

# Reclamar tus derechos en la era algorítmica: barreras y propuestas

Mayo, 2026

**Investigación realizada por el equipo investigador de ALIA - Associació Cultural de Dones per a la Recerca i l'Acció (Mireia Orra i De Salsas, Alex Haché y Eva Cruells López) y coordinada por Political Watch con la colaboración de IA Ciudadana.**

Esta investigación se realizó en el marco del Convenio que la entidad pública empresarial Red.es ha suscrito con la agrupación de entidades formada por Political Watch (Fundación Salvador Soler), la Fundación Hay Derecho y la Fundación Haz, para impulsar la implementación de la Carta de Derechos Digitales en el ámbito de los derechos de participación [c-38/23-ot].

## ÍNDICE

<b>RESUMEN EJECUTIVO</b> .....	<b>1</b>
<b>INTRODUCCIÓN</b> .....	<b>4</b>
Concepto de las vulneraciones derivadas del uso de sistemas algorítmicos o de IA.....	4
Daños y derechos afectados.....	6
<b>BLOQUE I: EL MARCO LEGAL Y SUS LÍMITES</b> .....	<b>8</b>
<b>Ámbito internacional</b> .....	<b>8</b>
<b>Ámbito europeo</b> .....	<b>9</b>
Reglamento de Protección de Datos (2016/679).....	9
Reglamento de Servicios Digitales (2022/2065).....	10
Reglamento de Inteligencia Artificial (2024/1689).....	12
<b>Ámbito español</b> .....	<b>14</b>
Carta de Derechos Digitales.....	15
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.....	16
Proyecto de Ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación (121/000068).....	18
Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial.....	19
Normativas sectoriales.....	21
<b>Estudios de caso en Europa</b> .....	<b>22</b>
Défenseur des droits y decisiones automatizadas en los servicios públicos (Francia)....	22
Acciones colectivas de reparación frente a sistemas algorítmicos por parte de Noyb (UE)	23
<b>Conclusiones del análisis normativo y los estudios de caso</b> .....	<b>25</b>
<b>BLOQUE II: RESULTADOS Y HALLAZGOS DE LA FASE CUALITATIVA</b> .....	<b>27</b>
<b>Barreras de acceso a mecanismos de reclamación</b> .....	<b>27</b>
Opacidad técnica: las cajas negras algorítmicas.....	27
Falta de notificación y reconocimiento del componente algorítmico.....	27
Carga individual y asimetría de poder.....	28
Complejidad procedimental y fragmentación de responsabilidades.....	28
Desconfianza institucional y barreras culturales.....	29
Temporalidad y urgencia del daño.....	29
<b>Buenas prácticas identificadas</b> .....	<b>29</b>
<b>Malas prácticas identificadas</b> .....	<b>30</b>
<b>Recomendaciones clave emergentes del proceso</b> .....	<b>31</b>
<b>BLOQUE III: GUÍA PRÁCTICA PARA LA PUESTA EN MARCHA DE PROCESOS PARTICIPATIVOS PARA CREAR SISTEMAS DE RECLAMACIÓN</b> .....	<b>34</b>
Principios transversales: enfoque de derechos humanos.....	34
Cómo usar esta guía.....	35
Antes de empezar: diagnóstico y mapa del ecosistema.....	35
<b>Ventanilla única (one stop shop)</b> .....	<b>37</b>
Qué es y por qué es necesaria.....	37

Hoja de ruta: fases del proceso.....	38
Diseño híbrido: presencial y digital.....	39
Ejemplos y referencias.....	40
<b>Autoridades e instituciones.....</b>	<b>41</b>
Por qué las autoridades necesitan adaptarse.....	41
Mapa de autoridades y sus competencias.....	41
Hoja de ruta para autoridades.....	42
Adaptación de procedimientos.....	43
Ejemplos y referencias.....	44
<b>Organizaciones de la sociedad civil.....</b>	<b>45</b>
El rol de las organizaciones en el ecosistema.....	45
Hoja de ruta para organizaciones.....	45
Acompañamiento comunitario efectivo.....	46
Herramientas de alfabetización algorítmica.....	47
Ejemplos y referencias.....	48
<b>RECOMENDACIONES FINALES.....</b>	<b>49</b>
<b>SOBRE LA INVESTIGACIÓN.....</b>	<b>51</b>
<b>ANEXOS.....</b>	<b>52</b>

## RESUMEN EJECUTIVO

En un contexto de uso generalizado de herramientas tecnológicas, los sistemas algorítmicos y la inteligencia artificial (IA) son, cada vez más, parte integral del día a día de las personas. Estas innovaciones han facilitado, entre otras cuestiones, el avance de descubrimientos científicos, la eficientización de procesos o la automatización de tareas. Sin embargo, y como consecuencia de su diseño, desarrollo, despliegue o utilización, también presentan riesgos por su posible impacto en cuestiones tan relevantes como el derecho a la igualdad y a la no discriminación, a la tutela judicial efectiva o al acceso a servicios esenciales, todas ellas dentro del marco de los derechos humanos.

Ante esto, los **mecanismos de reclamación por vulneraciones de derechos constituyen una pieza clave para que la regulación de los sistemas algorítmicos y de la IA sea realmente efectiva**. Sin vías accesibles para denunciar, impugnar y obtener reparación frente a daños concretos, los derechos reconocidos en los distintos marcos normativos corren el riesgo de quedar en un plano meramente declarativo. En este sentido, los mecanismos de reclamación operan como el eslabón que conecta la regulación abstracta con la tutela real y cotidiana de los derechos humanos en contextos digitales.

Esta investigación tiene como objetivo **identificar y analizar los mecanismos jurídicos de reclamación** actualmente disponibles en España frente a vulneraciones de derechos derivadas del uso de sistemas algorítmicos y de inteligencia artificial, **y proponer vías concretas para mejorarlos mediante procesos participativos**. El estudio parte del reconocimiento de que la efectividad de los derechos digitales depende en gran medida de la existencia de mecanismos accesibles, comprensibles y eficaces que permitan a las personas reclamar, impugnar y obtener reparación frente a posibles vulneraciones. Para ello, combina el estudio del marco normativo vigente en España con la presentación de varias experiencias europeas, una investigación cualitativa conducida a través de entrevistas y grupos focales con perfiles expertos del ámbito académico y activista, y el diseño de una guía práctica orientada a la co-creación de sistemas de reclamación con enfoque de derechos humanos.

### ¿Qué dicen las normas y casos de estudio?

El análisis jurídico examinó los mecanismos de reclamación disponibles en España a la luz de los principales marcos normativos nacionales e internacionales.

Dichos marcos se caracterizan por una **fragmentación institucional significativa**: las normas europeas (Reglamento General de Protección de Datos, RGPD; Reglamento de Servicios Digitales, RSD; y Reglamento de IA, RIA) articulan vías de reclamación distintas, gestionadas por autoridades diferentes sin un punto de entrada único ni criterios homogéneos de derivación. Una misma vulneración algorítmica puede quedar simultáneamente cubierta por varias normas o, por el contrario, no encajar plenamente en ninguna, generando inseguridad jurídica y riesgo de inacción administrativa.

A ello se suman **vacíos relevantes de protección**: el RGPD no cubre daños que no impliquen tratamiento de datos personales; el RIA prioriza el cumplimiento normativo del sistema sin garantizar reparación individual; y el RSD se limita a contextos de intermediación digital, como las plataformas digitales o los motores de búsqueda. Estas lagunas afectan especialmente a daños colectivos, discriminaciones indirectas, impactos acumulativos y decisiones algorítmicas opacas.

Desde la perspectiva de las personas afectadas, el acceso efectivo se ve obstaculizado por **barreras procedimentales y técnicas**: identificar la norma aplicable y la autoridad competente requiere conocimiento jurídico especializado; la denuncia no confiere automáticamente la condición de interesado en el procedimiento; y los plazos son incompatibles con la urgencia de los daños algorítmicos, que son inmediatos pero cuya resolución es lenta e incierta.

Por otro lado, el análisis de los dos casos de estudio a nivel europeo ilustra que para que la tutela de derechos frente a daños algorítmicos sea efectiva se requieren mecanismos complementarios. El caso del *Défenseur des droits* francés demuestra la eficacia de los mecanismos extrajudiciales gratuitos y accesibles, capaces de corregir decisiones algorítmicas en la administración pública y formular recomendaciones con impacto sistémico, mientras que el de Noyb, como “entidad habilitada” para interponer acciones colectivas de reparación en cualquier Estado de la UE, evidencia el potencial de la acción colectiva para agrupar reclamaciones individuales ante autoridades de protección de datos y tribunales, generando decisiones vinculantes.

## ¿Qué dicen las personas expertas del ámbito académico y activista?

La investigación cualitativa, que comprendió la realización de nueve entrevistas individuales y dos grupos focales, evidenció la existencia de barreras técnicas, jurídicas, económicas, culturales y sociales en el acceso a mecanismos de reclamación ante vulneraciones de derechos derivadas de sistemas algorítmicos y de IA. Así, se destaca la inviabilidad de que una persona afectada por estos procesos pueda conocer y ejercer sus derechos por sí sola.

Las principales barreras identificadas fueron: la **opacidad técnica de los sistemas**, que impide a las personas saber que han sido objeto de una decisión algorítmica; la **carga individual de la prueba**, que coloca toda la responsabilidad de impugnar sobre quien ha sufrido el daño frente a entidades con mayores recursos; la **complejidad procedimental y fragmentación de responsabilidades**, agravada cuando el sistema es suministrado por un tercero y desplegado por una administración; la **desconfianza institucional** de los colectivos sociales en situación de mayor vulnerabilidad; y la **paradoja temporal**, dado que los daños son inmediatos pero los procedimientos son lentos y de resultado incierto.

De la fase cualitativa emergieron tres recomendaciones clave:

1. **Garantizar la participación real de las comunidades afectadas en el diseño y supervisión de sistemas de IA**, como requisito obligatorio en las evaluaciones de impacto algorítmico previas al despliegue de sistemas de alto riesgo.

2. **Crear mecanismos de reclamación colectiva, accesibles y especializados**, con gratuidad total, inversión de la carga de la prueba, posibilidad de acciones colectivas, procedimientos en lenguaje accesible y salvaguardias frente a represalias.
3. **Reforzar la transparencia y la auditoría independiente como condición para el despliegue**, incluyendo registros públicos de sistemas de IA de alto riesgo, publicación de métricas de equidad y obligación contractual de mantenimiento y monitoreo continuo de los modelos.

## ¿Cómo generar mecanismos de reclamación para la protección efectiva de derechos ante vulneraciones por el uso de sistemas algorítmicos y de IA?

La última parte del informe presenta una guía práctica para co-crear o mejorar sistemas de reclamación accesibles, efectivos y con enfoque de derechos humanos, organizado en tres módulos que pueden implementarse de forma independiente o conjunta.

El primero propone un **punto de acceso centralizado**, en formato de ventanilla única de reclamaciones algorítmicas, donde cualquier persona pueda presentar una reclamación sin necesidad de identificar previamente la autoridad competente ni la norma infringida. Sus principios rectores son la gratuidad, el lenguaje accesible, el diseño híbrido y la derivación y seguimiento activo del caso.

El segundo aborda la necesidad de **adaptación interna de las autoridades competentes**, que disponen de instrumentos legales para actuar pero carecen en la mayoría de los casos de la capacidad técnica, los procedimientos específicos y la cultura institucional necesarios. La guía propone la admisión simplificada de reclamaciones basadas en la descripción del daño sufrido, la inversión de la carga de la prueba, plazos urgentes para daños graves y el monitoreo proactivo de sectores de alto riesgo.

El tercero ofrece **herramientas para que organizaciones de la sociedad civil puedan acompañar a personas afectadas** y articularse con el ecosistema más amplio de actores. Incluye un protocolo de primera atención, un sistema de documentación de patrones de daño sistémico y herramientas de alfabetización algorítmica orientadas no a la formación técnica, sino a dotar a las personas del conocimiento mínimo para identificar el daño y saber cómo actuar.

## Conclusiones

La brecha actual entre el reconocimiento formal de derechos y su garantía material efectiva no es atribuible a la ausencia de marcos normativos, sino a su fragmentación, a los vacíos de protección en supuestos que no encajan en ningún marco sectorial concreto, y a las múltiples barreras superpuestas que impiden a las personas afectadas ejercer sus derechos. El momento regulatorio actual, con el EU AI Act en implementación y debates activos sobre gobernanza de IA en España y Europa, ofrece una ventana de oportunidad que requerirá voluntad política, recursos suficientes y, sobre todo, la participación real de quienes más tienen que perder —o que ganar— en el resultado.

## INTRODUCCIÓN

A lo largo de las últimas décadas, el uso de sistemas algorítmicos y de inteligencia artificial (IA) ha pasado de ser una herramienta técnica especializada a convertirse en un componente transversal en todos los ámbitos de nuestra vida. Este auge plantea no solo oportunidades para la innovación y mejora de servicios públicos y privados, sino también riesgos concretos para los derechos humanos y digitales si carecen de mecanismos adecuados de protección y reclamación. La relación entre IA y derechos humanos, lejos de ser una intersección teórica, se manifiesta de forma práctica: **prácticamente en todos los ámbitos de aplicación de la IA existe un derecho humano vinculado**, desde la privacidad y la protección de datos hasta la igualdad de trato, la libertad de expresión o el acceso a la justicia, lo que exige una reflexión profunda sobre cómo articular la participación en la protección efectiva de estos derechos frente a decisiones automatizadas<sup>1</sup>.

Esta **protección de derechos tiene su punto de partida en la posibilidad de activar mecanismos de reclamación** en caso de que, por el uso de sistemas algorítmicos y de IA, se vulneren los derechos de un individuo o grupo social. Para ello, es necesario que existan marcos jurídicos y normativos que establezcan estos canales, pero también que el proceso sea realmente accesible y eficaz. Sólo con espacios para la reclamación y, en su caso, la reparación, que funcionen será posible que, en un contexto de creciente sofisticación e implementación de herramientas tecnológicas, el impacto en los derechos humanos no sea perjudicial.

