacional, en base al RD 729/2023).

f) Campaña autonómica "Consumo Digital Seguro" — Septiembre 2025

Campaña pública focalizada en menores, personas mayores y entornos rurales. Objetivos: alfabetización sobre privacidad y decisiones automatizadas; difusión de guías ciudadanas y procedimientos de reclamación.

g) Convenios con universidades de Castilla-La Mancha — Q2 2025

Programas de formación práctica para personal inspector y OMIC (módulos técnicos en auditoría algorítmica y módulos jurídicos sobre protección de consumidores y protección de datos). Por tanto, se deberán incluir módulos sobre el RGPD y la DSA.

(La programación y contenidos se hallan en el documento original del capítulo; aquí se mejora la precisión de las responsabilidades y la referencia a las agencias competentes).

3. Medidas a medio plazo (2026–2027) — Consolidación estructural

a) Sandbox regulatorio autonómico en IA y consumo — Q1 2026

Espacio controlado para pruebas de sistemas de IA que afecten a precios, rankings o publicidad dirigida, con participación preferente de pymes (en relación con el artículo 57 del AI Act, referente a los espacios controlados de prueba). El sandbox exigirá garantías de supervisión humana, auditoría externa y planes de mitigación de riesgos. El diseño se articulará para permitir interoperabilidad y coordinación técnica con sandboxes nacionales y normas europeas (AI Act y recomendaciones sectoriales). (Modelo análogo al previsto en el anteproyecto de Cantabria para sandboxes en salud digital).

b) Sistema autonómico de etiquetado de algoritmos y servicios digitales — Q3 2026

Etiqueta destinada al consumidor que informe, en términos comprensibles, sobre: uso de IA, finalidad principal, nivel de riesgo evaluado y derechos del usuario (p. ej. posibilidad de intervención humana). La etiqueta será complementaria de las obligaciones del AI Act (como la del artículo 50 referente al marco de contenidos), e interoperable con otras etiquetas sectoriales.

c) Programa plurianual de formación avanzada (2026–2027)

Certificación autonómica en materia de consumo digital, supervisión algorítmica e inteligencia artificial, con módulos jurídicos, técnicos y sectoriales. Dirigido a inspectores, técnicos de OMIC y miembros de servicios municipales. Para ello, será recomendable una adecuada cooperación con la AESIA y la AEPD.

d) Herramientas tecnológicas de monitorización — Q3 2026

Desarrollo/integración de herramientas para: detección de prácticas de precios dinámicos abusivos; monitorización de publicidad programática; auditoría de rankings en marketplaces. Los criterios de detección se diseñarán con base en métricas reproducibles y verificables por peritos, en base a lo establecido en el artículo 22 del RGPDA, así como el artículo 28 de la DSA.

e) Red interautonómica de Consumo Digital — Desde 2026

Foro semestral de intercambio de mejores prácticas, protocolos y resultados de inspección entre CCAA, con participación de AESIA, AEPD, CNMC y organizaciones de consumidores.

f) Evaluación Autonómica de Riesgos de Consumo Digital (EARCD) — Q2 2027

Evaluación metodológica homologada que incluya análisis sectorial y territorial y la participación de asociaciones de consumidores y pymes.

g) Observatorio Autonómico de Consumo Digital — 2026–2027

Informes anuales y base de datos pública de incidencias algorítmicas, integrado técnicamente con el Registro Autonómico de Plataformas. (Estas iniciativas siguen el patrón de gobernanza y observación de riesgos que se exponen en el anteproyecto de Cantabria). Este observatorio debe ser interoperable con registros nacionales y europeos.

h) Sistema de subvenciones para proyectos municipales innovadores — Q2 2027

Subvenciones destinadas a iniciativas municipales de protección digital, alfabetización y monitorización local. Se deben priorizar proyectos de alfabetización digital y protección de menores.

4. Recursos y presupuesto estimado (Resumen operativo)

La implementación exige planificación plurianual y recursos humanos especializados. Las cifras que siguen son estimativas y deben ajustarse mediante memoria económica (cifras provisionales que deberán ajustarse en la memoria económica):

- 2025: 2,5 M€ — creación UTIA, guías técnicas, campañas, inspecciones piloto.
- 2026: 3,0 M€ — sandbox, etiquetado, formación avanzada, observatorio.
- 2027: 4,0 M€ — EARCD (competencias autonómicas de inspección e información), cooperación interautonómica, subvenciones municipales, consolidación.

Recursos humanos estimados:

- 2025: 5 técnicos especializados (UTIA).
- 2026: +10 inspectores con formación en consumo digital.
- 2027: +5 analistas de datos para Observatorio y EARCD.

Fuentes de financiación previstas: presupuesto autonómico ordinario, fondos europeos (Digital Europe, Horizon, FEDER) y posibles líneas de cofinanciación con AESIA y ministerios competentes.

5. Comparación con otras CCAA y la Unión Europea — Posición estratégica

Tras compendiar iniciativas autonómicas y europeas, Castilla-La Mancha puede situarse en posición avanzada adoptando medidas diferenciales y coordinadas:

- Otras CCAA han avanzado en estrategias de IA y transparencia (p. ej. Cataluña, País Vasco o Galicia, con la Ley 2/2025 de la IA en Administración) y en campañas de alfabetización (Andalucía, C. Valenciana), pero raramente han articulado un sandbox autonómico centrado en consumo, un registro público de plataformas con conexión operativa a observatorios, ni un etiquetado de algoritmos dirigido al consumidor, tal como se propone aquí. (Comparación inspirada en el análisis de iniciativas autonómicas y en el dispositivo de gobernanza propuesto por el anteproyecto de Cantabria en salud digital).

A nivel de la UE, los instrumentos jurídicos relevantes (AI Act; RGPD; EHDS para el ámbito sanitario) configuran obligaciones y estándares que deben integrarse de forma operativa en la Hoja de Ruta. Las medidas propuestas buscan esa integración práctica.

6. Cronograma resumido (2025–2027)

2025 — Q1: UTIA; Q2: guías y protocolo OMIC; Q2: convenios con universidades; Q3: registro autonómico; Sept.: campaña; Q4: inspecciones conjuntas.

2026 — Q1: sandbox regulatorio; Q1–Q4: formación avanzada; Q2–Q4: observatorio; Q3: etiquetado y herramientas de monitorización.

2027 — Q2: EARCD; Q2: apertura de subvenciones municipales; Q4: consolidación institucional.

Durante toda la ejecución: hitos de evaluación intermedia, como informes anuales de UTIA y Observatorio.

7. Conclusión (resumida y operativa)

La hoja de ruta 2025–2027 es coherente, viable y técnicamente sólida. Integra el marco competencial autonómico, responde a riesgos concretos derivados de la IA en el consumo, garantiza derechos de transparencia y explicabilidad y articula instrumentos operativos (UTIA, sandbox, registro, observatorio, protocolos OMIC) para supervisión, prevención y respuesta. Su diseño toma en consideración el articulado y la arquitectura de gobernanza que ya se propone en textos autonómicos afines (p. ej. anteproyecto de Ley de Salud Digital de Cantabria) y las obligaciones europeas vigentes (RGPD, AI Act, EHDS).

CAPÍTULO IX. CONCLUSIONES EJECUTIVAS

Síntesis final

Castilla-La Mancha se encuentra en una posición idónea para reforzar de manera efectiva la protección de las personas consumidoras frente al uso creciente de sistemas de inteligencia artificial en el mercado digital. El reto consiste en articular un plan autonómico ajustado a sus competencias, centrado en obligaciones de información, transparencia y atención al consumidor, acompañado de mecanismos de supervisión preventiva y de una coordinación multinivel con autoridades estatales y europeas.

El presente documento vincula los principales problemas detectados en el mercado regional —opacidad en precios personalizados y rankings, dificultad para obtener revisión humana de decisiones automatizadas, publicidad dirigida a menores y brecha digital creciente— con un conjunto acotado de medidas orientadas a resolverlos de forma efectiva. La estrategia se apoya en la jurisprudencia del TJUE (asuntos C-634/21, SCHUFA, y C-203/22, Dun & Bradstreet), que consolidan la exigencia de supervisión humana real y efectiva y de transparencia algorítmica. El plan combina actuaciones inmediatas de orientación y vigilancia con reformas organizativas y mecanismos de cooperación interadministrativa.

Ejes estratégicos 2025–2027

Acción inmediata en 2025

- **UTIA (Unidad Técnica de IA en Consumo):** Creación de un equipo técnico especializado en apoyo a inspectores, OMIC y órganos directivos. Sus funciones se limitan a análisis preliminar de riesgos en transparencia, revisión humana e información al consumidor; asesoramiento en expedientes; y coordinación con AESIA, CNMC y AEPD. No incluye auditorías técnicas ni acceso a registros internos de alto riesgo, competencias reservadas al Estado.
- **Guías y protocolos operativos:** Elaboración de guías dirigidas a operadores y OMIC para identificar precios personalizados, sistemas de recomendación, chatbots y decisiones automatizadas que afecten a derechos básicos del consumidor. Se vinculan al artículo 97 bis TRLGDCU y al artículo 50 AI Act, incluyendo plantillas de información y criterios de actuación en reclamaciones.
- **Sensibilización ciudadana:** Campañas informativas sobre derechos en materia de IA, con materiales accesibles para pymes, personas mayores y colectivos vulnerables. Se prioriza el lenguaje claro y la accesibilidad universal.
- **Inspecciones piloto:** Actuaciones de vigilancia específicas en comercio electrónico, turismo y servicios digitales, centradas en transparencia, información previa y publicidad permitida. La cooperación con organismos estatales (AESIA, CNMC) se limita al apoyo técnico, sin delegación de funciones exclusivas.

Consolidación estructural 2026–2027

- **Registro autonómico de sistemas de IA con impacto en consumo:** De carácter declarativo, sin efectos jurídicos vinculantes. Mejora la trazabilidad de sistemas que influyen en precios, recomendaciones o contenidos. No implica certificación técnica ni validación del diseño.
- **Observatorio digital de consumo:** Seguimiento de tendencias, precios dinámicos, personalización comercial, reclamaciones con componente de IA y perfiles de vulnerabilidad digital. Produce informes anuales y propuestas de mejora regulatoria, interoperables con registros nacionales y europeos.
- **Formación avanzada:** Programas de especialización para personal inspector y OMIC en decisiones automatizadas, sesgos relevantes, obligaciones de información y normativa aplicable. Se vincula a la Estrategia Nacional de IA y a programas europeos como Digital Europe.