Bajo esta premisa, este informe tiene por objetivo indagar en **cómo podrían desarrollarse mecanismos de reclamación que vertebran la protección efectiva de derechos**. Para ello, en una primera fase se analiza, para España, el **marco legal que incide en la regulación de sistemas algorítmicos y de IA**, así como **dos casos de estudio** que ejemplifican fórmulas diversas de reclamación y reparación ante vulneraciones de derechos. En segundo lugar, se presentan los principales **hallazgos de la fase cualitativa de esta investigación**, consistente en la realización de entrevistas y grupos focales a un amplio espectro de perfiles profesionales y activistas. Por último, y partiendo de los resultados de las fases anteriores, se expone una **guía práctica para que administraciones, autoridades y organizaciones de la sociedad civil pongan en marcha, de manera participativa, mecanismos de reclamación ante vulneraciones de derechos por sistemas algorítmicos y de IA**. El informe se acompaña, además, de una serie de **Anexos** que complementan la información presentada.

## Concepto de las vulneraciones derivadas del uso de sistemas algorítmicos o de IA

Antes de ahondar en los distintos apartados del informe, conviene definir qué se entiende, a efectos del mismo, por *vulneraciones derivadas del uso de sistemas algorítmicos o de IA*.

<sup>1</sup> Castilla Juárez, Karlos A. (2023). *Intel·ligència artificial i drets humans: es necessiten mútuament?* [Informe]. Institut de Drets Humans de Catalunya. Consultado el 28 de diciembre de 2025. Disponible en: <https://www.idhc.org/es/publicaciones/inteligencia-artificial-y-derechos-humanos-se-necesitan-mutuamente/>

Estas se definen como **afectaciones a derechos humanos o derechos digitales que se producen como consecuencia del diseño, desarrollo, despliegue o utilización de sistemas automatizados de toma de decisiones**, incluidos los sistemas de inteligencia artificial, tanto en el sector público como en el privado. Estas vulneraciones no se limitan a supuestos de decisiones plenamente automatizadas, sino que abarcan también **sistemas de apoyo a la decisión**, modelos predictivos, sistemas de recomendación, clasificación, perfilado o priorización de contenidos, cuando su funcionamiento incide de manera relevante en la situación jurídica o material de las personas afectadas.

Desde una perspectiva jurídica, las **vulneraciones** analizadas incluyen, entre otras:

- Afectaciones al **derecho a la igualdad y no discriminación**, derivadas de sesgos en los datos o en los modelos;
- Lesiones al **derecho a la protección de datos** personales, especialmente relación con el perfilado, la opacidad del tratamiento y la toma de decisiones automatizadas;
- **Déficit de transparencia, explicabilidad y trazabilidad**, que dificultan la comprensión y la impugnación de decisiones algorítmicas;
- **Limitaciones al derecho a la tutela judicial efectiva y a un recurso efectivo**, cuando las personas afectadas carecen de mecanismos claros para reclamar o impugnar los resultados producidos por estos sistemas; e
- Impacto sobre otros derechos, como la **libertad de expresión**, el **acceso a servicios esenciales** o la presunción de inocencia, en función del contexto de uso.

El informe adopta una concepción amplia de la vulneración, que no exige necesariamente la existencia de un daño consumado, sino que incluye **riesgos estructurales o sistémicos** derivados del uso de sistemas algorítmicos o de IA, especialmente en aquellos calificados como de alto riesgo conforme el marco europeo de IA. En este sentido, se presta especial atención a las **dificultades prácticas para identificar, probar y reclamar frente a estas vulneraciones**, como las asimetrías de información, la complejidad técnica o la fragmentación de responsabilidades. Esta aproximación es coherente con análisis recientes de la Agencia de los Derechos Fundamentales de la Unión Europea, que advierten que los sistemas de IA de alto riesgo pueden generar **impactos simultáneos y acumulativos** sobre múltiples derechos, incluso en ausencia de una decisión automatizada individual claramente identificable, lo que dificulta su detección temprana y su encaje en los marcos tradicionales de reclamación.<sup>2</sup> Esta definición operativa permite analizar de forma transversal los **mecanismos jurídicos de reclamación existentes**, evaluando su capacidad real para responder a los retos específicos que plantea el uso creciente de sistemas algorítmicos y de IA.

A lo largo del informe se opta deliberadamente por emplear la **noción de derechos humanos, y no exclusivamente la de derechos fundamentales**, como categoría analítica de

<sup>2</sup> European Union Agency for Fundamental Rights (FRA). (2025). *Assessing high-risk artificial intelligence: Fundamental rights risks* [Informe]. Consultado el 28 de diciembre de 2025. Disponible en: <https://fra.europa.eu/en/publication/2025/assessing-high-risk-ai>

referencia. Esta elección responde a la necesidad de abordar las afectaciones derivadas del uso de sistemas algorítmicos o de IA desde una perspectiva amplia e integral, que no jerarquiza los derechos en función de su positivización en un ordenamiento concreto, y que resulta coherente con los estándares internacionales y europeos en materia de inteligencia artificial y derechos. En consecuencia, el análisis incluye tanto derechos constitucionalmente reconocidos como otros derechos y garantías relevantes desde una perspectiva de derechos humanos.

## Daños y derechos afectados

A partir de la definición operativa expuesta en el apartado anterior, el despliegue creciente de sistemas algorítmicos y de inteligencia artificial permite identificar daños concretos que inciden de manera directa o indirecta sobre un amplio abanico de derechos. Los **ejemplos** que se presentan a continuación no constituyen una lista cerrada ni exhaustiva, sino que ilustran los principales riesgos jurídicos observados en la práctica, tanto en forma de daños individuales como de impactos colectivos, estructurales o sistémicos.

En relación con el **derecho a la igualdad y a la no discriminación**, son paradigmáticos los casos de sesgos en **sistemas de reconocimiento facial**, que han mostrado tasas de error significativamente más altas para mujeres y personas de comunidades racializadas.<sup>3</sup> En el ámbito socioeconómico, el sistema algorítmico utilizado por la Agencia del Seguro Social de Suecia para **detectar fraude en prestaciones sociales** resultó discriminatorio por razón de género, origen y nivel socioeconómico, lo que motivó críticas y peticiones de retirada por parte de organizaciones de derechos humanos como Amnistía Internacional.<sup>4</sup> Estos casos ilustran cómo decisiones automatizadas pueden vulnerar directamente el principio de igualdad material.

Los daños al **derecho a la protección de datos** personales y a la privacidad se han manifestado también en contextos españoles. Un caso relevante es el de AENA, sancionada por la Agencia Española de Protección de Datos (AEPD) por el uso de **sistemas de reconocimiento facial y tratamientos biométricos sin una base jurídica adecuada** ni garantías suficientes para las personas usuarias, lo que puso de relieve los riesgos asociados al uso de tecnologías algorítmicas intrusivas en espacios públicos y de tránsito masivo.<sup>5</sup> Este caso, si bien centrado en el uso de datos biométricos, refleja problemas más amplios relacionados con el perfilado, la opacidad del tratamiento y la adopción de decisiones automatizadas sin garantías suficientes, que se reproducen en otros contextos de uso de sistemas algorítmicos.

<sup>3</sup> Buolamwini, Joy & Gebru, Timnit. (2020). *Gender Shades: Evaluación de la precisión de productos de clasificación de género con IA* [Informe]. Gender Shades Project. Consultado el 3 de noviembre de 2025. Disponible en: <http://gendershades.org/overview.html>

Amnistía Internacional (s. f.). *Ban the Scan: Stop facial recognition surveillance* [Campaña]. Consultado el 10 de febrero de 2026. Disponible en: <https://banthescan.amnesty.org/index.html>

<sup>4</sup> Amnesty International. (2024). *Sweden: Authorities must discontinue discriminatory AI systems used by welfare agency* [Artículo]. Consultado el 28 de diciembre de 2025. Disponible en: <https://www.amnesty.org/en/latest/news/2024/11/sweden-authorities-must-discontinue-discriminatory-ai-systems-used-by-welfare-agency/>

<sup>5</sup> Agencia Española de Protección de Datos (AEPD). (2024). *PS-00431-2024* [Resolución]. Consultado el 28 de diciembre de 2025. Disponible en: <https://www.aepd.es/documento/ps-00431-2024.pdf>

En cuanto a la falta de **transparencia, explicabilidad y trazabilidad**, resulta especialmente ilustrativo el caso del **sistema BOSCO**, utilizado en España para asignar el bono social eléctrico. La falta de información sobre su funcionamiento motivó un litigio estratégico impulsado por la organización Civio, que puso de relieve cómo la opacidad algorítmica puede afectar al derecho a la información, a la defensa y al acceso a servicios esenciales.<sup>6</sup> Este caso ejemplifica las dificultades prácticas para impugnar decisiones automatizadas adoptadas por administraciones públicas. De forma paralela, este déficit de transparencia algorítmica se ha manifestado también en el ámbito laboral. La aplicación de la denominada **Ley Rider** respondió precisamente a la opacidad de los algoritmos utilizados por diversas plataformas para asignar tareas, evaluar el rendimiento o desactivar cuentas, por ejemplo, reconociendo el derecho de la representación legal de las personas trabajadoras a conocer los parámetros y reglas que rigen estos sistemas automatizados.<sup>7</sup>

Finalmente, las afectaciones al **derecho a la tutela judicial efectiva y a un recurso efectivo** se evidencian por ejemplo en el uso de sistemas algorítmicos para la evaluación de riesgos en el ámbito penal y penitenciario. En Cataluña, el sistema RisCanvi, utilizado para **valorar el riesgo de reincidencia** y apoyar decisiones penitenciarias, ha sido objeto de críticas por su opacidad, por la dificultad de acceso a sus criterios de funcionamiento y por las limitaciones prácticas para impugnar las valoraciones algorítmicas ante los tribunales, lo que plantea dudas sobre el respeto al derecho de defensa y a la contradicción.<sup>8</sup>

Tal y como pone de relieve la Agencia de los Derechos Fundamentales de la Unión Europea, los daños derivados del uso de sistemas algorítmicos y de inteligencia artificial rara vez se presentan como episodios aislados o excepcionales, sino que responden a **patrones sistémicos vinculados al diseño, los datos, los contextos de despliegue y los modelos de gobernanza de estos sistemas**, especialmente en aquellos calificados como de alto riesgo.<sup>9</sup> Los ejemplos analizados en este apartado, que constituyen solo una muestra entre los múltiples casos documentados a nivel europeo e internacional, evidencian cómo estas vulneraciones tienden a **afectar de forma desproporcionada a determinados colectivos y a generar impactos acumulativos difíciles de atribuir, probar y corregir**. Esta realidad plantea desafíos específicos para la identificación de responsabilidades, y subraya la necesidad de examinar con detalle el marco normativo aplicable y la capacidad real de los mecanismos de reclamación existentes, cuestión que se aborda en el apartado siguiente.

<sup>6</sup> Fundación Ciudadana Civio. (2025). *Civio abre camino en la transparencia algorítmica: el Supremo condena al Gobierno a entregar el código fuente de BOSCO* [Artículo]. Consultado el 28 de diciembre de 2025. Disponible en: <https://civio.es/novedades/2025/09/17/civio-abre-camino-en-la-transparencia-algoritmica-el-supremo-condena-al-gobierno-a-entregar-el-codigo-fuente-de-bosco/>

<sup>7</sup> Ministerio de Trabajo y Economía Social (MITE-S). (2022). *Información algorítmica en el ámbito laboral: Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral* [Guía]. Consultado el 28 de diciembre de 2025. Disponible en: [https://www.mites.gob.es/ficheros/ministerio/inicio\\_destacados/Guia\\_Algoritmos\\_ES.pdf](https://www.mites.gob.es/ficheros/ministerio/inicio_destacados/Guia_Algoritmos_ES.pdf)

<sup>8</sup> Jiménez Arandía, Pablo. (2025). *RisCanvi* [Página web]. Consultado el 28 de diciembre de 2025. Disponible en: <https://pablojimenezarandia.com/tag/riscanvi/>

<sup>9</sup> European Union Agency for Fundamental Rights (FRA). (2025). *Assessing high-risk artificial intelligence: Fundamental rights risks* [Informe]. Consultado el 4 de enero de 2026. Disponible en: <https://fra.europa.eu/en/publication/2025/assessing-high-risk-ai>

## BLOQUE I: EL MARCO LEGAL Y SUS LÍMITES

Este apartado examina el marco normativo aplicable a los mecanismos de reclamación frente a vulneraciones de derechos derivadas del uso de sistemas algorítmicos y de IA, a través de un análisis escalonado de los **principales instrumentos** internacionales, europeos y nacionales. En primer lugar, se aborda brevemente el **ámbito internacional**, atendiendo a los estándares y recomendaciones desarrollados en foros multilaterales. A continuación, se analiza el **marco europeo**, y finalmente se examina el **marco jurídico español**, con el objetivo de identificar las vías de reclamación existentes, las autoridades competentes y las principales limitaciones prácticas en cada nivel. Además, se incorporan dos **estudios de caso** de mecanismos de reclamación ante vulneraciones de derechos que complementan el análisis jurídico.

### Ámbito internacional

En el ámbito internacional, si bien no existe todavía un marco jurídicamente vinculante y exhaustivo específico sobre inteligencia artificial y sistemas algorítmicos, se ha desarrollado un conjunto relevante de **instrumentos de soft law**<sup>10</sup> que establecen **estándares interpretativos fundamentales en materia de derechos humanos**. Estos marcos resultan especialmente significativos para el análisis de las vulneraciones derivadas del uso de sistemas algorítmicos, en la medida en que afirman de forma reiterada la **obligación de los Estados de garantizar mecanismos efectivos de reclamación y reparación**, tanto frente a actuaciones de autoridades públicas como frente a impactos causados por actores privados. Asimismo, estos instrumentos reconocen la necesidad de disponer de **vías judiciales y administrativas accesibles**, capaces de abordar daños complejos y difusos, y subrayan el papel de las autoridades administrativas y de supervisión en la tutela de los derechos afectados.

Aunque carecen de fuerza vinculante directa, estos estándares internacionales desempeñan una función clave como **marco interpretativo y orientador** para los poderes públicos, los órganos administrativos y judiciales, contribuyendo a **perfiar el contenido del derecho a un recurso efectivo, a la reparación y a la rendición de cuentas en contextos algorítmicos**.

En el **Anexo I** de este documento se reflejan, a modo de resumen, las notas características de los instrumentos desarrollados en el seno de las Naciones Unidas, los marcos globales específicamente dedicados a la inteligencia artificial y los instrumentos del Consejo de Europa, en relación con los procesos de reclamación que contemplan.

<sup>10</sup> Definición "soft law": *La expresión soft law busca describir la existencia de fenómenos jurídicos caracterizados por carecer de fuerza vinculante aunque no carentes de efectos jurídicos o al menos con cierta relevancia jurídica*. Obtenida de: <https://diccionariojuridico.org/definicion/soft-law/>

## Ámbito europeo

El marco europeo de regulación de los sistemas digitales y algorítmicos se configura como un **entramado normativo complejo y multinivel**, resultado de una estrategia de la Unión Europea (UE) para responder a los riesgos que plantean las tecnologías digitales desde perspectivas diversas: protección de datos personales, funcionamiento del mercado interior y salvaguarda de los derechos fundamentales. Instrumentos como el Reglamento General de Protección de Datos, el Reglamento de Servicios Digitales y el Reglamento de Inteligencia Artificial fueron concebidos en momentos normativos distintos y con lógicas regulatorias específicas, aunque comparten el objetivo de establecer **reglas armonizadas y directamente aplicables en todos los Estados miembros**.

Actualmente, este entramado se ve atravesado por una tendencia política posterior orientada a la **simplificación**<sup>11</sup> y reducción de cargas regulatorias, impulsada por la Comisión Europea, que no altera el origen ni la finalidad de estos Reglamentos, pero sí podría condicionar su implementación, coordinación institucional y aplicación práctica.

## Reglamento de Protección de Datos (2016/679)

El Reglamento General de Protección de Datos (ahora en adelante, RGPD)<sup>12</sup>, regula el **tratamiento de datos personales** realizado por responsables y encargados del tratamiento, tanto públicos como privados, cuando dicho tratamiento se lleve a cabo en el contexto de actividades establecidas en la UE o produzca efectos sobre personas situadas en ella. Su alcance material incluye operaciones automatizadas y no automatizadas, lo que lo hace plenamente aplicable a **sistemas algorítmicos y de IA que traten datos personales**, incluidos los supuestos de perfilado y toma de decisiones automatizadas. El ámbito subjetivo se articula en torno a las **personas interesadas**, titulares de los datos, y a los **responsables del tratamiento**, que asumen obligaciones reforzadas de licitud, transparencia y rendición de cuentas.

El RGPD configura un sistema explícito de vías de reclamación, tanto administrativas como judiciales. El artículo 77 reconoce el **derecho de cualquier interesado a presentar una reclamación** ante una autoridad de control si considera que el tratamiento de sus datos infringe el Reglamento, sin perjuicio de otros recursos administrativos o acciones judiciales. Este derecho se activa también de forma indirecta a través de las **obligaciones de transparencia**: el artículo 12.4 prevé expresamente que, si el responsable no da curso a una solicitud del interesado en el plazo de un mes, deberá informarle de la posibilidad de reclamar ante una autoridad de control y de ejercitar acciones judiciales. Asimismo, los artículos 13.2.d) y 14.2.e) obligan al responsable a **informar**, desde el inicio del tratamiento, del derecho a presentar una reclamación, tanto si los datos se obtienen directamente del

<sup>11</sup> Comisión Europea. (2025). *Paquete digital, Preguntas frecuentes* [Página web]. Consultado el 28 de diciembre de 2025. Disponible en: <https://digital-strategy.ec.europa.eu/es/faqs/digital-package>

<sup>12</sup> Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, 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 (RGPD)* [Reglamento]. Consultado el 28 de diciembre de 2025. Disponible en: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es>

interesado como si no. Estas disposiciones convierten la **reclamación en un elemento estructural** del régimen de protección, no accesorio.

El Capítulo VI del Reglamento instaura **autoridades de control independientes**, estableciendo un marco institucional sólido para la tutela efectiva de los derechos. Los artículos 51 a 55 regulan la designación, independencia y competencia de las autoridades de control, mientras que el artículo 57 detalla sus funciones, entre las que destaca expresamente la de **tratar las reclamaciones presentadas por los interesados, investigar su fundamento e informar al reclamante sobre el curso y el resultado en un plazo razonable**. Este mandato dota a las autoridades de control de un papel activo como **órganos de garantía cuasi-jurisdiccionales**. Además, el artículo 78 reconoce el derecho a la tutela judicial efectiva contra las decisiones (o inacción) de las autoridades de control, y el artículo 82 establece un **derecho a indemnización** por los daños materiales o inmateriales derivados de infracciones del Reglamento, reforzando la dimensión reparadora del sistema.

A pesar de ser una normativa consolidada, el uso del RGPD como vía de reclamación frente a sistemas algorítmicos presenta algunas limitaciones en la práctica. Su ámbito material se circunscribe al tratamiento de datos personales, lo que **excluye supuestos de daño algorítmico que no impliquen datos personales** o que se basen en inferencias no claramente atribuibles a una persona identificada. También debemos tener en cuenta que aunque el derecho de acceso (art. 15.1.f) y las obligaciones de transparencia constituyen herramientas clave, en la práctica **no siempre permiten comprender la lógica compleja de sistemas algorítmicos avanzados**, lo que dificulta la formulación de reclamaciones informadas. Asimismo, la **carga procedimental y la duración de las investigaciones** pueden limitar la efectividad del remedio, especialmente en contextos de decisiones automatizadas de impacto inmediato. Por último, el RGPD no fue diseñado específicamente para abordar daños colectivos o riesgos sistémicos, lo que restringe su capacidad para responder a prácticas algorítmicas estructurales más allá del caso individual.

## Reglamento de Servicios Digitales (2022/2065)

El **Reglamento Europeo de Servicios Digitales** (ahora en adelante, RSD)<sup>13</sup> crea un marco jurídico para intermediarios en línea con el objetivo de garantizar un **entorno digital seguro, transparente y respetuoso con derechos humanos**, regulando obligaciones de diligencia debida, transparencia en decisiones de moderación de contenidos y mecanismos de supervisión y transparencia. La normativa se aplica a los **prestadores de servicios intermediarios** (plataformas de redes sociales, *marketplaces*, motores de búsqueda, etc.) que operan en la UE, y a los **destinatarios de esos servicios**, definidos como cualquier persona física o jurídica que utiliza servicios intermediarios en línea.

Mientras que el Reglamento de Inteligencia Artificial (RIA) veremos que responde claramente a una lógica de mercado y seguridad de productos (*product safety* y *market*

<sup>13</sup> Parlamento Europeo y Consejo de la Unión Europea. (2022). *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) (Texto pertinente a efectos del EEE)*. [Reglamento]. Consultado el 28 de diciembre de 2025. Disponible en: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>

*surveillance*), el RSD adopta una **arquitectura híbrida entre la armonización del mercado interior y la protección de los derechos humanos**. Ambos Reglamentos comparten el objetivo de garantizar condiciones homogéneas en el mercado interior, el recurso a autoridades administrativas especializadas y la combinación de mecanismos de supervisión *ex ante* y *ex post*. Sin embargo, difieren de forma sustancial en su diseño normativo y en el papel que otorgan a las personas afectadas.

En el RSD, el **sujeto central de protección es el destinatario del servicio**, y no el producto o sistema tecnológico en sí. El Reglamento se construye alrededor de las decisiones que afectan directamente a los usuarios, como la moderación y retirada de contenidos, la suspensión o limitación de cuentas y la priorización o despriorización algorítmica de información. Las **obligaciones impuestas a los prestadores están directamente vinculadas a la protección de derechos fundamentales**, en particular la libertad de expresión e información, la no discriminación y el acceso a recursos efectivos. En este contexto, las **reclamaciones adquieren una dimensión cuasi-procedimental** de derechos, ya que el artículo 53 permite a los usuarios denunciar infracciones del Reglamento en su condición de destinatarios del servicio, y no meramente como denunciadores regulatorios.

Por último, el RSD aborda la **seguridad como una cuestión relativa al entorno digital y a los riesgos sistémicos que determinadas prácticas pueden generar para la sociedad y los derechos humanos**. En consecuencia, el control de los sistemas algorítmicos se vincula principalmente a sus impactos sociales, informativos y democráticos, y no a defectos técnicos o fallos de diseño del *software* en sentido estricto.

El **artículo 53** del RSD establece el derecho a **presentar una reclamación** contra prestadores de servicios intermediarios ante el **Coordinador de Servicios Digitales del Estado miembro** donde el destinatario esté situado o establecido, para alegar una infracción del Reglamento por parte del proveedor. El Coordinador evaluará la reclamación y, cuando sea pertinente, la remitirá al Coordinador del Estado miembro donde el prestador esté establecido o a otra autoridad competente, acompañada de un dictamen si procede.

Además de este mecanismo institucional, el RSD impone a los proveedores la **obligación de contar con mecanismos internos** de gestión de reclamaciones respecto a decisiones propias de moderación de contenidos, y ofrece la **posibilidad de recursos extrajudiciales** que complementan la reclamación ante autoridades.<sup>14</sup> En su artículo 54 reconoce expresamente el **derecho de los destinatarios del servicio a solicitar una indemnización** por los daños sufridos como consecuencia de una infracción del Reglamento. Este derecho se ejerce conforme al Derecho nacional aplicable y sin perjuicio de otros recursos disponibles, introduciendo una dimensión reparadora que complementa los mecanismos administrativos y refuerza la posición jurídica de las personas afectadas.

El **Coordinador de Servicios Digitales** designado en cada Estado miembro es la **autoridad principal** para recibir y gestionar las reclamaciones conforme al artículo 53, actuando como

---

<sup>14</sup> Comisión Nacional de los Mercados y la Competencia (CNMC). (2025). *Reclamaciones en el marco del Reglamento (UE) 2022/2065 sobre servicios digitales (DSA)* [Página web]. Consultado el 28 de diciembre de 2025. Disponible en: <https://www.cnmc.es/index.php/sectores-que-regulamos/servicios-digitales-dsa/reclamaciones>

autoridad administrativa especializada en la supervisión del cumplimiento del RSD. Tiene competencias para evaluar el fondo de las reclamaciones, transmitir las a otros coordinadores o autoridades competentes, y coordinar respuestas cuando la reclamación exige acción regulatoria, supervisión o medidas correctivas. La normativa también prevé la cooperación transfronteriza entre coordinadores de distintos Estados miembros, y la información mutua sobre el seguimiento de reclamaciones y actividades, fortaleciendo la vigilancia y coherencia del mercado único digital.

Aunque el RSD reconoce formalmente el derecho de reclamación, su **efectividad práctica puede verse limitada por varios factores**. Primero, el procedimiento depende de las **capacidades, recursos y especialización** de los coordinadores nacionales para interpretar reclamaciones relacionadas con sistemas complejos o algoritmos de moderación, por ejemplo. Segundo, la **remisión de reclamaciones** a autoridades competentes de otro Estado miembro o a otras autoridades nacionales puede introducir demoras y complejidad procesal, reduciendo la accesibilidad para las personas afectadas. Tercero, la **coexistencia de mecanismos internos del proveedor, recursos extrajudiciales** y la **reclamación ante coordinadores** puede generar fragmentación procedimental, exigiendo a las personas afectadas navegar diferentes rutas antes de lograr una resolución efectiva. Por último, los **informes de actividad exigidos a los coordinadores** (incluyendo estadísticas de reclamaciones) pueden mejorar la transparencia general, pero no garantizan reparaciones individuales ni criterios uniformes de tramitación entre jurisdicciones.

## Reglamento de Inteligencia Artificial (2024/1689)

El **Reglamento Europeo de Inteligencia Artificial (RIA)**<sup>15</sup>, tiene por objeto **regular la introducción al mercado, puesta en servicio y utilización de sistemas de IA**<sup>16</sup> en la Unión Europea (perspectiva *product safety*), garantizando un nivel elevado y coherente de protección de la salud, la seguridad y los derechos humanos recogidos en la Carta de Derechos Fundamentales de la UE. Su ámbito subjetivo abarca **operadores del ciclo de vida del sistema** (proveedores, responsables del despliegue, importadores, distribuidores, representantes automatizados), así como a las **autoridades designadas por los Estados miembros para la vigilancia del mercado** y otras autoridades competentes con competencias regionales.

El Reglamento opera en paralelo a otros marcos de la UE, y no sustituye las vías de recurso existentes, sino que las **complementa** con diferentes obligaciones. Aun así, debemos tener en cuenta que las **personas afectadas no constituyen el sujeto central del diseño**

<sup>15</sup> Parlamento Europeo y Consejo de la Unión Europea. (2024). *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 determinados Reglamentos y Directivas (Reglamento de Inteligencia Artificial) (Texto pertinente a efectos del EEE)* [Reglamento]. Consultado el 28 de diciembre de 2025. Disponible en: [https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ:L\\_202401689](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=OJ:L_202401689)

<sup>16</sup> Art.3 (1) RIA: «sistema de IA»: 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.

**normativo**, si bien el Reglamento les reconoce determinados derechos específicos en los artículos 85 a 87.

El **artículo 85** del RIA, que inspira el presente informe, reconoce explícitamente un **derecho de cualquier persona física o jurídica a presentar una reclamación ante la autoridad de vigilancia del mercado** cuando considere que ha infringido el Reglamento. Este derecho opera “sin perjuicio de otros recursos administrativos o judiciales”, lo que significa que la reclamación ante la autoridad de vigilancia del mercado es una **vía adicional** de acceso a la vigilancia y corrección de incumplimientos del Reglamento.

Las reclamaciones pueden dirigirse contra cualquier operador sujeto al Reglamento y también, en su caso, contra organismos notificados<sup>17</sup>. Estas reclamaciones activan mecanismos reactivos de vigilancia del mercado, que pueden dar lugar a **investigaciones, inspecciones, coordinación entre autoridades y eventual imposición de medidas correctivas o sancionadoras**. Además, las reclamaciones deben ser tenidas en cuenta como elemento estructural para futuras actividades proactivas de vigilancia, lo que convierte este derecho en una herramienta de **detección de incumplimientos sistémicos**.