Cooperación multinivel

La protección del consumidor ante sistemas de IA exige coordinación clara y respetuosa con la distribución competencial:

- **AESIA:** intercambio de información sobre prácticas de riesgo y criterios de transparencia.
- **CNMC:** cooperación en casos de afectación a la competencia y prácticas algorítmicas colusorias.
- **AEPD:** derivación de cuestiones relativas a decisiones automatizadas (art. 22 RGPD).
- **Otras comunidades autónomas:** armonización de criterios de inspección en comercio electrónico y plataformas digitales.
- **Consejo de Consumidores y Usuarios:** coordinación en la representación y defensa de intereses colectivos.

Gobernanza y responsabilidades

- **Unión Europea:** regulación del AI Act y políticas comunes de protección del consumidor digital. Castilla-La Mancha debe limitarse a información, transparencia y atención al consumidor, sin invadir competencias estatales en protección de datos o certificación técnica.
- **Estado:** normativa básica en consumo y protección de datos; supervisión de sistemas de alto riesgo a través de AESIA; vigilancia de competencia a cargo de CNMC.
- **Castilla-La Mancha:** transparencia en relaciones de consumo, supervisión de prácticas comerciales, inspección y sanción en su ámbito competencial; apoyo a OMIC; formación; observación del mercado digital.

Recomendaciones prioritarias

- Consolidar la **UTIA** como unidad de análisis y apoyo, sin funciones reservadas al Estado.
- Aprobar un **marco reglamentario claro** para el registro declarativo de sistemas con impacto en consumo.
- Publicar **guías prácticas** para empresas y OMIC sobre precios personalizados, publicidad dirigida a menores y decisiones automatizadas.
- Reforzar la **cooperación formal** con AESIA, CNMC y AEPD para evitar duplicidades.
- Desarrollar **campañas de alfabetización digital** dirigidas a personas mayores y pymes, en línea con la **Carta de Derechos Digitales**.
- Implantar un **sistema de seguimiento centrado en resultados**, con indicadores de accesibilidad y satisfacción ciudadana.

Indicadores de éxito y gestión de riesgos

Indicadores clave:

- Porcentaje de operadores que cumplen requisitos de información sobre uso de IA en precios, rankings o recomendaciones.
- Tiempo medio de revisión humana y resolución de reclamaciones automatizadas, incluyendo número de reclamaciones resueltas con intervención humana efectiva.
- Número de actuaciones inspectoras relacionadas con opacidad o publicidad ilícita.
- Participación de OMIC y empresas en programas formativos.
- Evolución de reclamaciones en zonas rurales y colectivos vulnerables.

Riesgos y mitigación:

- **Duplicidades competenciales:** mitigación mediante alineamiento estricto con el AI Act y coordinación con entidades estatales.
- **Carga para pymes:** mitigación mediante guías simplificadas y asistencia técnica.
- **Brecha digital:** mitigación con materiales en lenguaje claro y talleres locales.
- **Expectativas inadecuadas sobre supervisión técnica:** mitigación aclarando el alcance de las competencias autonómicas.

Mensaje final

Castilla-La Mancha dispone de una ruta clara y jurídicamente sólida para mejorar la protección del consumidor en un entorno digital impulsado por la inteligencia artificial. El plan propuesto se centra en las competencias autonómicas, evita cargas innecesarias para el tejido productivo y permite avanzar en transparencia, revisión humana e información veraz sin invadir ámbitos estatales o europeos. Su correcta implementación

fortalecerá la confianza ciudadana y la actuación administrativa en materia de consumo, contribuyendo a un mercado digital más justo, seguro y accesible para todos.

ANEXO FINAL DEL INFORME

IA Y PROTECCIÓN DE PERSONAS CONSUMIDORAS EN CASTILLA-LA MANCHA

Cuadro comparativo e integración normativa multiescalar

Este Anexo ofrece una síntesis comparada de competencias, riesgos y normativas aplicables en la protección de personas consumidoras frente a la IA, articulando los tres niveles competenciales: Unión Europea, Estado español y Comunidad Autónoma de Castilla-La Mancha. El contenido está fundamentado en las referencias jurídicas y doctrinales empleadas en los capítulos precedentes del informe.

I. COMPARATIVA MULTINIVEL: COMPETENCIAS, RIESGOS Y MARCO NORMATIVO

1. Unión Europea

Competencias y funciones:

- Competencia compartida en materia de consumo (artículo 4.2.f TFUE). Armonización del mercado interior (art. 114 TFUE).
- Armonización plena en contratos a distancia y mercados en línea (Directiva 2019/2161).
- Reglamentos directamente aplicables: RGPD, RSD (DSA), RMD (DMA), AI Act.
- Gobernanza europea: Oficina de IA, Consejo de IA, Foro consultivo y Grupo de expertos científicos (artículos 64 a 69 AI Act).

Riesgos de IA para los consumidores:

- Personalización opaca de precios y ofertas.
- Patrones oscuros en interfaces digitales.
- Publicidad segmentada discriminatoria.
- Riesgos sistémicos derivados de modelos de IA de uso general.

Normativa aplicable:

- **Tratado de Funcionamiento de la Unión Europea (TFUE)**, artículos 4, 12 y 169. Publicado en DOUE C 202 de 7 de junio de 2016 (versión consolidada).
- **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD). DOUE L 119, de 4 de mayo de 2016, p. 1–88.

- **Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022**, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales, DSA). DOUE L 277, de 27 de octubre de 2022, p. 1–102.
- **Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022**, sobre mercados disputables y equitativos en el sector digital y por el que se modifica el Reglamento (UE) 2019/1150 (Reglamento de Mercados Digitales, DMA). DOUE L 265, de 12 de octubre de 2022, p. 1–66.
- **Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019**, sobre la promoción de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. DOUE L 186, de 11 de julio de 2019, p. 57–79.
- **Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024**, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial, RIA). DOUE L 202, de 12 de julio de 2024, p. 1–152.
- **Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo, de 27 de noviembre de 2019**, por la que se modifican la Directiva 93/13/CEE, la Directiva 98/6/CE, la Directiva 2005/29/CE y la Directiva 2011/83/UE en lo que respecta a la mejora de la aplicación y la modernización de las normas de la Unión en materia de protección de los consumidores (Directiva Ómnibus). DOUE L 328, de 18 de diciembre de 2019, p. 7–28.
- **Directiva (UE) 2023/2225 del Parlamento Europeo y del Consejo, de 18 de octubre de 2023**, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 2008/48/CE. DOUE L 2023/2225, de 30 de octubre de 2023, p. 1–65.
- **Directiva (UE) 2023/2673 del Parlamento Europeo y del Consejo, de 22 de noviembre de 2023**, relativa a los contratos de servicios financieros celebrados a distancia y por la que se deroga la Directiva 2002/65/CE. DOUE L 2023/2673, de 27 de noviembre de 2023, p. 1–28.
- **Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2024**, relativa a la responsabilidad por productos defectuosos (revisión de la Directiva 85/374/CEE). DOUE L 2024/2853, de 29 de noviembre de 2024, p. 1–36.

2. Estado español

Competencias y funciones:

- Competencias estatales derivadas del artículo 149.1 CE (legislación civil, mercantil, procesal, bases del régimen económico, sanidad, régimen jurídico de las Administraciones Públicas). Artículo 51 CE como principio rector.
- Normativa básica: TRLGDCU, LCCC, LCCI, LOSSEAR, LCS.

- Gobernanza nacional: APLIA (Anteproyecto de Ley de gobernanza de la IA), AESIA (Agencia Española de Supervisión de Inteligencia Artificial), Secretaría de Estado de Digitalización e Inteligencia Artificial, ENAC.
- Funciones: régimen sancionador, espacios controlados de pruebas (sandboxes), alfabetización digital, designación de autoridades de vigilancia de mercado.

Riesgos de IA para los consumidores:

- Riesgos en crédito y seguros: scoring, evaluación de solvencia mediante IA, discriminación algorítmica.
- Sesgos y falta de transparencia en contratación digital.
- Opacidad en mercados y plataformas en línea.
- Defectos de productos con componentes de IA (responsabilidad civil objetiva).

Normativa aplicable:

- Constitución Española, artículos 51, 148, 149.
- TRLGDCU (Real Decreto Legislativo 1/2007).
- APLIA (Anteproyecto de Ley de Gobernanza de la IA).
- Real Decreto 729/2023 (Estatuto de la AESIA).
- Ley 20/2015 (LOSSEAR).
- Ley 50/1980 (LCS).
- Ley 3/1991 (LCD).
- Ley Orgánica 3/2018 (LOPDGDD).

3. Castilla-La Mancha

Competencias y funciones:

- Competencia autonómica en defensa de consumidores y usuarios (artículo 32.6 Estatuto de Autonomía de Castilla-La Mancha, LO 9/1982). Competencia de desarrollo legislativo y ejecución.
- Desarrollo normativo propio: Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras de Castilla-La Mancha.
- Límites competenciales: no puede innovar en materia contractual, procesal ni afectar a la unidad de mercado.
- Funciones posibles: alfabetización digital, formación de inspectores y personal OMIC, campañas de sensibilización, protocolos de actuación, coordinación con AESIA y Administración estatal.

Riesgos de IA para los consumidores:

- Falta de comprensión de precios personalizados y sistemas de recomendación.
- Manipulación algorítmica en interfaces digitales.
- Dificultad de reclamación ante decisiones automatizadas.
- Brecha digital y vulnerabilidad de colectivos sensibles (mayores, menores, personas con discapacidad, población rural).

Normativa aplicable:

- Estatuto de Autonomía de Castilla-La Mancha (LO 9/1982).
- Ley 3/2019, de 22 de marzo, del Estatuto de las Personas Consumidoras de Castilla-La Mancha.
- Jurisprudencia constitucional relevante: SSTC 26/2012, 54/2018, 3/2019, 72/2021, 20/2024, 119/2018.