Una vez una persona **ejerce su derecho a reclamar**, la autoridad de vigilancia del mercado pertinente **iniciará el proceso** que haya establecido para dar seguimiento a las reclamaciones, según el artículo 11 del **Reglamento Europeo relativo a la vigilancia del mercado y la conformidad de los productos (UE, 2019-1020)**<sup>18</sup>. Normalmente una vez iniciada una reclamación, la autoridad de vigilancia del mercado iniciará un procedimiento de inspección. Para incentivar el cumplimiento del Reglamento, las autoridades siempre podrán **colaborar** con otras autoridades pertinentes y organizaciones que representen operadores económicos o a usuarios finales.

Las **autoridades de vigilancia del mercado** ocupan una posición central en la tramitación de reclamaciones conforme el artículo 85 del RIA, actuando como nodos de recepción, análisis y activación de medidas de cumplimiento. Su actuación se rige tanto por el propio RIA como por el Reglamento 2019/1020, lo que refuerza la lógica de supervisión de productos. La autoridad competente puede variar en función del tipo de sistema de IA y del operador presuntamente infractor (art.74 RIA), y el marco normativo presupone que, en caso de error por parte del reclamante, la autoridad receptora remita la reclamación al órgano competente o informe adecuadamente a la persona afectada. La **gestión de reclamaciones** se integra en un **ecosistema institucional más amplio** que incluye autoridades notificantes, organismos de acreditación y, potencialmente, autoridades de protección de derechos humanos, aunque el Reglamento no articula mecanismos formales de coordinación centrados específicamente en la reparación de daños individuales.

<sup>17</sup> Comisión Europea. (2022). *The “Blue Guide” on the implementation of EU product rules 2022* (2022/C 247/01) [Comunicación]. Consultado el 28 de diciembre de 2025. Disponible en: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XC0629\(04\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XC0629(04))

<sup>18</sup> Parlamento Europeo y Consejo de la Unión Europea. (2019). *Reglamento (UE) 2019/1020, de 20 de junio de 2019, relativo a la vigilancia del mercado y a la conformidad de los productos* [Reglamento]. Consultado el 28 de diciembre de 2025. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R1020>

Pese a reconocer un derecho explícito de reclamación, el diseño del artículo 85 presenta **limitaciones estructurales** desde la perspectiva del acceso efectivo a la justicia en contextos de IA. Por un lado, el procedimiento no está concebido prioritariamente como un cauce de reparación individual ni de restitución de derechos, sino como un **instrumento de control del cumplimiento normativo**. Por otro lado, la efectividad del mecanismo depende en gran medida de la capacidad técnica, recursos y especialización de las autoridades de vigilancia para investigar sistemas de IA complejos y opacos. Asimismo, la **ausencia de un procedimiento armonizado a nivel europeo** puede generar desigualdades prácticas en el acceso y tratamiento de reclamaciones entre Estados miembros. Todo ello refuerza la necesidad de complementar este mecanismo con vías nacionales o de derechos humanos que traduzcan las reclamaciones en remedios más directamente orientados a las personas.

Si nos fijamos en los últimos tres mecanismos analizados, el RGPD, el RSD y el RIA, configuran **tres lógicas complementarias pero no equivalentes** de tutela frente a impactos algorítmicos o de inteligencia artificial. El **RGPD** ofrece el marco más consolidado y más operativo, al reconocer derechos individuales claros, vías administrativas y judiciales explícitas y un papel activo de las autoridades de control, aunque su alcance se limita a supuestos en los que existe tratamiento de datos personales. El **RIA**, en cambio, incorpora el derecho de reclamación desde una lógica de vigilancia del mercado y seguridad del producto, orientada principalmente a detectar y corregir incumplimientos normativos sistémicos, más que a proporcionar reparación individual directa a las personas afectadas, siempre que hablemos de sistemas que incorporen IA. Por su parte, el **RSD** adopta una arquitectura híbrida, en la que la reclamación se articula desde la posición del destinatario del servicio, conectando la supervisión administrativa con la protección de derechos fundamentales frente a decisiones de plataformas que afectan directamente a los usuarios. En el **Anexo II** de este documento se incorpora una tabla comparativa que refleja estas conclusiones de manera resumida.

## Ámbito español

El marco español de respuesta a los impactos de los sistemas algorítmicos y de IA se construye a partir de la **articulación y desarrollo interno de los instrumentos europeos**, complementados por iniciativas normativas propias. En este contexto, España ha optado por combinar **instrumentos de carácter orientador**, como la Carta de Derechos Digitales, con **propuestas normativas** destinadas a operativizar la gobernanza y supervisión de la tecnología

El análisis del ámbito español resulta clave para evaluar hasta qué punto los principios y derechos reconocidos a nivel europeo se traducen en **mecanismos efectivos de reclamación, denuncia y garantía** frente a vulneraciones derivadas del uso de sistemas algorítmicos. Asimismo, este apartado incorpora el examen de determinadas **normativas sectoriales** que han comenzado a incorporar disposiciones específicas relativas al uso de datos, algoritmos y sistemas de IA.

## Carta de Derechos Digitales

El análisis del ámbito español se inicia con la Carta de Derechos Digitales (ahora en adelante, CDD), instrumento que inspira de manera directa el presente informe y el trabajo del proyecto orientado a la co-creación de un mecanismo de reclamación frente a vulneraciones de derechos derivadas del uso de sistemas algorítmicos y de inteligencia artificial. La **Carta de Derechos Digitales** (2021)<sup>19</sup>, aprobada en el marco de la **Agenda España Digital**, tiene como finalidad **reconocer, articular y garantizar el contenido de los derechos humanos en el entorno digital**, integrando garantías ya existentes y adaptándolas a los retos derivados de la transformación digital.

Su alcance material abarca un amplio conjunto de **derechos vinculados al acceso, uso y participación en los entornos digitales**, incluyendo, entre otros, la protección de datos personales, la transparencia y supervisión de los sistemas algorítmicos, y la participación democrática en el ámbito digital. Desde el punto de vista subjetivo, la Carta se dirige a **todas las personas físicas**, así como a las **relaciones entre personas y administraciones públicas y proveedores de servicios digitales**, en tanto interactúan en contextos digitales. Si bien no constituye una norma jurídicamente vinculante ni crea obligaciones directamente exigibles a actores privados, sí establece **compromisos y orientaciones dirigidos a los poderes públicos**, llamados a garantizar estos derechos y a desarrollar marcos normativos y políticas públicas en el ámbito digital.

Así, la CDD **no establece un mecanismo específico de reclamación**, sino que actúa como un **marco de principios y garantías** que orienta la actuación normativa y administrativa en España frente a vulneraciones de derechos en el entorno digital. Además, en lugar de crear procedimientos *ad hoc*, **remite a las vías de reclamación ya existentes** en el ordenamiento jurídico, de modo que las personas afectadas deben acudir a los mecanismos previstos en la normativa sectorial correspondiente, como las reclamaciones ante la AEPD en materia de privacidad y tratamiento automatizado.

No crea nuevos órganos de supervisión ni incorpora un régimen sancionador, aunque **refuerza el papel de las autoridades** existentes como garantes de los derechos digitales y establece un marco interpretativo que debe guiar la actuación de los poderes públicos. Su eficacia práctica como instrumento de tutela depende, no obstante, de la **concreción de sus principios en normas sectoriales vinculantes**, de la coordinación entre autoridades administrativas y órganos jurisdiccionales, y de la disponibilidad de capacidades técnicas e institucionales suficientes para abordar vulneraciones derivadas del uso de sistemas algorítmicos.

<sup>19</sup> Ministerio de Asuntos Económicos y Transformación Digital. (2021). *Carta de Derechos Digitales* [Documento institucional]. Consultado el 4 de enero de 2026. Disponible en: <https://espanadigital.gob.es/lineas-de-actuacion/carta-de-derechos-digitales>

## Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

La **Ley Orgánica 3/2018, de 5 de diciembre (ahora en adelante, LOPDGDD)**,<sup>20</sup> tiene como finalidad principal adaptar y complementar el ordenamiento jurídico español al Reglamento (UE) 2016/679 (RGPD), **garantizando el ejercicio efectivo del derecho fundamental a la protección de datos personales reconocido en el artículo 18.4 de la Constitución Española**. Su alcance material se extiende a cualquier tratamiento total o parcialmente automatizado de datos personales, así como a tratamientos no automatizados incorporados o destinados a incorporarse a un fichero, lo que la hace plenamente aplicable a sistemas algorítmicos y de IA que traten datos personales, incluidos los supuestos de perfilado y toma de decisiones automatizadas.

Desde el punto de vista subjetivo, la Ley se aplica a **responsables y encargados del tratamiento**, tanto públicos como privados, que operen en el territorio español o estén sujetos al Derecho español conforme al RGPD. Asimismo, refuerza la posición jurídica de las personas físicas como titulares de los datos y derechos, y articula el papel de las autoridades de control, en particular, la **Agencia Española de Protección de Datos (AEPD)** y las **autoridades autonómicas**, como órganos de garantía del sistema. La LOPDGDD no introduce una regulación específica de la IA, pero constituye el **principal marco nacional para canalizar reclamaciones frente a daños algorítmicos cuando estos implican tratamiento de datos personales**.

La LOPDGDD desarrolla y **concreta las vías de reclamación previstas en el RGPD**, reforzando su operatividad en el ámbito nacional. El Título VIII regula los procedimientos en caso de posible vulneración de la normativa de protección de datos, estableciendo que las reclamaciones pueden iniciarse a instancia de la persona afectada ante la autoridad de control competente. La Ley detalla aspectos procedimentales relevantes, como la admisión a trámite de las reclamaciones, las actuaciones previas de investigación, la adopción de medidas provisionales y de garantía de los derechos, incluida la posibilidad de bloqueo de datos, y los plazos de tramitación.

Un elemento relevante desde la perspectiva de los sistemas algorítmicos es la posibilidad de **canalizar reclamaciones de forma escalonada**. La Ley prevé que la autoridad de control pueda remitir la reclamación al delegado de protección de datos (DPD) del responsable o encargado, o a mecanismos de resolución extrajudicial previstos en códigos de conducta, antes de iniciar formalmente un procedimiento sancionador. Esta configuración refuerza el acceso a vías administrativas de reclamación, aunque mantiene una lógica predominantemente individual y centrada en la infracción normativa, más que en la reparación estructural de daños algorítmicos complejos.

<sup>20</sup> Boletín Oficial del Estado (BOE). (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* [Ley]. Consultado el 4 de enero de 2026. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

La LOPDGDD **consolida el papel de la AEPD** como autoridad administrativa independiente y órgano central de garantía en materia de protección de datos y reclamaciones. El Título VII regula sus funciones y potestades, atribuyéndole competencias de investigación, supervisión, regulación y sanción, así como la tramitación y resolución de reclamaciones presentadas por las personas interesadas. Estas potestades incluyen la posibilidad de requerir información técnica, realizar auditorías y adoptar medidas correctivas frente a tratamientos ilícitos, aspectos clave en contextos de sistemas algorítmicos opacos o complejos. Asimismo, la Ley reconoce el **papel de las autoridades autonómicas de protección de datos** en sus respectivos ámbitos competenciales y articula mecanismos de cooperación y coordinación con la AEPD, en línea con el sistema de “ventanilla única” del RGPD. De forma complementaria, la **figura del delegado de protección de datos** adquiere relevancia como mecanismo interno de garantía, al permitir la resolución temprana y no contenciosa de reclamaciones.

Pese a su solidez institucional como vía de reclamación, la LOPDGDD presenta **limitaciones** relevantes. Su **ámbito material se circunscribe al tratamiento de datos personales**, lo que excluye daños algorítmicos que no impliquen datos identificables o que se basen en inferencias agregadas o no directamente atribuibles a una persona. Asimismo, aunque los derechos de acceso, oposición y limitación del tratamiento, incluidos los relativos a decisiones automatizadas, constituyen herramientas clave, en la práctica no siempre permiten comprender la lógica y el funcionamiento de sistemas algorítmicos complejos, **dificultando la formulación de reclamaciones informadas**. A ello se suma que los procedimientos administrativos pueden resultar largos y técnicamente exigentes, lo que reduce la efectividad del remedio frente a decisiones automatizadas de impacto inmediato, y que el marco mantiene una **lógica predominantemente individual y reactiva**, con una capacidad limitada para abordar daños colectivos o riesgos sistémicos derivados del uso generalizado de sistemas algorítmicos.

En el **Anexo III** del presente informe se incorpora una figura explicativa del proceso de reclamación en el marco de la LOPDGDD.

## Proyecto de Ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación (121/000068)

El Proyecto de Ley 121/000068 (ahora en adelante, Proyecto de Ley)<sup>21</sup> <sup>22</sup> tiene como finalidad principal adaptar el ordenamiento jurídico español al Reglamento (UE) 2022/2065 de Servicios Digitales (RSD) y al Reglamento (UE) 2024/1083 sobre libertad de los medios de comunicación, mediante la modificación de normas internas preexistentes, en particular la Ley 34/2002 (LSSI), la Ley 13/2022 General de Comunicación Audiovisual y la Ley 3/2013 de creación de la CNMC. Se trata, por tanto, de una **norma de desarrollo y ejecución interna de Reglamentos europeos directamente aplicables**, orientada a garantizar su efectividad práctica en el contexto institucional español. Su alcance material se centra en la supervisión de los servicios intermediarios, las obligaciones de diligencia debida y los mecanismos de control de contenidos y prácticas digitales, incluyendo de forma indirecta el funcionamiento de sistemas algorítmicos de moderación, recomendación y priorización de contenidos. El ámbito subjetivo comprende a los **prestadores de servicios digitales** que operan en España, así como a las **autoridades administrativas** encargadas de su control, afectando de manera mediata a las **personas usuarias** como destinatarias de estos servicios.