II. SÍNTESIS DE RIESGOS, NORMATIVA Y DERECHOS DE LAS PERSONAS CONSUMIDORAS

Riesgo identificado	Normativa aplicable	Derecho del consumidor
Personalización opaca de precios y ofertas.	Artículos RGPD. 13–15, 22; TRLGDCU artículos 20, 97 bis; REGLAMENTO (UE) 2019/1150 artículo 5; artículo 28 DSA.	Derecho a información clara, acceso a datos, explicación significativa de la lógica aplicada.
Patrones oscuros en interfaces	Artículos DSA. 25; artículo 16 sexies Directiva 2011/83/UE, introducido por la Directiva 2023/2673.	Derecho a decisiones libres e informadas; prohibición de manipulación deliberada.
Publicidad segmentada discriminatoria	Artículo 26 de la DSA; artículo 9 del RGPD; artículo 5 de la LCD; artículo 28 DSA.	Derecho a no discriminación; transparencia y trazabilidad de la segmentación publicitaria.
Decisiones automatizadas sin revisión humana	Artículo RGPD. 22; artículo AI Act. 86; Directiva 2023/2673 artículo 16 quinquies. Jurisprudencia TJUE C-634/21 (SCHUFA) y C-203/22 (Dun & Bradstreet).	Derecho a intervención humana, a obtener explicación comprensible ya impugnar la decisión.

Riesgo identificado	Normativa aplicable	Derecho del consumidor
Responsabilidad por IA defectuosa	Directiva 2024/2853 (DRPD); LCS; Ley de Responsabilidad Civil por Productos Defectuosos.	Derecho a indemnización por daños materiales, personales y psicológicos.

III. ABREVIATURAS CLAVE CONSOLIDADAS

- RGPD: Reglamento (UE) 2016/679, General de Protección de Datos.
- RIA: Reglamento (UE) 2024/1689, de Inteligencia Artificial.
- RSD/DSA: Reglamento (UE) 2022/2065, de Servicios Digitales.
- RMD/DMA: Reglamento (UE) 2022/1925, de Mercados Digitales.
- REGLAMENTO (UE) 2019/1150: Reglamento (UE) 2019/1150, sobre equidad y transparencia para usuarios profesionales de plataformas.
- TRLGDCU: Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (RDLeg 1/2007).
- APLIA: Anteproyecto de Ley para la gobernanza de la Inteligencia Artificial en España.
- AESIA: Agencia Española de Supervisión de Inteligencia Artificial.
- ENAC: Entidad Nacional de Acreditación.
- LOSSEAR: Ley 20/2015, de ordenación, supervisión y solvencia de entidades aseguradoras y reaseguradoras.
- LCS: Ley 50/1980, de Contrato de Seguro.
- LCD: Ley 3/1991, de Competencia Desleal.
- LOPDGDD: Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.
- DRPD 2024: Directiva 2024/2853 sobre responsabilidad por productos defectuosos.
- FRIA: Evaluación de Impacto en Derechos Fundamentales.
- DIC: Declaración de Impacto en Consumo.
- OMIC: Oficina Municipal de Información al Consumidor.

IV. RESUMEN OPERATIVO PARA LA ACTUACIÓN AUTONÓMICA

Problema detectado	Normativa aplicable	Recomendación y nivel de competencia
Falta de información al consumidor sobre IA en la toma de decisiones (personalización, recomendación, clasificación).	RIA, RGPD, TRLGDCU, Ley 3/2019	Creación de una unidad técnica autonómica de información y asesoría. Campañas de concienciación. Integración en formularios OMIC. Formación de inspectores y personal técnico. (Ley 3/2019, artículos 5, 22, 41, 43, 44, 54, 100, 130-134). Las medidas son declarativas y de apoyo, sin invadir competencias estatales en materia de protección de datos.
Dificultad o ausencia de mecanismos efectivos de recuperación ante decisiones automatizadas.	Artículo AI Act. 86, RGPD artículo 22 Ley 3/2019	Refuerzo de protocolos OMIC para identificación y tramitación electrónica de incidencias derivadas de IA. Desarrollo de un Observatorio Autonómico sobre IA y Derechos del Consumidor. (Ley 3/2019, artículos 100, 108, 123 y ss.). Competencia plena.
Riesgo de discriminación algorítmica o sesgos en sistemas de IA.	Artículos AI Act. 10, 86; Artículo RGPD. 22; TRLGDCU; LCD; Directiva 2024/2853	Inspección y campañas informativas específicas sobre sesgos y alfabetización. Apoyo a auditorías y mecanismos de revisión humana garantizados. Competencia ejecutiva para inspección, sanción y mediación.
Uso de IA sin evaluación previa de riesgos éticos y legales.	RIA, DSA, REGLAMENTO (UE) 2019/1150, APLIA, Ley 3/2019, Ley 14/2013 de Emprendedores	Implementación de auditoría autonómica y protocolos de autoevaluación para empresas que desarrollan o implantan IA en consumo. Supervisión institucional transversal. Competencia coordinada con el Estado.

Problema detectado	Normativa aplicable	Recomendación y nivel de competencia
Tratamiento de datos personales sin consentimiento o sin base legal.	RGPD, LOPDGDD	Supervisión de tecnologías digitales. Competencia limitada, subordinada al marco estatal y europeo, pero con margen para actuación en información, prevención y protección.

V. FORMULARIOS Y PLANTILLAS ÚTILES PARA LA GESTIÓN DE DERECHOS VINCULADOS A IA

Se incorporan como anexos al presente informe los siguientes modelos normalizados, cuyo uso se recomienda a las OMIC, asociaciones de consumidores y personas interesadas, que deben ser adaptados a personas con discapacidad (lectura fácil, formatos accesibles, etc.):

1. Formulario de ejercicio del derecho de acceso a datos personales (artículo 15 RGPD).
2. Formulario de ejercicio del derecho de rectificación (artículo 16 RGPD).
3. Formulario de ejercicio del derecho de oposición (artículo 21 RGPD).
4. Formulario de ejercicio del derecho de supresión (artículo 17 RGPD).
5. Formulario de ejercicio del derecho a la limitación del tratamiento (artículo 18 RGPD).
6. Formulario de ejercicio del derecho a la portabilidad de datos (artículo 20 RGPD).
7. Formulario de ejercicio del derecho a no ser objeto de decisiones individuales automatizadas (artículo 22 RGPD y Considerando 50 AI Act).
8. Plantilla de triaje en reclamaciones de consumo relacionadas con inteligencia artificial (para uso en OMIC y asociaciones).
9. Modelo de requerimiento de información y documentación técnica sobre sistemas de IA (dirigido a empresas responsables, solo es exigible información básica de transparencia, no documentación técnica reservada al AI Act).
10. Modelo de análisis normativo reducido para casos de IA y consumo (para técnicos e inspectores).
11. Modelo de cadena de custodia de evidencias digitales para procedimientos de consumo.

VI. REFERENCIAS LEGISLATIVAS Y DOCTRINALES BÁSICAS

Se remite al cuerpo del informe ya los capítulos I, II, III, IV, V, VII y VIII para la relación completa y actualizada de normas, resoluciones administrativas y judiciales, y literatura doctrinal citada.

VII. CONCLUSIÓN

El marco jurídico vigente otorga a la Comunidad Autónoma de Castilla-La Mancha amplias competencias en el empoderamiento y protección efectiva de las personas consumidoras frente a los nuevos riesgos derivados de la inteligencia artificial. La coordinación multinivel (Unión Europea, Estado y Comunidad Autónoma), la integración transversal de la transparencia algorítmica, los mecanismos claros de recuperación y la formación de inspectores y personal de las OMIC resultan esenciales para garantizar una tutela real y efectiva.

La acción administrativa debe priorizar la prevención (formación, evaluación y sensibilización), con herramientas prácticas (observatorios, formularios, campañas sectoriales), y el refuerzo de la supervisión (auditorías, inspección, mediación, arbitraje), garantizando la centralidad de las personas consumidoras ante los retos y oportunidades de la inteligencia artificial.

ANEXOS

1. FORMULARIO DERECHO DE ACCESO DATOS PERSONALES

EJERCICIO DEL DERECHO DE ACCESO

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza nº …. C.Postal ……. Localidad …….. Provincia……Comunidad Autónoma…….

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico… por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

Que se le facilite gratuitamente el derecho de acceso por ese responsable en el plazo de un mes a contar desde la recepción de esta solicitud, y que se remita, a la dirección arriba indicada, la siguiente información:

- Copia de mis datos personales que son objeto de tratamiento por ese responsable.
- Los fines del tratamiento, así como las categorías de datos personales que se traten.
- Los destinatarios o categorías de destinarios a los que se han comunicado mis datos personales, o serán comunicados, incluyendo, en su caso, destinatarios en terceros u organizaciones internacionales.
- Información sobre las garantías adecuadas relativas a la transferencia de mis datos a un tercer país o a una organización internacional, en su caso.
-El plazo previsto de conservación, o de no ser posible, los criterios para determinar este plazo.
-Si existen decisiones automatizadas, incluyendo la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento.
-Si mis datos personales no se han obtenido directamente de mí, la información disponible sobre su origen.

La existencia del derecho a solicitar la rectificación, supresión o limitación del tratamiento de mis datos personales, o a oponerme a dicho tratamiento.
El derecho a presentar una reclamación ante una autoridad de control.

En .....a.....de.....de 20.....

Firmado

2. FORMULARIO DERECHO DE RECTIFICACIÓN

EJERCICIO DERECHO DE RECTIFICACIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de rectificación: C/Plaza nº ..... C.Postal .... …….. Localidad …….. Provincia…….. Comunidad Autónoma……..

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico…….. por medio del presente escrito ejerce el derecho de rectificación, de conformidad con lo previsto en el artículo 16 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

Que se proceda a acordar la rectificación de los datos personales, que se realice en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Datos sobre los que solicito el derecho de rectificación: …… ……

Que, en caso de que se acuerde que no procede practicar la rectificación solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda. Asimismo, en caso de que mis datos personales hayan sido comunicados por ese responsable a otros responsables del tratamiento, se comunique esta rectificación a los mismos. Se recomienda que acompañe al presente formulario un escrito en el que exponga de manera detallada todos los datos que permitan identificar el objeto de su pretensión

En .....a.....de.....de 20.....

Firmado:

3. FORMULARIO DERECHO DE OPOSICIÓN

EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: C/Plaza nº ..... C.Postal .... …….. Localidad…….. Provincia …….. Comunidad Autónoma ……..

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico… por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 21 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

La oposición al tratamiento de mis datos personales, teniendo en consideración que:

- El tratamiento de mis datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, debiendo limitarse el tratamiento de estos hasta que obtenga respuesta del ejercicio de este derecho.
- El interesado puede oponerse al marketing directo en cualquier momento.
- El tratamiento de mis datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, debiendo limitarse el tratamiento de estos hasta que se obtenga respuesta del ejercicio de este derecho.
- El tratamiento de mis datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos.

Sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades (en los dos primeros supuestos), o una misión realizada en interés público (en el tercer supuesto), acredito como situación personal para oponerme al tratamiento de mis datos personales …… …… ……

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, prorrogable dos meses en casos complejos (art. 12.3 RGPD).

En .....a.....de.....de 20.....

Firmado:

4. FORMULARIO DERECHO DE SUPRESIÓN

EJERCICIO DEL DERECHO DE SUPRESIÓN

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de supresión: C/Plaza nº ..... C.Postal .... Localidad Provincia Comunidad Autónoma

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico…….. por medio del presente escrito ejerce el derecho de supresión, de conformidad con lo previsto en el artículo 17 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

Que se proceda a acordar la supresión de sus datos personales en el plazo de un mes a contar desde la recepción de esta solicitud, y que se me notifique de forma escrita el resultado de la supresión practicada. Que en caso de que se acuerde que no procede practicar total o parcialmente la supresión solicitada, se me comunique motivadamente a fin de, en su caso, reclamar ante la Autoridad de control que corresponda. Que en caso de que mis datos personales hayan sido comunicados por ese responsable a otros

responsables del tratamiento, se comunique esta supresión. Siendo conocedor de que el derecho no aplica cuando el tratamiento sea necesario para obligaciones legales o defensa de reclamaciones.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, prorrogable dos meses en casos complejos (art. 12.3 RGPD).

En .....a.....de.....de 20.....
Firmado:

5. FORMULARIO DERECHO DE LIMITACIÓN

EJERCICIO DEL DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de limitación: C/Plaza nº ..... C.Postal .... …….. Localidad …….. Provincia ……..Comunidad Autónoma ……..

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico, por medio del presente escrito ejerce el derecho de limitación, de conformidad con lo previsto en el artículo 18 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

Que se limite el tratamiento de mis datos personales, teniendo en consideración:
Que el tratamiento es ilícito y me opongo a su supresión.
Que el responsable ya no necesita mis datos personales para los fines para los cuales fueron recabados, pero los necesito para la formulación, ejercicio o defensa de mis reclamaciones.
Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes, prorrogable dos meses en casos complejos (art. 12.3 RGPD), y que se comunique esta limitación a cada uno de los destinatarios que ese responsable del tratamiento haya comunicado mis datos personales. Se recomienda que acompañe al presente formulario un escrito en el que exponga de manera detallada todos los datos que permitan identificar el objeto de su pretensión.

En .....a.....de.....de 20.....

Firmado:

6. FORMULARIO DE DERECHO A LA PORTABILIDAD

EJERCICIO DEL DERECHO A LA PORTABILIDAD DE LOS DATOS

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza nº .... C.Postal .... Localidad ……. Provincia…. Comunidad Autónoma …….

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad, con domicilio en la C/Plaza ..... nº....., Localidad ..... Provincia ..... C.P. ..... Comunidad Autónoma ..... con D.N.I....., con correo electrónico …….....por medio del presente escrito ejerce

el derecho a la portabilidad de los datos, de conformidad con lo previsto en el artículo 20 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD).

AUTORIDAD COMPETENTE

.....

SOLICITA

Que se me faciliten en el plazo de un mes sus datos personales en un formato estructurado, de uso común y lectura mecánica. Siendo conocedor que el derecho solo aplica a tratamientos basados en consentimiento o contrato y realizados por medios automatizados.

En su caso, que los citados datos personales sean transmitidos directamente al responsable (especifíquese nombre o razón social), siempre que sea técnicamente posible.

En .....a.....de.....de 20.....
Firmado

7. FORMULARIO DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

EJERCICIO DEL DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALES AUTOMATIZADAS

DATOS DEL RESPONSABLE DEL TRATAMIENTO

Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que ejercita el derecho a la portabilidad de los datos: C/Plaza nº ..... C.Postal ..... Localidad …….. Provincia…….. Comunidad Autónoma ……..

DATOS DEL AFECTADO O REPRESENTANTE LEGAL

D./ Dª. ....., mayor de edad con domicilio en la C/Plaza .....

nº....., Localidad ..... Provincia ..... C.P. .....Comunidad Autónoma ..... con D.N.I....., con correo electrónico …….. por medio del presente escrito ejerce el derecho de oposición previsto en el artículo 22 del Reglamento (UE) 2019/1150, General de Protección de Datos (RGPD), así como lo establecido en el artículo 86 del Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial (RIA), y el Considerando 40 Directiva (UE) 2023/2673 (servicios financieros a distancia).

AUTORIDAD COMPETENTE

.....

SOLICITA

No ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que me produzca efectos jurídicos o me afecte significativamente de modo similar, atendiendo a las SSTJUE C 634/21 (SCHUFA) y C 203/22 (Dun & Bradstreet), que refuerzan el derecho a explicación y revisión humana, en particular en los siguientes aspectos:

Que se adopten las medidas necesarias para salvaguardar mis derechos y libertades, así como mis intereses legítimos, el derecho a la intervención humana y que pueda exponer mi punto de vista e impugnar la decisión, todo ello en el supuesto de que el tratamiento de mis datos personales se fundamente en la celebración o ejecución de un contrato, o bien en mi consentimiento explícito.

Que sea atendida mi solicitud en los términos anteriormente expuestos en el plazo de un mes.

En .....a.....de.....de 20.....

Firmado

8. PLANTILLA A: FORMULARIO TRIAJE EN UNA RECLAMACIÓN DE CONSUMO RELACIONADA CON INTELIGENCIA ARTIFICIAL

DATOS DEL CONSUMIDOR/A

- Nombre y apellidos: _____
- DNI/NIE/Pasaporte: _____
- Dirección: _____
- Teléfono de contacto: _____

- Correo electrónico: _____

A LA ATENCIÓN DE (DATOS DEL EMPRESARIO / EMPRESA / ENTIDAD RECLAMADA)

- Nombre comercial / razón social: _____
- CIF/NIF (si se conoce): _____
- Dirección o sede (si se conoce): _____
- Teléfono / contacto web (si se conoce): _____

DESCRIPCIÓN DE LOS HECHOS

(Describa de forma clara y resumida qué ha sucedido. Incluya fechas, productos/servicios implicados, nombres de plataformas, aplicaciones, o sistemas de inteligencia artificial involucrados, etc.)

_____
_____
_____
_____
_____

PROBLEMA RELACIONADO CON LA INTELIGENCIA ARTIFICIAL

☐ Uso indebido de datos personales por parte de un sistema de IA
☐ Toma de decisiones automatizadas sin intervención humana
☐ Discriminación algorítmica / sesgo en el tratamiento
☐ Falta de transparencia o explicabilidad del sistema de IA
☐ Imposibilidad de contactar con un responsable humano
☐ Incumplimiento del derecho de oposición / supresión
☐ Otro (especificar): _____

PRETENSIÓN DEL CONSUMIDOR/A

(¿Qué solución desea? Por ejemplo: reembolso, corrección, cese del uso de IA, acceso a información, indemnización, etc.)

_____

DOCUMENTACIÓN APORTADA (Adjuntar copias):

☐ Factura o justificante de compra
☐ Capturas de pantalla / comunicaciones electrónicas
☐ Condiciones del servicio / política de privacidad
☐ Reclamaciones previas enviadas a la empresa
☐ Otro (especificar): _____

REFERENCIA NORMATIVA APLICABLE

☐ RGPD
☐ AI Act
☐ TRLGDCU

OTRAS CUESTIONES

☐ Derivación a AESIA
☐ Derivación a AEPD.

En .....a.....de.....de 20.....

Firmado

Nota adicional:

Este formulario tiene como objetivo facilitar el análisis preliminar de una queja o reclamación en materia de consumo en relación con el uso de tecnologías de inteligencia artificial. Su presentación no sustituye el procedimiento oficial ante la OMIC u otras autoridades competentes. Base legal: Ley 3/2019 de Castilla-La Mancha como fundamento autonómico

9. PLANTILLA B: MODELO DE REQUERIMIENTO DE INFORMACIÓN Y DOCUMENTACIÓN TÉCNICA SOBRE SISTEMAS DE INTELIGENCIA ARTIFICIAL

DATOS DEL CONSUMIDOR/A

- Nombre y apellidos: _____
- DNI/NIE/Pasaporte: _____
- Dirección: _____
- Teléfono de contacto: _____
- Correo electrónico: _____

A LA ATENCIÓN DE (DATOS DEL EMPRESARIO / EMPRESA / ENTIDAD RECLAMADA RESPONSABLE DEL SISTEMA DE IA)

- Nombre comercial / razón social: _____
- CIF/NIF (si se conoce): _____
- Dirección o sede (si se conoce): _____
- Teléfono / contacto web (si se conoce): _____
- Dirección o contacto de

ASUNTO: Requerimiento de información y documentación técnica sobre sistema de inteligencia artificial que ha producido efectos sobre personas consumidoras

Me dirijo a ustedes, en mi condición de persona consumidora afectada (o interesada) por el uso de un sistema de inteligencia artificial implementado por su entidad, que ha generado efectos directos sobre mi situación como cliente/usuario, y posiblemente sobre otras personas consumidoras.