En relación con las vías de reclamación, el Proyecto no introduce un derecho autónomo distinto del previsto en el RSD, sino que **desarrolla y operativiza a nivel nacional el derecho de los destinatarios del servicio a presentar reclamaciones ante el Coordinador de Servicios Digitales**. La reclamación se configura principalmente como un mecanismo de activación de la supervisión administrativa frente a posibles infracciones de las obligaciones impuestas a los prestadores, incluidas aquellas relacionadas con el uso de sistemas algorítmicos, sin perjuicio de otras vías judiciales o extrajudiciales disponibles. El texto refuerza una **lógica de denuncia administrativa orientada a la detección y corrección de incumplimientos normativos**, más que a la reparación individual directa de los daños sufridos por las personas afectadas. Las reclamaciones pueden dar lugar a actuaciones inspectoras, requerimientos de información, órdenes de actuación o procedimientos sancionadores, en función de la gravedad de la infracción detectada y de las competencias atribuidas a la autoridad competente.

En cuanto al papel de las autoridades, el Proyecto de Ley consolida a la **Comisión Nacional de los Mercados y la Competencia como Coordinador de Servicios Digitales** en España, atribuyéndole competencias centrales de supervisión, investigación y coordinación en la

<sup>21</sup> Congreso de los Diputados. (2025). *Proyecto de Ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación (121/000068)* [Proyecto de Ley]. Consultado el 3 de enero de 2026. Disponible en: [https://www.congreso.es/es/proyectos-de-ley?p\\_p\\_id=iniciativas&p\\_p\\_lifecycle=0&p\\_p\\_state=normal&p\\_p\\_mode=view&iniciativas\\_mode=mostrarDetalle&iniciativas\\_legislatura=XV&iniciativas\\_id=121/000068](https://www.congreso.es/es/proyectos-de-ley?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&iniciativas_mode=mostrarDetalle&iniciativas_legislatura=XV&iniciativas_id=121/000068)

<sup>22</sup> Ministerio para la Transformación Digital y de la Función Pública (España). (2025). *El Gobierno aprueba el anteproyecto de ley que impulsa la gobernanza democrática en servicios digitales y crea el registro de medios de comunicación* [Nota de prensa]. Consultado el 28 de diciembre de 2025. Disponible en: [https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion\\_ministro/2025/02/2025-02-25/NdPCminDSAE\\_MFA.pdf](https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion_ministro/2025/02/2025-02-25/NdPCminDSAE_MFA.pdf)

aplicación del Reglamento de Servicios Digitales. De forma complementaria, la AEPD mantiene sus competencias específicas cuando las prácticas digitales o algorítmicas impliquen tratamiento de datos personales, lo que refuerza un modelo de supervisión distribuida y transversal.

Desde la perspectiva del acceso efectivo a mecanismos de reclamación frente a vulneraciones derivadas de sistemas algorítmicos, el Proyecto de Ley presenta limitaciones relevantes. Al concebir la reclamación principalmente como una herramienta de control regulatorio, el sistema ofrece una **respuesta indirecta a las personas afectadas y depende en gran medida de la capacidad institucional de las autoridades para traducir las denuncias en actuaciones efectivas**. Además, la coexistencia de múltiples vías, mecanismos internos de plataformas, recursos extrajudiciales y reclamaciones ante autoridades administrativas, puede generar fragmentación procedimental y dificultar la accesibilidad para los usuarios.

Finalmente, al **encontrarse en fase de tramitación parlamentaria**, la eficacia real de este marco dependerá de su desarrollo, de la dotación de recursos técnicos y humanos a las autoridades competentes y de la capacidad de estas para abordar reclamaciones relativas a sistemas algorítmicos complejos.

En el **Anexo IV** del presente informe se incorpora una figura explicativa del proceso de reclamación previsto en el Proyecto de Ley 121/000068.

## Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial

El Anteproyecto de Ley para el Buen Uso y la Gobernanza de la Inteligencia Artificial (ahora en adelante, Anteproyecto)<sup>23 24</sup> tiene por objeto **adaptar la legislación española al Reglamento (UE) 2024/1689 (RIA) y desarrollar aspectos clave de su gobernanza y régimen sancionador en el ámbito nacional**. Este texto normativo regula el diseño, comercialización, introducción en el mercado, puesta en servicio y utilización de sistemas de IA por parte de entidades públicas y privadas en España, con especial atención a los usos que puedan plantear riesgos para los derechos fundamentales, la seguridad y la transparencia. El ámbito subjetivo incluye a **operadores de sistemas de IA** (proveedores, responsables del despliegue, importadores, distribuidores y otros agentes económicos), así como a **autoridades públicas** encargadas de la supervisión, control e inspección de estos sistemas y del cumplimiento de las obligaciones normativas españolas y europeas en materia de IA.

<sup>23</sup> Ministerio para la Transformación Digital y de la Función Pública (España). (2025). *Documento de análisis y participación pública sobre el anteproyecto de ley de mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación* [Documento de participación pública]. Consultado el 3 de enero de 2026. Disponible en: <https://avance.digital.gob.es/layouts/15/HttpHandlerParticipacionPublicaAnexos.ashx?k=19128>

<sup>24</sup> Ministerio para la Transformación Digital y de la Función Pública (España). (2025). *Aprobación del anteproyecto de Ley de mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación* [Nota de prensa]. Consultado el 3 de enero de 2026. Disponible en: [https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion\\_ministro/2025/03/2025-03-11/NdPAPLIACM.pdf](https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion_ministro/2025/03/2025-03-11/NdPAPLIACM.pdf)

El Anteproyecto no crea un derecho autónomo de reclamación distinto del previsto en el Reglamento Europeo de IA, pero **operativiza de forma clara la vía de denuncia** como mecanismo de activación del control administrativo. El artículo 29 establece que los **procedimientos sancionadores se inician** de oficio, bien por iniciativa de la propia autoridad competente, por petición razonada de otros órganos administrativos o en virtud de **denuncia de un tercero**, conectando directamente con el derecho a presentar reclamaciones ante autoridades de vigilancia del mercado reconocido en el artículo 85 del RIA. La denuncia debe incluir la identidad de la persona denunciante y un relato de los hechos, si bien no confiere por sí sola la condición de interesado en el procedimiento. De forma complementaria, el Anteproyecto prevé que la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) habilite un **canal externo** de información (artículo 29 Anteproyecto), accesible por medios electrónicos, que permitirá a cualquier persona física informar de manera anónima sobre posibles infracciones, reforzando las vías de alerta temprana frente a usos indebidos de sistemas de IA.

El Anteproyecto define una arquitectura institucional compleja y por sectores. En primer lugar, distingue entre **autoridades notificantes** (art. 4) y **autoridades de vigilancia del mercado** (art. 6), siendo estas últimas las responsables directas de la supervisión del cumplimiento del RIA. La autoridad de vigilancia competente dependerá del sector en el que se utilice el sistema de IA, lo que implica que **distintas autoridades administrativas puedan ejercer funciones de control según el ámbito material afectado**. En este contexto, la **AESIA asume un papel central de coordinación**, participando en la Comisión Mixta de Coordinación de Autoridades de Vigilancia del Mercado (art. 8), concebida como órgano clave para asegurar coherencia, intercambio de información y actuación coordinada entre autoridades.

Desde la perspectiva del acceso a mecanismos de reclamación, el Anteproyecto presenta limitaciones relevantes. En primer lugar, la denuncia se configura principalmente como un **instrumento de activación del poder sancionador**, no como un cauce orientado a la tutela directa de la persona afectada, que no adquiere automáticamente la condición de interesada en el procedimiento. En segundo lugar, la **sectorialización de las autoridades de vigilancia** puede generar dificultades prácticas para identificar el órgano competente, especialmente en casos de sistemas algorítmicos complejos o transversales. En tercer lugar, aunque el artículo 29 fija plazos máximos de resolución (18 meses para infracciones graves y muy graves, y 9 meses para leves), estos plazos pueden resultar **poco compatibles con la necesidad de respuestas ágiles** frente a impactos algorítmicos inmediatos y los tiempos de prescripción (artículo 31). Finalmente, aunque el artículo 34 reconoce la posibilidad de reparación del daño e indemnización, su efectividad dependerá de la articulación práctica con el derecho civil y contencioso-administrativo, así como de la capacidad probatoria de las personas afectadas y la debida investigación por parte de la autoridad competente.

Por último, se trata, de nuevo, de un Anteproyecto **en fase de tramitación parlamentaria**, por lo que su eficacia dependerá de su desarrollo, de la dotación de recursos técnicos y humanos a las autoridades competentes y de la capacidad de estas para abordar reclamaciones relativas a sistemas algorítmicos complejos.

En el **Anexo V** del presente informe se incorpora una figura explicativa del proceso de reclamación previsto en el RIA y en el Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA, mientras que en el **Anexo VI** se incorpora una tabla comparativa de las normas analizadas para el ámbito nacional.

## Normativas sectoriales

Junto al marco específicamente orientado a la gobernanza de la inteligencia artificial, el ordenamiento jurídico español cuenta con **instrumentos sectoriales** consolidados que ya **ofrecen vías de reclamación aplicables** a vulneraciones derivadas del uso de sistemas algorítmicos e IA. Aunque estos instrumentos no se diseñaron expresamente para regular la IA, han comenzado a integrar de forma explícita elementos relacionados con la automatización, la toma de decisiones algorítmica y la transparencia.

La **Ley 15/2022, de igualdad de trato y no discriminación**<sup>25</sup> resulta particularmente relevante para abordar daños algorítmicos con impacto discriminatorio. Sus Títulos IV y V regulan, respectivamente, los mecanismos de tutela frente a la discriminación y el régimen sancionador, reconociendo el derecho a la reparación integral del daño, incluida la indemnización por daños morales. La Ley prevé además la creación de un **organismo estatal independiente para la igualdad de trato y la no discriminación**,<sup>26</sup> con funciones de asistencia a víctimas, recepción de quejas y promoción de acciones, lo que abre la puerta a integrar supuestos de discriminación algorítmica dentro de sus competencias.

Esta orientación se refuerza de manera expresa en el **artículo 23**, dedicado específicamente a la *inteligencia artificial y los mecanismos de toma de decisión automatizados*, imponiendo a las **administraciones públicas la obligación de favorecer mecanismos de minimización de sesgos, transparencia, rendición de cuentas y evaluaciones de impacto** para detectar posibles efectos discriminatorios.

En el **ámbito laboral** encontramos un ejemplo avanzado de **transparencia algorítmica** y litigación efectiva, a partir de la denominada "**Ley Rider**"<sup>27</sup> y del desarrollo jurisprudencial posterior. La obligación de informar sobre el uso de algoritmos que afectan a las condiciones de trabajo ha dado lugar tanto a informes administrativos del Ministerio de Trabajo<sup>28</sup> como a resoluciones judiciales que rechazan la opacidad empresarial respecto al uso de sistemas automatizados en la gestión laboral. En este contexto, la reciente jurisprudencia, incluida la sentencia que declara ilícita la negativa empresarial a reconocer el

<sup>25</sup> Boletín Oficial del Estado (BOE). (2021). Ley 13/2021, de 24 de mayo, de modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [Ley]. Consultado el 25 de enero de 2026. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-1663>

<sup>26</sup> Ministerio de Inclusión, Seguridad Social y Migraciones (España). (2025). *El Gobierno aprueba el nombramiento de D<sup>a</sup> María Teresa Verdugo como presidenta de la Autoridad Independiente para la Igualdad de Trato y la No Discriminación* [Artículo]. Consultado el 3 de enero de 2026. Disponible en: <https://www.inclusion.gob.es/ca/web/oberaxe/w/el-gobierno-aprueba-el-nombramiento-de-d-maria-teresa-verdugo-como-presidenta-de-la-autoridad-independiente-para-la-igualdad-de-trato-y-la-no-discriminacion>

<sup>27</sup> Boletín Oficial del Estado (BOE). (2021). Ley 7/2021, de 20 de mayo, de cambio climático y transición energética [Ley]. Consultado el 3 de enero de 2026. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2021-15767>

<sup>28</sup> Ministerio de Trabajo y Economía Social (MITE-S). (2022). *Guía sobre algoritmos: información en el ámbito laboral y obligaciones empresariales* [Guía]. Consultado el 4 de enero de 2026. Disponible en: [https://www.mites.gob.es/ficheros/ministerio/inicio\\_destacados/Guia\\_Algoritmos\\_ES.pdf](https://www.mites.gob.es/ficheros/ministerio/inicio_destacados/Guia_Algoritmos_ES.pdf)

uso de algoritmos<sup>29</sup> muestra cómo los **mecanismos clásicos de reclamación laboral y judicial pueden adaptarse para abordar conflictos derivados del uso de sistemas algorítmicos**, configurando un precedente relevante para otros sectores.

Estos ejemplos muestran que **cada marco sectorial genera sus propias autoridades, procedimientos y lógicas de reclamación**, dando lugar a un ecosistema fragmentado de tutela frente a daños algorítmicos. No obstante, con independencia del sector afectado, existen **actores y vías transversales** que siguen desempeñando un papel central. Los **órganos jurisdiccionales** constituyen la instancia última de tutela efectiva, con capacidad para controlar decisiones automatizadas y acordar medidas de reparación o indemnización, aunque su acceso suele verse limitado por costes, duración y dificultades probatorias. Asimismo, las **plataformas y proveedores de sistemas de IA** concentran muchos de los impactos algorítmicos y gestionan mecanismos internos de queja y revisión que, sin sustituir las garantías públicas, pueden operar como primer nivel de resolución. Finalmente, las **organizaciones de la sociedad civil, sindicatos y entidades especializadas** resultan clave para asistir a las personas afectadas, articular reclamaciones colectivas o estratégicas y hacer visibles patrones sistémicos de daño algorítmico que difícilmente emergen a través de reclamaciones individuales.

## Estudios de caso en Europa

Con el fin de contrastar el análisis normativo con la práctica existente en otros países europeos, este apartado examina **dos casos que ilustran modelos complementarios de reclamación** frente a vulneraciones derivadas del uso de sistemas algorítmicos. Ambos casos han sido seleccionados por su relevancia para el diseño de mecanismos de reclamación en el contexto europeo y por la transferibilidad de sus aprendizajes al contexto español.