De conformidad con lo previsto en la normativa de protección de los derechos de las personas consumidoras, así como en aplicación de lo dispuesto en el Reglamento (UE) 2016/679 (RGPD), el Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial (RIA)y demás normativa sectorial, les requiero formalmente la siguiente información:

INFORMACIÓN REQUERIDA:

1. **Identificación del sistema de inteligencia artificial utilizado**
    - Denominación del sistema
    - Finalidad para la cual se utiliza
    - Ámbito de aplicación sobre personas consumidoras

2. **Naturaleza de la toma de decisiones**
    - Indicar si las decisiones fueron totalmente automatizadas o si existió intervención humana significativa
    - Descripción del tipo de decisión o impacto generado (por ejemplo: clasificación de usuarios, denegación de servicios, modificación de precios, etc.)
3. **Base legal y legitimación para el tratamiento automatizado**
    - Fundamento legal que ampara el uso del sistema de IA en el contexto de la relación de consumo
    - Referencia a las condiciones contractuales o políticas de privacidad aplicables
4. **Fuentes de datos utilizadas y variables consideradas**
    - Qué tipos de datos personales o no personales se utilizaron para entrenar o alimentar el sistema
    - Procedencia de dichos datos
    - Variables clave que determinan las decisiones
5. **Medidas adoptadas para garantizar la transparencia y explicabilidad**
    - Cómo se informa a las personas consumidoras sobre el uso de IA
    - Medios disponibles para obtener una explicación clara y comprensible de las decisiones tomadas por el sistema
6. **Mecanismos de revisión humana o reclamación**
    - Procedimiento habilitado para que los usuarios puedan impugnar decisiones automatizadas
    - Identidad o canal de contacto con la persona o equipo responsable del sistema
7. **Evaluaciones de impacto realizadas** (si aplica)
    - ¿Se ha realizado alguna evaluación de impacto en protección de datos (EIPD) o evaluación de impacto en derechos fundamentales?
    - ¿Se han detectado riesgos de sesgo, discriminación o perjuicio para las personas consumidoras?
8. **Política de auditoría, supervisión o rendición de cuentas del sistema de IA**

DOCUMENTACIÓN QUE SE SOLICITA:

- Copia o extracto del documento técnico explicativo del sistema de IA
- Información técnica resumida accesible para personas consumidoras (documentación de uso, glosarios, etc.)
- Política interna sobre uso ético de la IA
- Procedimiento de revisión o supervisión humana
- Informe de evaluación de impacto en derechos fundamentales (si existe)

Solicito que esta información me sea facilitada en plazo no superior a 30 días naturales en relación con RGPD y AI Act desde la recepción de la presente, en formato accesible y comprensible, sin perjuicio de ejercer otras acciones ante la Oficina Municipal de

Información al Consumidor (OMIC), autoridades de protección de datos o agencias sectoriales de supervisión tecnológica.

Agradezco de antemano su colaboración y quedo a la espera de su pronta respuesta.

Atentamente,

En .....a.....de.....de 20.....

Firmado

Nota adicional: el requerimiento no puede exigir documentación técnica reservada al AI Act, solo información básica de transparencia.

10. PLANTILLA C: MODELO DE ANÁLISIS NORMATIVO REDUCIDO

MODELO A

1. IDENTIFICACIÓN DEL CASO

- **Título del caso:**
  (Breve denominación descriptiva)
  Ejemplo: *Uso de IA para segmentación de precios en plataforma de e-commerce*
- **Entidad responsable / empresa implicada:**
- **Fecha del incidente o detección del sistema de IA:**
  ____ / ____ / _____
- **Ámbito del consumo afectado:**
  ☐ Comercio electrónico
  ☐ Servicios financieros
  ☐ Atención al cliente
  ☐ Telecomunicaciones
  ☐ Seguros
  ☐ Otros: _____

2. DESCRIPCIÓN BREVE DE LOS HECHOS

(Máx. 10 líneas – resumen del problema o situación detectada)

3. ELEMENTOS CLAVE DEL SISTEMA DE INTELIGENCIA ARTIFICIAL IMPLICADO

- **Tipo de sistema de IA:**
  ☐ Sistema automatizado de decisión
  ☐ Sistema predictivo
  ☐ Motor de recomendación
  ☐ Chatbot / asistente virtual
- **Finalidad declarada:** _____
- **Impacto sobre la persona consumidora:**
  ☐ Discriminación o trato desigual
  ☐ Denegación de servicios
  ☐ Alteración de precios o condiciones contractuales
  ☐ Uso indebido de datos personales
  ☐ Falta de transparencia / explicación insuficiente

4. MARCO NORMATIVO APLICABLE (SELECCIÓN REDUCIDA)

A) Derechos de las personas consumidoras

- **Texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU)**
  - Artículo 8: Derecho a la protección contra prácticas desleales
  - Artículo 60 y ss.: Información previa al contrato
  - Artículo 47: Cláusulas abusivas en contratos

B) Protección de datos personales

- **Reglamento (UE) 2016/679 (RGPD)**
  - Artículo 5: Principios de tratamiento (transparencia, minimización, etc.)
  - Artículo 13-14: Derecho de información y explicación
  - Artículo 15: Derecho de acceso del interesado
  - Artículo 16: Derecho de rectificación
  - Artículo 17: Derecho de supresión
  - Artículo 18: Derecho a la limitación del tratamiento
  - Artículo 19: Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento
  - Artículo 20: Derecho a la portabilidad de los datos
  - Artículo 21: Derecho de oposición.
  - Artículo 22: Decisiones automatizadas individuales

C) Normativa emergente sobre inteligencia artificial

- **Reglamento (UE) 2024/1689 (RIA)**

- Clasificación del sistema como “alto riesgo” (artículo 6 y 7)
- Obligaciones de transparencia (artículo 52)
- Evaluación de conformidad y derechos fundamentales

D) Otra normativa sectorial / transversal (si aplica)

- Reglamento 2022/2065 (DSA)
- Normas sectoriales (finanzas: Reglamento Delegado (UE) Nº 447/2012 de la Comisión, de 21 de marzo de 2012, por el que se completa el Reglamento (CE) nº 1060/2009 del Parlamento Europeo y del Consejo sobre las agencias de calificación crediticia; seguros: Ley 50/1980, de 8 de octubre, de Contrato de Seguro, BOE núm. 250, de 17 de octubre de 1980; energía: Ley 24/2013, de 26 de diciembre, del Sector Eléctrico, BOE 310, de 27 de diciembre de 2013; telecomunicación: Ley 11/2022, de 28 de junio, General de Telecomunicaciones, BOE núm. 155, de 26 de junio de 2022…)

5. AUTORIDAD COMPETENTE

- OMIC
- AEPD
- AESIA
- CNMC

6. VULNERACIONES POTENCIALES DETECTADAS

(Marca o resume las posibles infracciones que se observan)

☐ Falta de información clara y accesible sobre el uso de IA
☐ Ausencia de consentimiento o base legal para el tratamiento de datos
☐ Discriminación algorítmica o trato desigual no justificado
☐ Incumplimiento del derecho a revisión humana de decisiones
☐ Práctica comercial desleal o engañosa
☐ Cláusulas abusivas en contratos con consumidores
☐ Uso opaco o excesivo de datos personales
☐ Falta de medidas para minimizar sesgos o errores

7. CONCLUSIÓN Y RECOMENDACIÓN PRELIMINAR

(Análisis breve – ¿Qué acciones deberían considerarse?)

☐Reclamación formal ante OMIC
☐ Reclamación ante la AEPD (protección de datos)
☐ Solicitud de auditoría del sistema de IA
☐ Solicitud de retirada o modificación del sistema de IA
☐ Derivación a asociación de consumidores / soporte legal

8. DOCUMENTOS SOPORTE ADJUNTOS

☐ Capturas de pantalla o evidencias
☐ Reclamación previa a la empresa
☐ Condiciones del servicio / contrato
☐ Política de privacidad

9. FICHA TÉCNICA RESUMIDA (opcional)

Elemento clave	Descripción breve
Sistema de IA	[Nombre o tipo]
Empresa responsable	[Nombre]
Datos implicados	[Ej. personales, comportamiento, etc.]
Impacto principal	[Ej. discriminación, denegación, etc.]
Normas posiblemente vulneradas	[Listar 2–3 normas clave]
Acción propuesta	[Ej. reclamación, inspección, etc.]

MODELO B

I. HECHOS RELEVANTES

(Descripción clara y breve de los hechos. Incluir fechas, actores, tecnología implicada y efectos sobre la persona consumidora)

Ejemplo: El sistema de recomendación de una plataforma de seguros ajusta las primas de forma automática según perfiles de comportamiento, sin informar al consumidor ni ofrecer opción de revisión humana. La persona consumidora nota un aumento significativo sin explicación.

II. PREGUNTA JURÍDICA PRINCIPAL

(Cuál es la cuestión jurídica concreta que se quiere responder)

Ejemplo: ¿Puede una empresa ajustar condiciones contractuales (como precios) mediante decisiones automatizadas sin ofrecer información clara ni posibilidad de impugnación?

III. NORMATIVA GENERAL APLICABLE (LISTA BREVE)

- TRLGDCU (Texto Refundido Ley General de Defensa de los Consumidores y Usuarios)
- Reglamento (UE) 2016/679 (RGPD) – artículo 5, 13-15, 22
- Reglamento de Inteligencia Artificial (UE) 2024/XXX – artículos 5-7, 52
- Ley de Servicios Digitales (DSA)

IV. AUTORIDAD COMPETENTE

- OMIC
- AEPD
- AESIA
- CNMC

V. NORMATIVA SECTORIAL APLICABLE (SI PROCEDE, NO OBLIGATORIO)

1. Sector financiero

   - Ley 10/2014, de ordenación, supervisión y solvencia de entidades de crédito (LOSSEC), BOE núm. 156, de 27 de junio de 2014. (Regula bancos, cajas y cooperativas de créditos y establece requisitos de solvencia).
   - Real Decreto-ley 19/2017 (MiFID II), BOE núm. 287, de 25 de noviembre de 2017. (Recoge normas de transparencia y protección del inversor).

2. Sector asegurador

- Ley 20/2015 de ordenación, supervisión y solvencia de entidades aseguradoras y reaseguradoras (LOSSEAR), BOE núm. 168, de 15 de julio de 2015. (Establece requisitos de solvencia y gobierno corporativo).
- Ley 50/1980 del Contrato de Seguro. BOE núm. 250, de 17/10/1980. (Recoge el marco legal de las pólizas y relaciones asegurado-aseguradora).

3. Sector energético

- Ley 7/2021 de Cambio Climático y Transición Energética, BOE núm. 121, de 21 de mayo de 2021. (Incluye los objetivos de descarbonización y energías renovables)
- Reglamentos europeos de Energía y Mercado Interior (paquete *Clean Energy* 2019). En concreto, Reglamento (UE) núm. 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad DOUE, de 14 de junio de 2019. (Regula operaciones del mercado eléctrico, autoconsumo, agregadores, etc.).

4. Sector de telecomunicaciones

- Ley 11/2022 General de Telecomunicaciones, BOE núm. 155, de 29 de junio de 2022. (Recoge el marco actual de servicios electrónicos y redes).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE núm. 166, de 12 de julio de 2002. (Regula el comercio electrónico, empresas digitales, responsabilidad de intermediarios, etc.).
- Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) nº 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión, DOUE núm. 310, de 26 de noviembre de 2015. (Regula el acceso abierto y tratamiento igual del tráfico).

VI. JURISPRUDENCIA CLAVE

(Citas o referencias breves a resoluciones relevantes – judiciales o administrativas)

- SSTJUE – C-61/19, de 11 de noviembre de 2020; C-203/22, de 27 de febrero de 2025, sobre decisiones automatizadas y derecho a revisión
- AEPD – Resoluciones de 23 de septiembre de 2025, núm. expediente: 001-106829; de 20 de diciembre de 2024, núm. de expediente: 00001-00099010, sobre IA y falta de transparencia

- STEDH – Caso López Ribalda vs. España, de 17 de octubre de 2019 (principio de proporcionalidad tecnológica)

VII. ANÁLISIS JURÍDICO-TÉCNICO (EN VIÑETAS)

- El uso de sistemas automatizados que producen efectos significativos debe estar sujeto a información clara y opción de intervención humana (artículo 22 RGPD).
- Si el sistema de IA afecta a derechos contractuales, debe analizarse si se trata de una cláusula abusiva o práctica desleal (TRLGDCU).
- El AI Act clasifica como de alto riesgo aquellos sistemas que impactan sobre la vida económica de las personas (precios, condiciones, accesos).
- La falta de información comprensible sobre los criterios del algoritmo vulnera principios de transparencia y lealtad.
- La empresa debe prever mecanismos de revisión, reclamación y supervisión humana significativa.

VIII. CONCLUSIÓN PRÁCTICA Y MEDIDAS PROPUESTAS

(Resumen útil para la toma de decisiones administrativas o legales)

Se identifica una posible infracción en materia de transparencia y derechos del consumidor.
Se propone requerir a la empresa:
- ▫ Información técnica del sistema
- ▫ Justificación de legalidad del tratamiento
- ▫ Mecanismos de revisión o reclamación humana

Puede iniciarse procedimiento ante:
- ▫ OMIC (consumo)
- ▫ AEPD (protección de datos)
- ▫ Supervisores sectoriales (si aplica)

X. EVIDENCIA REQUERIDA

☐ Capturas de pantalla / mensajes del sistema
☐ Términos y condiciones del servicio
☐ Historial de precios / decisiones tomadas
☐ Reclamaciones previas a la empresa
☐ Política de privacidad y avisos legales
☐ Respuestas del sistema automatizado

X. RIESGOS DE EJECUCIÓN

(Posibles obstáculos o contingencias)

- Dificultad para acceder a información técnica del sistema (caja negra algorítmica)
- Reticencia empresarial a colaborar sin requerimiento formal
- Escasa jurisprudencia consolidada en el ámbito IA-consumo
- Dificultad para probar la discriminación o el perjuicio económico
- Limitaciones de recursos técnicos o periciales para evaluación externa

En ....., a.....de.....de 20.....

Firmado

11. PLANTILLA D: MODELO DE CADENA DE CUSTODIA DE EVIDENCIAS DIGITALES PARA PROCEDIMIENTOS DE CONSUMO

1. IDENTIFICACIÓN GENERAL

- **Número de expediente / referencia interna:** _____
- **Fecha de inicio de la cadena de custodia:** ____ / ____ / _____
- **Persona responsable del inicio:**
  Nombre: _____
  Cargo o relación con el caso: _____
  Firma: _____

2. DESCRIPCIÓN DE LA EVIDENCIA DIGITAL

Tipo de evidencia	Formato	Medio de obtención
☐ Captura de pantalla	PNG/JPG	Herramienta nativa / Snipping Tool
☐ Documento digital	PDF	Descargado desde plataforma
☐ Comunicación electrónica	EML / PDF	Cliente de correo (Outlook, Gmail)

Tipo de evidencia	Formato	Medio de obtención
☐ Registro de actividad	TXT / CSV	Exportado desde panel de usuario

3. INTEGRIDAD Y PRESERVACIÓN

- **Hash de verificación (si aplica):**
  (Utilizar SHA-256 / MD5 si es posible)
  Ejemplo: 3e2f1a73c7a894e9f1c0a2f5e91571e6bbef...
- **Medio de almacenamiento original:**
  ☐ Disco duro local
  ☐ Unidad USB
  ☐ Plataforma en la nube
  ☐ Dispositivo móvil
  ☐ Otro: _____
- **Formato de conservación actual:**
  ☐ Original sin modificaciones
  ☐ Copia autenticada / firmada digitalmente
  ☐ Exportación forense con metadatos preservados

4. TRANSFERENCIA / ACCESO A LA EVIDENCIA

Nº	Fecha	Persona que accede o recibe	Cargo / función	Motivo del acceso	Firma y hora
1	/				
2	/				

5. OBSERVACIONES / INCIDENCIAS

(Registrar cualquier cambio, error, alteración detectada o dificultad técnica)

---

6. CIERRE DE CADENA DE CUSTODIA

- **Fecha de cierre o archivo de evidencia:** ____ / ____ / _____
- **Destino final de la evidencia:**
  ☐ Adjuntada a expediente ante OMIC
  ☐ Enviada a autoridad competente

☐ Conservada en almacenamiento seguro
☐ Otro: _____

- **Persona responsable del cierre:**
  Nombre: _____
  Cargo o rol: _____
  Firma: _____

INSTRUCCIONES DE USO

- Este documento **debe acompañar a cada evidencia digital** presentada.
- Siempre que sea posible, realiza un **cálculo de hash (MD5/SHA-256)** para preservar la integridad (recomendación).
- Evita modificar el archivo original. Si haces copias, **registra la acción**.
- Firma esta ficha con fecha cada vez que se acceda, modifique, transfiera o archive la prueba.
- Si se entregan pruebas en soporte físico (USB, CD), registrar el número de serie o identificador del soporte.

12. PLANTILLA E: FICHA-EXPLICACIÓN PARA CONSUMIDORES

INFORMACIÓN SOBRE EL USO DE INTELIGENCIA ARTIFICIAL EN SU CASO

¿Por qué recibe esta información?

Usted ha sido parte de un proceso (compra, contratación, servicio digital, atención al cliente, etc.) en el que se ha utilizado un sistema de inteligencia artificial (IA). Esta ficha tiene como objetivo explicarle, de forma sencilla, qué es ese sistema, cómo se ha usado y cómo puede ejercer sus derechos como persona consumidora.

¿Qué es un sistema de inteligencia artificial (IA)?

Un sistema de IA es una tecnología que toma decisiones, ofrece recomendaciones o realiza análisis automáticamente a partir de datos. A veces, estas decisiones pueden afectarlo directa o indirectamente como consumidor, por ejemplo:

- Cambiar precios según su perfil o comportamiento

- Mostrarle ciertas ofertas y ocultar otras
- Denegarle un servicio o modificar condiciones automáticamente
- Atenderlo a través de chatbots o sistemas automáticos

¿Cómo se ha usado la IA en su caso?

Nombre del sistema (si se conoce): _____
Empresa responsable: _____
Tipo de decisión o acción tomada por la IA:
☐ Recomendación de productos/servicios
☐ Cambio de precio o condiciones de contrato
☐ Clasificación de su perfil como cliente
☐ Denegación automática de servicio
☐ Otro: _____

¿Se usaron sus datos personales?

Sí / No / No se ha especificado *(marcar lo que corresponda)*

En caso afirmativo:

- ¿Qué datos?: Nombre, historial de compras, localización, navegación web, otros
- ¿Para qué?: Entrenar el sistema de IA, personalizar su experiencia, tomar decisiones automatizadas

¿Qué derechos tiene usted?

Como persona consumidora, usted tiene derecho a:

- Ser informado de forma clara si se ha utilizado IA
- Solicitar una explicación comprensible sobre cómo se tomó una decisión automatizada
- Pedir la revisión humana de decisiones importantes (por ejemplo, si se le denegó un servicio)
- Oponerse al tratamiento de sus datos personales en ciertos casos
- Presentar una reclamación si considera que ha sido tratado de forma injusta o discriminatoria

¿Qué puede hacer ahora?

Si desea más información o no está de acuerdo con cómo se ha utilizado la IA:

1. Puede solicitar más detalles a la empresa.
2. Puede presentar una reclamación ante la OMIC (Oficina Municipal de Información al Consumidor).

3. Si se han usado sus datos sin su consentimiento o de forma incorrecta, puede reclamar ante la Agencia Española de Protección de Datos (AEPD).

Contactos útiles

- Nombre de la empresa / entidad responsable del sistema de IA: _____
- Correo o teléfono de contacto de atención al cliente: _____
- Oficina Municipal de Información al Consumidor (OMIC): _____
- Asociación de consumidores (si corresponde): _____
- Agencia Española de Protección de Datos (AEPD): www.aepd.es

Firma del profesional que entrega la información

Nombre: _____
Cargo: _____
Fecha: ____ / ____ / _____

13. PLANTILLA MODELO EVALUACIÓN DE IMPACTO ALGORÍTMICO

1. PARTE GENERAL.

1.1. Nombre del proyecto: _____
1.2. Descripción del proyecto: _____
1.3. Fase Actual: Seleccione una opción en relación con el momento temporal del proyecto:
☐Conceptualización y diseño.