### *Défenseur des droits* y decisiones automatizadas en los servicios públicos (Francia)

El *Défenseur des droits* (DdD) es la figura del Defensor del Pueblo de Francia, creado en 2008 mediante la reforma constitucional que introdujo el **artículo 71.1 en la Constitución francesa**<sup>30</sup> y consolidado por la **Ley orgánica n.º 2011-333**, de 29 de marzo de 2011, relativa al Defensor de los Derechos<sup>31</sup>. La institución integró en un único organismo cuatro entidades previas: la Alta Autoridad para la Lucha contra la Discriminación y por la Igualdad

<sup>29</sup> Audiencia Nacional, Sala de lo Social. (2025). *Sentencia núm. 101/2025, de 4 de julio de 2025 (ROJ: SAN 2867/2025; ECLI: ES:AN:2025:2867)* [Sentencia]. Consultado el 3 de enero de 2026. Disponible en: <https://www.poderjudicial.es/search/AN/openDocument/53f7e6ad5a39dd3fa0a8778d75e36f0d/20250715>

<sup>30</sup> Título XI-A de la Constitución Francesa. El Defensor de los Derechos. Artículo 71-1 "El Defensor de los Derechos velará por el respeto de los derechos y las libertades por parte de las administraciones del Estado, las entidades territoriales, los establecimientos públicos, así como cualquier otro organismo encargado de una misión de servicio público o respecto de la cual la ley orgánica le atribuya competencias."

<sup>31</sup> Legifrance. (2011). *Loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits* [Ley]. Consultada el 18 de febrero de 2026. Disponible en: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000023781167#JORFARTI000023781243>

(HALDE), el Defensor de la Infancia, el Mediador de la República y la Comisión Nacional de Ética Policial.

Actúa como **mecanismo de reclamación extrajudicial, independiente y gratuito**, al que puede acudir cualquier persona, con independencia de su nacionalidad o residencia, que considere que una administración pública ha vulnerado sus derechos. Las reclamaciones pueden presentarse en línea, por correo, por teléfono o en persona ante los delegados territoriales del DdD.

En el ámbito de las decisiones automatizadas, el DdD ha desarrollado una práctica de tutela especialmente adaptada a los **daños mediados por algoritmos en la administración pública**. Su actuación frente al algoritmo de la *Caisse d'allocation familiale* (CAF, Fondo de Subsidios Familiares francés) ilustra cuatro **dimensiones** clave de su eficacia: (1) la **corrección de errores algorítmicos mediante acuerdos amistosos**, que han permitido recuperar prestaciones sociales suspendidas o bloqueadas por fallos en el procesamiento automatizado, incluyendo el pago de atrasos; (2) el **refuerzo de garantías procedimentales y supervisión humana**, recordando a las administraciones que el uso de herramientas algorítmicas no las exime de sus obligaciones de diligencia, examen individualizado y consideración efectiva de las pruebas aportadas; (3) la **complementariedad con la tutela judicial**, actuando de forma paralela a los tribunales y contribuyendo a clarificar estándares jurídicos aplicables a las decisiones algorítmicas; y (4) el **impacto sistémico más allá del caso individual**, mediante recomendaciones e informes temáticos, como el Informe DdD 2024 sobre algoritmos, sistemas de IA y servicios públicos, que identifican patrones recurrentes de daño y orientan la reforma de procedimientos a escala institucional.

Las resoluciones del DdD no son jurídicamente vinculantes como las sentencias judiciales, pero su **peso institucional es considerable**: las administraciones están obligadas a responder a sus intervenciones y a justificar cualquier incumplimiento de sus recomendaciones. La publicidad de los casos y la posibilidad de derivar asuntos a la autoridad judicial o fiscal crean una presión institucional *de facto* eficaz para que las administraciones actúen. Este modelo demuestra que los mecanismos extrajudiciales de reclamación pueden constituir vías efectivas de tutela de derechos frente a decisiones algorítmicas en la administración pública, especialmente cuando integran la resolución individual de reclamaciones con la capacidad de detectar y señalar patrones sistémicos de daño.

## Acciones colectivas de reparación frente a sistemas algorítmicos por parte de Noyb (UE)

**Noyb**<sup>32</sup> es una organización no gubernamental con sede en Austria, especializada en la **aplicación del derecho europeo de protección de datos**, en particular el RGPD y la Directiva ePrivacy. Actúa como organización de litigio estratégico y actuación regulatoria, centrada en impugnar prácticas sistemáticas de tratamiento de datos y algorítmicas que afectan a

<sup>32</sup> NOYB – None of Your Business. (s. f.). *Sitio web institucional*. [Página web] Consultado el 20 de febrero de 2026. Disponible en: <https://noyb.eu/es>

millones de personas en toda la UE, incluidas la publicidad en línea, el perfilado, los sistemas de recomendación y la toma de decisiones automatizada.

A finales de 2024, Noyb fue designada formalmente como **Entidad Habilitada** (*Qualified Entity*) en Austria e Irlanda en virtud de la Directiva (UE) 2020/1828 sobre acciones de representación, lo que le otorga **legitimación para interponer acciones colectivas de reparación en cualquier Estado miembro de la UE**. Esta designación formaliza en el derecho positivo un modelo de acción colectiva que Noyb venía desarrollando de forma estructural desde su fundación, a través de un sistema de mandatos estandarizados que permite a personas de toda Europa autorizar a la organización a actuar en su nombre.

El modelo de actuación de Noyb ha transformado reclamaciones individuales en **intervenciones jurídicas y regulatorias coordinadas con efectos sistémicos**. Dos acciones ilustran su alcance: en primer lugar, en agosto de 2021 presentó **422 reclamaciones RGPD** contra empresas que utilizaban *banners* de *cookies* diseñados para inducir el consentimiento mediante patrones engañosos (*dark patterns*), lo que desencadenó la creación de un grupo de trabajo del Comité Europeo de Protección de Datos (CEPD) y propició cambios generalizados en el diseño de interfaces digitales a escala europea.

En segundo lugar, entre 2020 y 2022, tras la sentencia *Schrems II*, presentó **101 reclamaciones coordinadas** contra empresas europeas que utilizaban herramientas como *Google Analytics* o *Facebook Connect* bajo marcos jurídicos considerados incompatibles con el RGPD, resultando en decisiones vinculantes de las autoridades de protección de datos con alcance práctico en toda Europa. Estas acciones se complementan con iniciativas impulsadas en el marco de la Directiva de Acciones de Representación, como la acción colectiva del *Verbraucherzentrale Bundesverband (vzbv)* contra Meta en Alemania por la filtración de datos de 2021.

A diferencia del modelo del DdD, los resultados de las acciones de Noyb tienen **plena fuerza jurídica**: tanto las sentencias judiciales como las resoluciones de las autoridades de protección de datos derivadas de sus reclamaciones son vinculantes para las entidades demandadas y ejecutables conforme al derecho nacional. La coordinación del CEPD amplifica el alcance de las decisiones individuales de las autoridades de protección de datos de los distintos Estados miembros. Este modelo evidencia que los **mecanismos de acción colectiva son indispensables para abordar daños algorítmicos** difusos que afectan a grandes grupos de personas, en los que la reclamación individual resulta impracticable o ineficiente desde el punto de vista del acceso a la justicia.

Ambos estudios de caso ponen de relieve la **complementariedad de los modelos de reclamación extrajudicial** (DdD) y **judicial-colectiva** (Noyb), y revelan la **necesidad de diseñar mecanismos de tutela capaces de operar tanto a escala individual como colectiva**, y tanto frente a las administraciones públicas como frente a plataformas privadas. Sus aprendizajes se integran en el análisis y las conclusiones del presente informe, y orientan las propuestas que se desarrollarán en las siguientes fases del proyecto.

## Conclusiones del análisis normativo y los estudios de caso

Del análisis se desprende que, en **España**, los mecanismos de reclamación ante vulneraciones de derechos derivadas del uso de sistemas algorítmicos o de IA siguen siendo prácticamente inexistentes o insuficientemente desarrollados, lo que deja a las personas afectadas en una situación **desprotección efectiva**. Además, los proyectos y anteproyectos normativos actualmente en discusión no contemplan, por el momento, sistemas de reclamación específicos ni establecen vías operativas que aseguren una rendición de cuentas real y una reparación efectiva frente a daños algorítmicos o que provienen de la aplicación de IA.

Actualmente, este marco de reclamación frente a vulneraciones derivadas del uso de sistemas algorítmicos e IA se caracteriza por una **fragmentación institucional significativa**, derivada de la coexistencia de múltiples normas y autoridades con competencias parciales y sectoriales. RGPD, RSD y RIA articulan vías de reclamación distintas, gestionadas por autoridades diferentes (AEPD, CNMC, AESIA y otras autoridades de vigilancia del mercado), sin un punto de entrada único ni criterios homogéneos de derivación. En el contexto español, esta fragmentación se intensifica con la incorporación de la AESIA como órgano de coordinación, sin que ello implique una centralización efectiva de la tramitación de reclamaciones. El resultado es un sistema en el que una **misma vulneración algorítmica puede quedar simultáneamente cubierta por varias normas o, por el contrario, no encajar plenamente en ninguna**, generando inseguridad jurídica y riesgo de inacción administrativa.

Otro aspecto a considerar en la fase de implementación es la **densidad normativa existente**, donde persisten vacíos relevantes de protección, especialmente en supuestos en los que los daños algorítmicos no se manifiestan como infracciones claras de una norma sectorial concreta. El RGPD no cubre daños que no impliquen tratamiento de datos personales; el RIA prioriza el cumplimiento normativo del sistema como producto, sin garantizar reparación individual; y el RSD se limita a contextos de intermediación digital. Asimismo, instrumentos como la Carta de Derechos Digitales carecen de mecanismos propios de exigibilidad. Estas lagunas afectan de manera particular a daños colectivos, discriminaciones indirectas, impactos acumulativos o decisiones algorítmicas opacas, que resultan difíciles de encuadrar en los marcos actuales de reclamación.

Desde la **perspectiva de las personas afectadas**, el acceso efectivo a los mecanismos de reclamación se ve obstaculizado por **barreras procedimentales y técnicas**. Identificar la norma aplicable y la autoridad competente requiere un conocimiento jurídico especializado que no puede presumirse. A ello se suma la asimetría de información frente a proveedores y plataformas, la dificultad para acceder a explicaciones comprensibles sobre el funcionamiento de los sistemas algorítmicos y los plazos prolongados de los procedimientos administrativos y judiciales. En el caso del RIA y del Anteproyecto español, además, la denuncia no confiere automáticamente la condición de interesado, lo que debilita la posición procesal de quien ha sufrido el daño y refuerza la percepción de que los mecanismos existentes están orientados al control regulatorio más que a la tutela directa de derechos.

Las limitaciones descritas se **agravan en el caso de sistemas de IA de alto riesgo**, definidos por su impacto potencial en derechos fundamentales como el acceso al empleo, la educación, la protección social, la seguridad o la justicia. En estos contextos, los **daños pueden ser difusos, difíciles de atribuir y de carácter estructural**, afectando de forma desproporcionada a determinados colectivos. La fragmentación competencial, la falta de mecanismos ágiles de suspensión o corrección y la ausencia de cauces claros de reparación temprana incrementan el riesgo de normalización del daño algorítmico antes de que exista una respuesta institucional efectiva. Todo ello pone de manifiesto la **necesidad de mecanismos de reclamación específicos, accesibles y coordinados**, capaces de operar transversalmente en escenarios de IA compleja y de alto impacto.

Los **estudios de caso europeos** examinados en el cuarto apartado aportan evidencia empírica que refuerza y matiza las conclusiones del análisis normativo:

- El **modelo del *Défenseur des droits*** muestra que los **mecanismos extrajudiciales pueden ser altamente eficaces para corregir daños algorítmicos en la administración pública**, especialmente cuando combinan la resolución individual de reclamaciones con la capacidad de señalar patrones sistémicos y formular recomendaciones institucionales de alcance general: el resultado práctico no es solo la reparación de la situación de la persona reclamante, sino la rehumanización del proceso de decisión y la corrección de procedimientos automatizados defectuosos.
- El **modelo de *Noyb***, por su parte, ilustra el **potencial transformador de los mecanismos de acción colectiva**, que permiten agregar reclamaciones individuales frente a prácticas algorítmicas masivas y convertirlas en decisiones vinculantes con efectos estructurales sobre el mercado digital y sobre las prácticas de tratamiento de datos. La complementariedad entre ambos modelos, el no judicial y el colectivo-judicial, subraya que **no existe una respuesta única al problema** de la reclamación frente a daños algorítmicos, sino un **ecosistema de mecanismos complementarios** que deben articularse de forma coherente y accesible.

## BLOQUE II: RESULTADOS Y HALLAZGOS DE LA FASE CUALITATIVA

El presente bloque recoge los principales hallazgos del proceso de investigación cualitativa llevado a cabo en el marco de este informe, a través de nueve entrevistas individuales y dos grupos focales. El objetivo central fue explorar, desde perspectivas plurales y complementarias, la experiencia con mecanismos de reclamación frente a decisiones adoptadas por sistemas de inteligencia artificial (IA) y automatizados, así como las posibilidades de participación ciudadana en su diseño y gobernanza.

Las personas participantes representan un amplio espectro de perfiles profesionales y activistas: sindicatos, activismo de derechos digitales, periodismo especializado, ingeniería, investigación académica, autoridades de protección de datos, litigio estratégico, plataformas de participación democrática. Esta diversidad permite articular un análisis robusto y matizado que atraviesa tanto dimensiones técnico-jurídicas como sociales y políticas.

En el **Anexo VII** de este informe se encuentra detallada la metodología empleada para el análisis cualitativo, así como una descripción anonimizada de los perfiles entrevistados que incorpora el código de la persona o grupo focal (por ejemplo: E1, GF2, etc).

### Barreras de acceso a mecanismos de reclamación

Todas las personas participantes identificaron, desde sus distintas posiciones, un conjunto de barreras estructurales que dificultan o impiden en la práctica el ejercicio del derecho a recurrir decisiones adoptadas por sistemas algorítmicos o de IA. Estas barreras son de naturaleza técnica, jurídica, económica, social y cultural.