☐Recolección y procesamiento de datos.
☐Uso y monitoreo
1.4. Razones para la automatización de este proceso.
Utilizar enfoques innovadores
El sistema realiza tareas que los humanos no podrían realizar en un periodo de tiempo razonable
Reducción de los costos de un programa existente
Mejorar la calidad general de las decisiones
1.5. ¿Es este proyecto una ampliación o adaptación de algún proyecto existente?
☐Sí
☐No
1.6. ¿El sistema de IA, incluido el modelo central, se basa en un modelo ya existente?
☐Sí
☐No
1.7. ¿Ha documentado con claridad la descripción del problema que busca resolver?
☐Sí
☐No

2. PROPORCIONALIDAD

2.1. ¿Se ha considerado detenidamente las opciones no algorítmicas que pueden utilizarse para lograr el mismo objetivo?
☐Sí
☐No
2.2. ¿Por qué se favorece la opción que implica un sistema basado en algoritmos? (Una opción)
Utilizar enfoques innovadores. El sistema realiza tareas que los humanos no podrían realizar en un periodo de tiempo razonable. Reducción de los costos de un programa existente. Mejorar la calidad general de las decisiones
2.3. ¿Ha revisado casos similares y sus impactos?
☐Sí
☐No
2.4. ¿Son los impactos que ha identificado reversibles?
☐Sí
☐No
2.5. ¿La aplicación del sistema tiene algún impacto en derechos humanos según la constitución?
☐Sí
☐No

3. NORMATIVA

3.1. ¿Se implementa el algoritmo para la ejecución de una normativa específica?

☐Sí

☐No

3.2. ¿Has identificado las normativas que pueden impactar en el sistema y el proyecto en el que se inserta?

☐Sí

☐No

4. LICENCIA SOCIAL

4.1. ¿El proyecto y/o sus objetivos están relacionados con temas de intenso debate público que podrían generar judicialización o peticiones administrativas?

☐Sí

☐No

4.2. ¿Se han diseñado mecanismos de participación ciudadana para recibir retroalimentación del sistema?

☐Sí

☐No

4.3. ¿Se han diseñado mecanismos para la difusión del sistema?

☐Sí

☐No

5. GOBERNANZA

5.1. ¿Existe alguna unidad interna encargada de supervisar la gobernanza (operación, manejo, despliegue) de la solución desarrollada?

☐Sí

☐No

5.2. ¿El equipo de desarrollo interno estará compuesto por un grupo diverso de personas en términos de raza, género, profesiones, edades y otros criterios sociodemográficos?

☐Sí

☐No

5.3. ¿Está documentado el proceso de toma de decisiones del sistema?

☐Sí

☐No

5.4. ¿Están todas las contrapartes internas identificadas?

☐Sí

☐No

6. PROTECCIÓN DE DATOS

6.1. ¿Utilizará el sistema datos personales como datos de entrada para la toma de decisiones automatizadas?

☐Sí

☐No

6.2. ¿Los datos son recogidos por sensores automatizados?

☐Sí

☐No

6.3. ¿Los datos utilizados vienen de entidades externas?

☐Sí

☐No

6.4. ¿Se aplica el principio de minimización de datos?

☐Sí

☐No

6.5. Se implementará el sistema para algunos de estos usos o casos:

a) Evaluación sistemática y exhaustiva de aspectos personales de los titulares de datos, basadas en tratamiento o decisiones automatizadas, como la elaboración de perfiles, y que produzcan en ellos efectos jurídicos significativos.

b) Tratamiento masivo de datos o gran escala.

c) Tratamiento que implique observación o monitoreo sistemático de una zona de acceso público.

d) Tratamiento de datos sensibles y especialmente protegidos, en las hipótesis de excepción del consentimiento.

☐Sí

☐No

6.6. Cuenta la entidad con procesos establecidos para el ejercicio de los derechos vinculados a los datos: ¿Acceso, Rectificación, Supresión, Oposición, Portabilidad e Impugnación a las decisiones automatizadas?

☐Sí.

☐Sí, pero solo parcialmente (Acceso, Rectificación, Supresión, Oposición)

☐No

6.7. ¿El sistema implica toma de decisiones automatizadas, incluida la elaboración de perfiles, que afecten significativamente a los titulares de datos, esto es, por ejemplo, en la negación de un beneficio, la asistencia sanitaria, evaluación de beneficios, acceso a servicios públicos, resolución de controversias, etc.?

☐Sí

☐No

6.8. ¿Se han diseñado medidas necesarias para asegurar explicaciones adecuadas para ayudar a los usuarios y otras personas afectadas a comprender el proceso de toma de decisiones o el funcionamiento del sistema?

☐Sí

☐No

7. CIBERSEGURIDAD

7. .1. ¿Forma parte su organización de la administración del Estado (Ministerios, las Delegaciones Presidenciales Regionales y Provinciales, los Gobiernos Regionales, las Municipalidades, las Fuerzas Armadas, las Fuerzas de Orden y Seguridad Pública, las empresas públicas creadas por ley, y los órganos y servicios públicos creados para el

cumplimiento de la función administrativa) o empresa del Estado en que éste tenga participación accionaria superior al 50% o mayoría en el directorio?

☐Sí

☐No

7.2. ¿Su organización presta servicios mediante redes y sistemas informáticos, y su afectación, interceptación, interrupción o destrucción tendría un impacto significativo en la seguridad y el orden público, en la provisión continua y regular de sus servicios, en el efectivo cumplimiento de las funciones del Estado o, en general, de los servicios que éste debe proveer o garantizar?

☐Sí

☐No

7.3. ¿Posee su organización una política de seguridad de la información o ciberseguridad?

☐Sí

☐No

7.4. ¿El sistema está siendo o será subcontratado a un tercero para su desarrollo o implementación?

☐Sí

☐No

7.5. ¿Ha implementado un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio?

☐Sí

☐No

7.6. ¿Ha evaluado los riesgos de ciberseguridad particulares que afectan a los sistemas de IA que gestiona la organización?

☐Sí

☐No

7.7. ¿Ha evaluado los riesgos específicos de ciberseguridad que pueda afectar el funcionamiento del sistema algorítmico?

☐Sí

☐No

8. EQUIDAD

8.1. ¿Utiliza el sistema datos que representen algunas de estas características: la raza o etnia, la nacionalidad, la situación socioeconómica, el idioma, la ideología u opinión política, la religión o creencia, la sindicación o participación en organizaciones gremiales o la falta de ellas, ¿el estado civil, la edad, la filiación o información sobre la enfermedades o discapacidades?

☐Sí

☐No

8.2. ¿La ley lo obliga a fundar sus decisiones en alguna de las características descritas anteriormente?

☐Sí

☐No

8.3. ¿El sistema utilizará datos de varias bases de datos o fuentes diferentes?

☐Sí

☐No

8.4. ¿El algoritmo fue desarrollado originalmente fuera de Chile o para un contexto distinto al propuesto?

☐Sí

☐No

8.5. ¿Está planificado realizar un análisis exploratorio inicial de los datos para evaluar la calidad, integridad, temporalidad, consistencia y posibles sesgos, daños potenciales e implicaciones de su uso?

☐Sí

☐No

9. TRANSPARIENCIA

9.1. ¿El algoritmo participa de una decisión que forma parte de un proceso administrativo?

☐Sí

☐No

9.2. ¿Se enmarca el sistema en alguna de estas finalidades: las áreas de educación, ¿empleo, servicios básicos, subsidios y ayuda económica, capacitación laboral, salud, seguridad pública, vivienda, protección social, autorizaciones o permisos administrativos?

☐Sí

☐No

9.3. ¿Sabrán los titulares que la decisión será mediada por un sistema de IA o tomada con base en algoritmos de IA?

☐Sí

☐No

9.4. ¿Existe una limitación técnica insalvable, acorde con el estado del artículo—por ejemplo, derivada de modelos de aprendizaje automático 'caja negra' en sistemas de decisiones automatizadas o semiautomatizadas— que impida entregar información sobre el funcionamiento y los resultados del algoritmo?

☐Sí

☐No

9.5. ¿El algoritmo estará protegido por derechos de propiedad intelectual de terceros desarrolladores?

☐Sí

☐No

☐No Aplica

9.6. ¿Será exigida la entrega de Código fuente al tercero desarrollador?

☐Sí
☐No
☐No aplica
9.7. ¿Se ha considerado algún mecanismo para que los usuarios internos o externos se comuniquen con la institución por los efectos o impactos que pueda producir el sistema?
☐Sí
☐No

10. RENDICIÓN DE CUENTAS

10.1. Indique las principales características del sistema a desarrollar:
☐Sistemas de reconocimiento y de detección de eventos
☐Predicción
☐Personalización
☐Soporte de interacción
☐Optimización
☐Razonamiento con estructuras de conocimiento
10.2. ¿El sistema automatizado va a ser utilizado reemplazando la toma de decisiones?
☐Sí
☐No
10.3. ¿El sistema para la toma de decisiones estará completamente automatizado?
☐Sí
☐No
10.4. ¿Se proporcionará un mecanismo para obtener retroalimentación de los usuarios durante la operación del sistema?
☐Sí
☐No
10.5. ¿Están planificadas auditorías algorítmicas?
☐Sí
☐No
10.6. ¿Existe algún diseño para atender requerimientos de información de usuarios externos respecto del sistema?
☐Sí
☐No
10.7. ¿Se ha planificado el resguardo de documentación técnica, minutas de reuniones, actas y en general de la documentación que vaya justificando las decisiones que se adopten en el proyecto?
☐Sí
☐No

En ....., a.....de.....de 20.....

Firmado

14. PLANTILLA MODELO DE SOLICITUD DE EXPLICACIONES SIGNIFICATIVAS

[Encabezado de la entidad solicitante]
Oficina Municipal de Información al Consumidor (OMIC)
[Dirección / contacto]
[Fecha]

A la atención de:
[Nombre de la empresa/proveedor/plataforma]
[Dirección / contacto

Asunto: Solicitud de explicaciones significativas sobre el uso de sistemas de Inteligencia Artificial en relación con [indicar servicio/producto]

En el marco de las competencias de protección y defensa de los consumidores, y conforme a lo dispuesto en el Reglamento Europeo de Inteligencia Artificial (AI Act), el Reglamento de Servicios Digitales (DSA) y el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios (TRLGDCU), se solicita a esa entidad que proporcione explicaciones significativas respecto al caso que se detalla a continuación:

1. Identificación del caso

Consumidor afectado: [Nombre / referencia]

Producto/servicio: [Descripción]

Fecha de la incidencia: [dd/mm/aaaa]

Tipo de decisión automatizada o sistema de IA implicado: [ej. recomendación de producto, denegación de crédito, moderación de contenido]

2. Solicitud de información

Se requiere que la entidad proporcione, de manera clara y accesible para el consumidor:

Finalidad del sistema de IA utilizado en el caso.

Criterios y variables principales que han sido considerados en la decisión automatizada.

Impacto esperado de dicha decisión en los derechos del consumidor.