### Opacidad técnica: las cajas negras algorítmicas

La barrera más mencionada de manera transversal es la **opacidad de los sistemas**. Los algoritmos utilizados en la toma de decisiones que afectan derechos son, en la mayoría de los casos, inaccesibles no sólo para las personas afectadas, sino también para los operadores que los despliegan y para las personas que se encargan de la supervisión institucional.

### Falta de notificación y reconocimiento del componente algorítmico

Una barrera previa a cualquier mecanismo de reclamación es que la **persona afectada sepa que la decisión que la perjudica fue adoptada o influida por un sistema algorítmico o de IA**. E6 señaló que el artículo 22 del RGPD establece derechos en relación con las decisiones automatizadas, pero su aplicación efectiva depende del cumplimiento de los deberes de

información de los artículos 13 y 14, lo que en la práctica raramente ocurre de manera comprensible.

Relacionado con la falta de notificación también se ha mencionado en diversas entrevistas la falta de respuesta de la Administración Pública cuando se ejerce el **derecho a acceder a la información pública**, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por la Ley de Transparencia. Son pocos los casos donde se comparte información relevante para entender la lógica del sistema y cómo se ha diseñado e implementado.

En este contexto, conviene introducir una **distinción importante entre decisión automatizada y daño algorítmico**. Como señala E9, no todo daño algorítmico deriva de una decisión automatizada en el sentido del artículo 22 del RGPD. Existen supuestos en los que el perjuicio se origina en el propio diseño del sistema (en formularios, categorías o criterios de clasificación) sin que medie una decisión automatizada visible. Casos como el sistema BOSCO o experiencias documentadas en la administración de servicios sociales en Nueva York muestran que la exclusión puede producirse en fases previas, a través de la configuración del sistema.

## Carga individual y asimetría de poder

E7 analizó en profundidad la estructura de la **carga individual de la reclamación**: el sistema legal vigente coloca toda la responsabilidad de impugnar sobre la persona afectada, que debe identificar el daño, buscar asesoramiento, recabar evidencias, navegar procedimientos complejos y asumir costes, mientras que la entidad que desplegó el sistema dispone de recursos técnicos, jurídicos y económicos incomparablemente mayores.

## Complejidad procedimental y fragmentación de responsabilidades

Diferentes actores, como GF2 y E3, señalaron la dificultad adicional que supone **identificar quién es responsable** de una decisión algorítmica, especialmente cuando el sistema es suministrado por un tercero (empresa tecnológica), desplegado por una administración o empresa, y ejecutado por un/a funcionario/a o empleado/a.

Esta fragmentación tiene además una consecuencia poco señalada: actúa como **barrera de acceso también a la vía judicial**. Las personas que agotan las vías administrativas sin resultado llegan a los tribunales ya debilitadas (sin documentación suficiente, sin pruebas del funcionamiento del sistema, sin haber podido acceder a la información necesaria). El caso de Civio con el algoritmo BOSCO ilustra este recorrido: el proceso judicial fue largo y costoso, la sentencia del Tribunal Supremo tardó años en llegar, y a la fecha de este informe sigue sin haber sido cumplida por la administración. La fragmentación institucional y las barreras de acceso a la información, lejos de ser obstáculos solo en el ámbito administrativo, se trasladan y amplifican en el acceso a la tutela judicial efectiva.

## Desconfianza institucional y barreras culturales

GF1 puso de relieve que en comunidades en situación de mayor vulnerabilidad (migrantes, personas sin recursos, personas con menor alfabetización digital, entre otras) existe una **desconfianza estructural hacia las instituciones** que inhibe el ejercicio de cualquier tipo de reclamación.

## Temporalidad y urgencia del daño

Varias personas participantes (E7, GF1, GF2) señalaron la **paradoja temporal de la reclamación algorítmica**: los daños son inmediatos (suspensión de una prestación, pérdida de empleo, denegación de un crédito) pero los procedimientos de reclamación son lentos, costosos y de resultado incierto. Cuando el proceso concluye, el daño ya se ha producido en toda su extensión.

## Buenas prácticas identificadas

A pesar del diagnóstico crítico sobre las barreras existentes, el proceso permitió identificar experiencias de éxito relativo que representan avances significativos en el acceso a mecanismos de reclamación y en la participación en la gobernanza de sistemas de IA.

- **Litigio estratégico** articulado por la sociedad civil: los casos SyRI (E4), las acciones frente a la CAF francesa (E2), el caso de Civio sobre BOSCO demuestran como la combinación de litigio jurídico, investigación y comunicación puede generar cambios sistémicos que benefician a colectivos amplios, incluso cuando los recursos individuales son insuficientes.
- **Uso de herramientas de ingeniería inversa para generar evidencias**: S1 presentó software y metodologías para recolectar y analizar datos de aplicaciones laborales, permitiendo documentar de forma técnica y sistemática vulneraciones para apoyar el litigio estratégico o procesos de reclamación.
- **Negociación colectiva** sobre algoritmos: E1 y E5 describieron convenios colectivos que incorporan cláusulas específicas sobre el uso de algoritmos en la gestión laboral, por ejemplo, el derecho de los comités de empresa a ser informados de los sistemas desplegados y la participación sindical en la evaluación de su impacto.
- **Proactividad de las autoridades de protección de datos**: E6 destacó el valor del monitoreo proactivo por parte de las APDs, que van más allá de la respuesta a reclamaciones individuales y analizan de manera sistemática sectores o tipos de sistemas con mayor potencial de impacto en derechos.
- **Redes de apoyo mutuo y acompañamiento comunitario**: GF1 y GF2 subrayaron el papel de las redes de apoyo entre personas afectadas como mecanismo informal pero efectivo de difusión de información, identificación de patrones de daño y activación de vías de reclamación.

- **Plataformas de participación democrática** en la gobernanza tecnológica: E8 presentó el modelo Decidim como ejemplo de como es posible articular procesos de co-diseño y deliberación pública sobre tecnología de manera accesible e inclusiva.
- **Procesos internos de gobernanza y auditoría como mecanismo preventivo:** E9 destacó la importancia de incorporar mecanismos de evaluación desde las fases más tempranas del diseño de sistemas de IA, como el *AI Strategy Kit* de I2CAT.
  - Este enfoque propone auditorías internas que clasifican riesgos desde la fase de propuesta y que integran perfiles multidisciplinares (jurídicos, de estrategia política europea, de sociedad digital y de ingeniería).
  - Combina métricas técnicas tradicionales (como *accuracy* o *F1*) con métricas de equidad (como paridad demográfica o igualdad de oportunidades).
  - La lógica subyacente “si llega una reclamación, hemos fracasado” introduce una perspectiva preventiva que complementa los enfoques reactivos predominantes, donde todos los riesgos deben de ser identificados al principio.
  - Este modelo se apoya además en el enfoque de cuádruple hélice (academia, sector público, sector privado y sociedad civil) como marco para integrar a las comunidades afectadas desde la fase de diseño.

## Malas prácticas identificadas

Simétricamente, el proceso identificó **patrones recurrentes** de malas prácticas que contribuyen a la opacidad, al daño y a la impunidad de los sistemas algorítmicos y de IA.

- **Diseño sin participación** de las comunidades afectadas: los sistemas son diseñados por equipos técnicos sin contacto con quienes van a ser afectados, lo que genera sesgos invisibles que solo emergen cuando el daño ya se ha producido.
- Despliegue de sistemas de **IA sin evaluación previa** de impacto en derechos: la ausencia de evaluaciones de impacto algorítmico (EIA) como requisito previo al despliegue fue mencionada de manera unánime como una mala práctica estructural.
- E9 señala que los modelos de IA, a diferencia del software tradicional, pueden **degradarse si no se monitorizan y reentrenan**, y que esto raramente se contempla en los contratos de despliegue. El daño puede llegar no en el momento de lanzamiento, sino meses después, cuando el modelo ha derivado. Es una mala práctica estructural que afecta especialmente a la administración pública.
- **Ausencia de mecanismos de apelación** específicos para decisiones algorítmicas: las vías de reclamación existentes son genéricas y no están adaptadas a la especificidad técnica del daño algorítmico o de IA.

- **Fragmentación y dilución de responsabilidades:** la cadena de subcontratación tecnológica permite que ningún actor asuma plena responsabilidad sobre los efectos de los sistemas desplegados.
- **Supervisión humana formal, pero no real:** muchos sistemas contemplan formalmente una supervisión humana de las decisiones automatizadas, pero en la práctica el funcionario o empleado ratifica de manera rutinaria lo que el sistema decide.
- **Uso de IA en contextos de alta vulnerabilidad** sin salvaguardias: servicios sociales, gestión de prestaciones, evaluación de riesgos de menores son exactamente los contextos en los que el impacto de las decisiones algorítmicas es más grave y la capacidad de respuesta de las personas afectadas es menor.
- Diseño de hipótesis detrás de los sistemas de IA, tanto en el sector público como en el privado, los sistemas parten de **asunciones incorrectas** o simplificadoras de los contextos que pretenden abordar o en los que van a operar. Estas premisas erróneas estructuran el sistema desde su origen y reproducen decisiones injustas a gran escala.
- **Ausencia de mecanismos efectivos de responsabilidad** en el sector público y privado. En el sector público no existe en la práctica un mecanismo claro y operativo para exigir responsabilidad a la administración por los daños causados por sistemas algorítmicos o de IA. En el sector privado, aunque formalmente pueden existir canales de reclamación o cumplimiento normativo, pocas veces se traducen en mecanismos internos realmente efectivos, independientes y accesibles para las personas afectadas.
- **Uso de la IA como estrategia de captación de financiación:** mecanismo por el que los incentivos de financiación, pública y privada, favorecen incluir "inteligencia artificial" en las propuestas independientemente de si es la herramienta adecuada para resolver el problema que se pretenden abordar. Esto no es una decisión malintencionada, es una consecuencia del sistema de incentivos.

## Recomendaciones clave emergentes del proceso

Del análisis integrado de las aportaciones en las entrevistas y grupos focales emergen tres recomendaciones clave que sintetizan los consensos más sólidos del proceso. Estas recomendaciones son complementarias y mutuamente reforzadoras.

### **RECOMENDACIÓN 1: Garantizar participación real de comunidades afectadas en el diseño y supervisión de sistemas de IA**

La participación de las personas que van a ser afectadas por los sistemas algorítmicos debe ser una condición de diseño, no un añadido cosmético posterior. Se recomienda:

- Establecer la participación de comunidades afectadas como requisito obligatorio en las evaluaciones de impacto algorítmico (EIA), antes del despliegue de cualquier sistema de alto riesgo.
- La definición misma del problema y de la “pregunta inicial” que el sistema pretende resolver debe ser co-diseñada con las comunidades potencialmente impactadas, integrando un marco participativo estructurado desde el inicio del proceso.
- Financiar metodologías participativas accesibles que superen la brecha digital y sean inclusivas para comunidades con menor alfabetización digital.
- Incorporar representantes de las comunidades afectadas en los órganos de supervisión y control de sistemas de IA, garantizando su participación significativa y formación adecuada.
- Apoyar y financiar procesos de investigación acción participativa con comunidades afectadas, reconociendo su conocimiento experto sobre los efectos de los sistemas algorítmicos.
- Promover plataformas de participación democrática en la gobernanza de la IA, siguiendo modelos como Decidim, que garanticen la transparencia del proceso y la trazabilidad de las decisiones adoptadas.
- Impulsar una educación digital integral y continua, orientada no solo a competencias técnicas, sino también a la comprensión cívica de los derechos digitales, los riesgos algorítmicos y los mecanismos de reclamación disponibles. La alfabetización algorítmica debe concebirse como una política pública estructural y no como una intervención puntual.

## **RECOMENDACIÓN 2: Crear mecanismos de reclamación colectiva, accesibles y especializados**

Los mecanismos actuales de reclamación frente a decisiones algorítmicas e de IA son insuficientes para el tipo de daños que estos sistemas generan. Se recomienda diseñar e implementar mecanismos específicos con las siguientes características:

- Procedimientos simplificados, en lenguaje accesible, disponibles en formato presencial y digital, con plazos razonables y respuestas en tiempo útil.
- Posibilidad de acciones colectivas y reclamaciones grupales, con legitimación activa para organizaciones de la sociedad civil y sindicatos.
- Gratuidad total, incluyendo asistencia jurídica especializada en IA y acceso a peritaje técnico independiente.
- Inversión de la carga de la prueba: quien despliega el sistema debe demostrar su equidad y conformidad con la ley, no quien sufre el daño.

- Salvaguardias explícitas frente a represalias por el ejercicio del derecho de reclamación.
- Integración de las APDs como receptoras de reclamaciones algorítmicas con procedimientos específicos y capacidad técnica reforzada.

### **RECOMENDACIÓN 3: Reforzar la transparencia y la auditoría independiente como condición para el despliegue**

La transparencia real es la condición previa de cualquier mecanismo de reclamación efectivo. Se recomienda:

- Crear y mantener registros públicos, comprensibles y accesibles de todos los sistemas de IA de alto riesgo en uso, especialmente en la administración pública.
- Obligación de publicar *model cards*, gráficos de causalidad y *dashboards* de métricas de equidad (*demographic parity, equal opportunity*) para todos los sistemas de alto riesgo en la administración pública, con formatos accesibles que no requieran conocimiento técnico avanzado para ser interpretados.
- Se propone asimismo la creación de un observatorio público de sistemas algorítmicos/IA y de daños asociados, que permita centralizar información, identificar patrones transversales y fortalecer la rendición de cuentas.
- Establecer como obligación legal la realización de evaluaciones de impacto antes del despliegue de cualquier sistema de alto riesgo, con participación de personas afectadas y publicación de los resultados.
- Garantizar el derecho a una explicación significativa, no meramente formal o técnica, de cualquier decisión con efectos sobre derechos o condiciones de vida, que sea comprensible y permita ejercer derechos de impugnación.
- Establecer un régimen de auditorías técnicas independientes de sistemas de IA de alto riesgo, con acceso garantizado a auditores independientes acreditados y publicación de los resultados.
- Reforzar los recursos técnicos y humanos de las autoridades de supervisión para que puedan ejercer un control efectivo sobre sistemas de IA complejos. La capacitación continua de estas autoridades es una condición indispensable para evitar que la complejidad técnica de los sistemas supere la capacidad de control público.
- Obligación contractual de mantenimiento y monitoreo continuo de los modelos desplegados, con responsabilidad explícita en el contrato, registros auditables de seguimiento y posibilidad de exigir responsabilidad cuando la degradación del modelo no fue detectada ni corregida.