Medidas de transparencia y explicabilidad aplicadas para garantizar que el consumidor pueda comprender el proceso.

Mecanismos de recurso o revisión humana disponibles para impugnar o solicitar reconsideración de la decisión.

Garantías de protección de datos personales y cumplimiento de la normativa vigente.

3. Plazo de respuesta

Se solicita que la información requerida sea remitida en un plazo máximo de **[15 días hábiles]**, en formato escrito y accesible, a la dirección de contacto indicada.

4. Advertencia legal

La falta de respuesta o la entrega de información incompleta podrá ser considerada como incumplimiento de las obligaciones de transparencia y protección de los consumidores, con las consecuencias legales que correspondan.

Atentamente,
[Firma / sello de la OMIC o del consumidor solicitante]

15. PLANTILLA MODELO DE ACUERDO SAAS CON CLÁUSULAS DE TRANSPARENCIA

ACUERDO DE PRESTACIÓN DE SERVICIOS DE SOFTWARE COMO SERVICIO (SaaS)

Entre:

Proveedor: [Nombre de la empresa proveedora], con domicilio en [dirección], representada por [nombre].

Cliente: [Nombre de la empresa/entidad contratante], con domicilio en [dirección], representada por [nombre].

Ambas partes acuerdan lo siguiente:

1. Objeto del contrato

El proveedor se compromete a poner a disposición del cliente el acceso al software [nombre del SaaS] bajo modalidad de servicio en la nube, conforme a las condiciones establecidas en este acuerdo.

2. Duración y renovación

El contrato tendrá una duración inicial de [X meses/años].

Se renovará automáticamente salvo notificación expresa con [30 días] de antelación.

3. Cláusulas de transparencia

El proveedor se compromete a garantizar la máxima transparencia en la prestación del servicio, en relación con lo establecido en el Reglamento 2022/2065, incluyendo:

- Información clara sobre el funcionamiento del software: descripción de algoritmos, procesos automatizados y limitaciones técnicas.
- Acceso a documentación técnica y funcional: manuales, guías de uso y actualizaciones.
- Notificación previa de cambios relevantes: modificaciones en funcionalidades, precios o condiciones contractuales con al menos [30 días] de antelación.
- Explicaciones significativas en decisiones automatizadas, teniendo en cuente lo establecido en el artículo 22 del RGPD y el artículo 50 del AI Act: cuando el software utilice IA o algoritmos que afecten al cliente o a sus usuarios, se proporcionará información comprensible sobre los criterios utilizados.
- Transparencia en costes y facturación: desglose detallado de tarifas, impuestos y posibles cargos adicionales.
- Registro de incidencias y métricas de servicio: acceso a informes periódicos sobre disponibilidad, rendimiento y seguridad.

4. Protección de datos

El proveedor actuará como encargado del tratamiento de los datos personales conforme al artículo 28 del RGPD y a la LOPDGDD.

Se garantizará la confidencialidad, integridad y disponibilidad de los datos.

Se informará al cliente de cualquier brecha de seguridad en un plazo máximo de 72 horas.

5. Niveles de servicio (SLA)

Disponibilidad mínima garantizada: [99,5 %].

Tiempo máximo de respuesta a incidencias críticas: [4 horas].

Penalizaciones en caso de incumplimiento: [descuento o compensación].

6. Derechos del cliente

Derecho a recibir información clara y accesible sobre el servicio.

Derecho a exportar sus datos en formato interoperable en cualquier momento.

Derecho a rescindir el contrato si el proveedor incumple las obligaciones de transparencia o seguridad.

7. Resolución de conflictos

Las partes se comprometen a resolver cualquier conflicto mediante mediación previa en [OMIC / entidad de consumo], antes de acudir a la vía judicial.

Se podrá acudir a la Junta Arbitral de Consumo como mecanismo extrajudicial.

8. Legislación aplicable

Este contrato se regirá por la legislación española y europea aplicable en materia de consumo, servicios digitales y protección de datos.

Firmas:

Proveedor: _____

Cliente: _____

16. PLANTILLA MODELO DIC (DECLARACIÓN DE IMPACTO PARA EL CONSUMIDOR)

DECLARACIÓN DE IMPACTO PARA EL CONSUMIDOR

Entidad responsable:
[Nombre de la empresa/proveedor]
[Dirección / contacto]
[Persona responsable del cumplimiento]

Fecha de elaboración: [dd/mm/aaaa]
Versión: [número]

1. Identificación del sistema

Nombre del servicio/producto: [ej. Motor de recomendación de productos]

Tipo de tecnología utilizada: [IA, algoritmos de precios dinámicos, moderación automatizada, etc.]

Ámbito de aplicación: [sector, mercado, usuarios afectados]

2. Finalidad y beneficios esperados

Objetivo principal del sistema: [ej. mejorar la experiencia de compra, personalizar contenidos]

Beneficios para el consumidor: [ej. acceso más rápido a productos relevantes, precios ajustados]

Beneficios para la empresa: [ej. optimización de ventas, reducción de costes]

3. Riesgos identificados para los consumidores (artículo 27 AI Act)

Transparencia: ¿Se informa claramente de cómo funciona el sistema?

Sesgos y discriminación: ¿Puede afectar de forma desigual a ciertos grupos?

Privacidad y protección de datos: ¿Qué datos se recogen y cómo se protegen?

Manipulación o presión comercial: ¿Existen prácticas que puedan limitar la libertad de elección?

Accesibilidad: ¿El sistema es comprensible para todos los perfiles de consumidores?

4. Medidas de mitigación y garantías

Explicaciones significativas: [ej. mensajes claros sobre criterios de recomendación o variación de precios]

Derecho a recurso humano: [ej. posibilidad de revisión manual de decisiones automatizadas]

Protección de datos: [ej. cifrado, minimización de datos, anonimización]

Información accesible: [ej. política de uso publicada en lenguaje claro]

Supervisión y auditoría: [ej. revisiones periódicas de sesgo y transparencia]

Obligación de accesibilidad conforme a la Directiva (UE) 2019/882 sobre accesibilidad de productos y servicios.

5. Impacto esperado en derechos de los consumidores

Derecho	Posible impacto	Medidas de protección
Información veraz	*Riesgo de opacidad* TRLGDCU artículos 60 y 97 bis.	Política de transparencia y explicaciones significativas
Igualdad	*Riesgo de sesgo* Carta de Derechos Fundamentales UE artículo 21.	Auditoría de algoritmos y revisión de datos de entrenamiento
Privacidad	*Riesgo de uso excesivo de datos* RGPD artículos 5 y 22.	Minimización y consentimiento informado
Libertad de elección	*Riesgo de manipulación* DSA artículo 25.	Prohibición de dark patterns, mensajes claros
Seguridad	*Riesgo de brechas* RGPD artículo 32.	Protocolos de seguridad y notificación en 72h

6. Procedimiento de revisión y actualización

Periodicidad de revisión: [ej. anual / semestral]

Responsable de seguimiento: [nombre / cargo]

Mecanismos de participación del consumidor: [ej. canal de reclamaciones, encuestas de satisfacción]

7. Conclusión

La entidad declara que ha evaluado el impacto del sistema sobre los consumidores, ha identificado riesgos y ha adoptado medidas de mitigación para garantizar el respeto de sus derechos conforme al AI Act, DSA, TRLGDCU y RGPD.

Firma y sello de la entidad responsable
[Nombre / cargo]
[Fecha]

17. MODELO CHECKLIST DE "DARK PATTERNS" EN INTERFACES.

1. Consentimiento y privacidad (Directiva 2023/2673 art. 16 sexies, prohibición de *dark patterns* en interfaces financieras).

☐ ¿El consentimiento para cookies o datos está claramente diferenciado entre Aceptar y Rechazar?

☐ ¿Se evita el uso de botones engañosos (ej. Aceptar en color llamativo y Rechazar oculto)?

☐ ¿Se informa de forma clara sobre qué datos se recogen y para qué?

☐ ¿El usuario puede retirar su consentimiento con la misma facilidad con la que lo otorgó?

2. Diseño de elección (el preseleccionado por defecto está prohibido por la Directiva 2019/2161)

☐ ¿Las opciones están presentadas de manera equilibrada, sin sesgos visuales que induzcan a una preferencia?

☐ ¿Se evita el "pre-seleccionado por defecto" en suscripciones o compras adicionales?

☐ ¿Se ofrece siempre una opción gratuita o básica cuando corresponde?

☐ ¿El lenguaje es claro y no induce a error (sin dobles negaciones ni tecnicismos confusos)?

3. Proceso de compra (TRLGDCU artículo 20, información precontractual).

☐ ¿Se evita la presión artificial ("quedan 2 unidades", "otros usuarios están mirando ahora")?

☐ ¿No se añaden costes ocultos al final del proceso (ej. tasas no informadas)?

☐ ¿El botón de "Cancelar" o "Volver" es tan visible como el de "Comprar"?

☐ ¿Se informa claramente de las condiciones de devolución y garantía antes de la compra?

4. Suscripciones y cancelaciones (TRLGDCU artículo 97 bis, información en *marketplaces*).

☐ ¿El proceso de alta y baja es simétrico en facilidad y pasos?

☐ ¿No se ocultan las opciones de cancelación en menús complejos?

☐ ¿Se informa de forma clara sobre la renovación automática y cómo desactivarla?

☐ ¿Se evita el "rodeo" de confirmaciones múltiples para cancelar?

5. Interacción y comunicación

☐ ¿No se utilizan notificaciones intrusivas o repetitivas para forzar la acción del usuario?

☐ ¿Se evita el uso de mensajes emocionales manipulativos ("Tus amigos te echarán de menos si cancelas")?

☐ ¿El diseño respeta la accesibilidad (contraste, legibilidad, navegación sencilla)?

☐ ¿Se ofrece siempre un canal de contacto claro para dudas o reclamaciones?

6. Evaluación ética y legal (obligación de auditoría periódica conforme al art. 64 AI Act, supervisión)

☐ ¿La interfaz cumple con el DSA y la normativa de consumo (TRLGDCU)?

☐ ¿Se han evaluado los riesgos de manipulación o discriminación en el diseño?

☐ ¿Existe un procedimiento interno para revisar periódicamente la interfaz y detectar dark patterns?

☐ ¿Se documentan las decisiones de diseño y sus justificaciones?