## **BLOQUE III: GUÍA PRÁCTICA PARA LA PUESTA EN MARCHA DE PROCESOS PARTICIPATIVOS PARA CREAR SISTEMAS DE RECLAMACIÓN**

En base al análisis jurídico, los estudios de caso y los hallazgos de las entrevistas y grupos focales, esta guía propone un camino para revertir esta situación mediante un **proceso participativo híbrido, que combine canales presenciales y digitales, orientado a crear o mejorar sistemas de reclamación accesibles, efectivos y con enfoque de derechos humanos**. Este enfoque incluye el diseño de procedimientos específicos para reclamaciones algorítmicas, como la admisión simplificada, la inversión de la carga de la prueba y el establecimiento de plazos urgentes en casos de daños graves, así como el desarrollo de formularios en lenguaje claro y accesible, sometidos a testeo con personas usuarias para garantizar su comprensión, usabilidad y eficacia.

No existe un modelo único ni definitivo: la guía ofrece un marco orientador que cada organización, autoridad o proceso deberá adaptar a su contexto específico.

### **Por qué un proceso participativo híbrido**

La investigación mostró que los mecanismos de reclamación suelen diseñarse sin participación de las personas más afectadas. Cuando solo se contempla el canal digital, se excluye a quienes tienen menor alfabetización digital, que suelen ser exactamente quienes más sufren las consecuencias de los sistemas algorítmicos. La hibridación, presencial y digital, es una condición de equidad, no una opción técnica.

### **Principios transversales: enfoque de derechos humanos**

Todos los módulos de esta guía están atravesados por los siguientes principios, derivados directamente de los hallazgos del proceso de investigación:

- **Universalidad y no discriminación:** el sistema debe ser accesible para cualquier persona, con especial atención a quienes enfrentan más barreras (personas migrantes, con menor alfabetización digital, sin recursos económicos).
- **Participación significativa:** las personas afectadas no son solo usuarias del sistema de reclamación, sino actoras en su diseño, implementación y evaluación. La participación debe tener impacto real en las decisiones.
- **Transparencia y rendición de cuentas:** el sistema debe ser comprensible para las personas que lo usan, y quienes lo gestionan deben rendir cuentas de sus decisiones y resultados.

- **Acceso a la reparación:** el objetivo no es únicamente procesar reclamaciones, sino garantizar que las personas afectadas reciban una reparación efectiva: corrección de la decisión, compensación del daño y prevención de su repetición.
- **Protección frente a represalias:** ejercer el derecho de reclamación no puede tener consecuencias negativas para la persona que lo ejerce.
- **Mejora continua:** el sistema debe aprender de las reclamaciones recibidas y adaptarse de manera continuada.

## Cómo usar esta guía

La guía se organiza en tres módulos que pueden leerse de manera independiente o en conjunto:

- **Módulo 1. Ventanilla única (One Stop Shop):** proceso para crear un punto de acceso único para reclamaciones relacionadas con IA, que coordine a múltiples actores.
- **Módulo 2. Autoridades e instituciones:** proceso de adaptación interna para autoridades como el Defensor del Pueblo, las APDs u otras instituciones que necesitan mayor conocimiento y especialización en daños algorítmicos.
- **Módulo 3. Organizaciones de la sociedad civil:** herramientas para que organizaciones, clínicas jurídicas y redes comunitarias puedan acompañar a personas afectadas y articularse con el ecosistema más amplio.

Cada módulo incluye: (a) marco conceptual y justificación, (b) hoja de ruta por fases, (c) orientaciones para el diseño híbrido, y (e) ejemplos y referencias.

Además, en el **Anexo VIII** puedes encontrar, **para el diagnóstico inicial y para cada uno de los tres módulos, una lista de verificación de puesta en marcha**, pensada específicamente para **facilitar la aplicación de esta guía por actores que se planteen diseñar mecanismos de reclamación**.

## Antes de empezar: diagnóstico y mapa del ecosistema

Antes de iniciar cualquiera de los tres módulos, resulta imprescindible realizar un diagnóstico del contexto y mapear los actores existentes. Este paso previo evita duplicar esfuerzos, identifica alianzas posibles y permite adaptar las propuestas al contexto específico. El siguiente mapa recoge los actores clave identificados en el proceso de investigación y su rol en un sistema de reclamación algorítmico efectivo:

Actor	Rol en el ecosistema
-------	----------------------

<b>Autoridades de Protección de Datos (APDs)</b>	Recepción de reclamaciones, investigación, sanción. Competencia legal en tratamientos automatizados. Necesitan más capacidad técnica especializada.
<b>Defensor del Pueblo / Síndic de Greuges</b>	Supervisión de la administración pública. Potencial rol como punto de acceso neutral y de confianza para reclamaciones contra organismos públicos.
<b>Inspección de Trabajo</b>	Control del cumplimiento del ET (Ley Rider) en gestión algorítmica laboral. Necesita formación técnica específica.
<b>Sindicatos y comités de empresa</b>	Representación colectiva de trabajadores. Negociación de cláusulas sobre algoritmos en convenios. Formación de representantes.
<b>ONGs</b>	Acompañamiento jurídico y psicosocial a personas afectadas. Litigio estratégico. Alfabetización algorítmica comunitaria.
<b>Plataformas de participación democrática</b>	Co-diseño de mecanismos. Herramientas digitales para la participación. Ejemplo: Decidim.
<b>Periodismo especializado en IA</b>	Visibilización de casos. Presión pública. Educación ciudadana. Documentación de patrones de daño.
<b>Comunidades afectadas y redes de apoyo mutuo</b>	Conocimiento experto de los efectos reales de los sistemas algorítmicos. Participación en el diseño del sistema. Difusión de información.
<b>Investigación académica</b>	Producción de evidencia técnica y jurídica. Apoyo a litigios. Evaluación de impacto.
<b>Profesionales técnicos especializados en gobernanza de la IA</b>	Personal técnico (ingeniero/as de datos, científico/as de datos, etc.). Gobernanza de sistemas de IA. Identificación temprana de riesgos, implementación de métricas de equidad y explicabilidad. Agentes de cambio internos clave para transformar cultura de las entidades.

MÓDULO

1

## Ventanilla única (*one stop shop*)

Punto de acceso único · Coordinación de actores · Proceso híbrido

### Qué es y por qué es necesaria

Una ventanilla única de reclamaciones algorítmicas es un **punto de acceso centralizado** donde cualquier persona puede presentar una reclamación relacionada con una decisión adoptada por un sistema algorítmico o de IA, sin necesidad de saber de antemano a qué autoridad u organismo corresponde el caso. La ventanilla recibe la reclamación, la orienta hacia el actor competente y hace seguimiento hasta su resolución.

El proceso de investigación mostró que uno de los principales obstáculos para el ejercicio efectivo de los derechos de reclamación es la fragmentación del sistema. En muchos casos, la persona afectada no puede identificar con claridad qué le está ocurriendo ni si se trata de una vulneración de derechos; incluso cuando reconoce el daño, desconoce qué derechos le asisten o a qué autoridad debe dirigirse.

Esta situación se agrava por la falta de coordinación entre organismos, que con frecuencia deriva a las personas de una institución a otra, generando desorientación, desgaste y, en muchos casos, el abandono del proceso. Frente a este problema estructural, la creación de mecanismos de ventanilla única se plantea como una solución clave para simplificar el acceso y resolver dudas iniciales, centralizar la entrada de reclamaciones y garantizar una gestión más coherente y eficaz.

#### Principios de la ventanilla única

- **Punto de entrada único:** la persona solo necesita saber que ha sufrido un daño o que algo no funciona correctamente, sin necesidad de identificar quién es el responsable ni qué norma resulta aplicable.
- **Espacio de orientación y verificación de dudas:** la ventanilla única no únicamente actúa ante reclamaciones formales, sino que ofrece un canal accesible para que las personas puedan consultar, contrastar y comprender si están siendo afectadas por un sistema algorítmico o de IA, qué derechos podrían estar en juego y qué opciones tienen.
- **Gratuidad total:** ningún coste para la persona que reclama o consulta, en ningún canal (presencial, telefónico o digital).
- **Derivación y seguimiento activo:** la ventanilla no solamente recibe, sino que orienta, deriva de forma informada y acompaña el caso hasta su resolución, evitando que la persona quede desatendida entre distintas instituciones.

- **Lenguaje accesible:** toda comunicación se realiza en lenguaje claro, comprensible y sin tecnicismos jurídicos ni informáticos.
- **Multi-canal e híbrida:** acceso presencial, telefónico y digital, con equivalencia real entre todos los canales.
- **Protección de datos de la persona reclamante:** especial cuidado con la confidencialidad y la minimización de datos, particularmente frente a la entidad reclamada.

## Hoja de ruta: fases del proceso

Fase	Nombre y actores principales	Qué se hace
<b>F0</b> 1-2 meses	<b>Diagnóstico y alianzas</b> <i>Equipo promotor + actores clave</i>	Mapeo de actores, análisis del contexto legal, identificación de casos piloto, primeras reuniones de alianza con APD, Defensor del Pueblo, organizaciones y sindicatos.
<b>F1</b> 2-3 meses	<b>Co-diseño participativo</b> <i>Equipo promotor + personas afectadas + actores del ecosistema</i>	Proceso participativo (talleres presenciales y en línea) para definir: que reclamaciones se aceptan, como se reciben, quien las deriva, que plazos aplican, como se comunica con la persona reclamante.
<b>F2</b> 2-3 meses	<b>Diseño técnico e institucional</b> <i>Equipo técnico + instituciones</i>	Desarrollo o adaptación del sistema digital (formulario accesible, base de datos, trazabilidad). Firma de acuerdos de colaboración con actores del ecosistema. Formación del equipo de la ventanilla.
<b>F3</b> 3-4 meses	<b>Piloto con casos reales</b> <i>Equipo ventanilla + personas afectadas + actores referidos</i>	Funcionamiento piloto con casos reales acompañados. Evaluación continua. Ajustes sobre la marcha. Documentación de aprendizajes.
<b>F4</b>	<b>Consolidación y escalado</b>	Comunicación pública de la ventanilla. Formación de nuevos actores. Ampliación de casos y sectores

<p>Continuo</p>	<p><i>Todos los actores del ecosistema</i></p>	<p>cubiertos. Publicación de informes periódicos de transparencia.</p>
<p><b>F5</b></p> <p>Cada 6-12 meses</p>	<p><b>Evaluación y mejora continua</b></p> <p><i>Equipo ventanilla + comunidades afectadas + evaluación externa</i></p>	<p>Evaluación participativa de resultados. Actualización del protocolo. Informe público de impacto. Ajuste del diseño del sistema.</p>

## Diseño híbrido: presencial y digital

El enfoque híbrido no es opcional: es una condición de equidad y de calidad institucional. El canal digital puede facilitar el acceso ágil, la trazabilidad y la escalabilidad, mientras que la presencialidad aporta cercanía, confianza y mayor capacidad de acompañamiento en situaciones complejas; ambos deben garantizar el mismo nivel de atención y posibilidades reales de resolución.

### Canal presencial

- Puntos de atención en espacios de confianza: centros comunitarios, bibliotecas, sindicatos, sedes de organizaciones sociales. No en edificios institucionales que generen desconfianza.
- Atención personalizada por personas formadas en derechos digitales, informadas en trauma y con habilidades de comunicación inclusiva y no violenta.
- Materiales en lenguaje claro, con versión en diferentes idiomas y en formatos accesibles (lectura fácil, pictogramas).
- Posibilidad de acompañamiento por personas de confianza de la comunidad (mediadores, intérpretes).
- Sin requisito previo de documentación técnica: el equipo de atención ayuda a identificar y documentar el caso.

### Canal digital

- Formulario accesible, compatible con lectores de pantalla y en múltiples idiomas.
- Proceso guiado paso a paso, con preguntas en lenguaje sencillo: no es necesario saber que fue un algoritmo para poder reclamar.
- Posibilidad de adjuntar documentación de apoyo (capturas, cartas, notificaciones recibidas).
- Acuse de recibo automático con número de caso e información sobre los próximos pasos.
- Canal de seguimiento en tiempo real del estado de la reclamación.

- Opción de continuar el proceso de manera presencial en cualquier momento.
- Referencia a Decidim u otras plataformas *open source* como base tecnológica con garantías democráticas.

## Ejemplos y referencias

Decidim (Barcelona): plataforma de participación democrática *open source*, usada para co-diseño de políticas públicas. Su modelo de gobernanza participativa puede adaptarse al co-diseño de mecanismos de reclamación.

Caso SyRI (Países Bajos): la coalición de organizaciones que litigó contra el SyRI funcionó de facto como una ventanilla informal de acceso a reclamaciones colectivas. El modelo de coordinación entre organización social, clínica jurídica y comunicación pública es un referente.

Redes de apoyo mutuo: las redes informales de apoyo en comunidades afectadas actúan como canal de primer acceso. Una ventanilla única efectiva debería formalizarse sobre estas redes existentes. Organizaciones que trabajan tradicionalmente en ejes de discriminación concretos que tengan acceso directo a estas redes de apoyo mutuo.

MÓDULO

2

## Autoridades e instituciones

Especialización · Coordinación · Procedimientos adaptados

### Por qué las autoridades necesitan adaptarse

Las autoridades con competencia en la supervisión de sistemas algorítmicos, Autoridades de Protección de Datos (APDs), Defensor del Pueblo, Inspección de Trabajo, AESIA, entre otras, disponen de los instrumentos legales necesarios para actuar, pero en la mayoría de los casos carecen de la capacidad técnica, los procedimientos específicos y la cultura institucional necesarios para hacerlo de manera efectiva.

A ello se suma la falta de coordinación operativa entre estas entidades, que no siempre cuentan con mecanismos claros de derivación entre sí ni con tiempos de tramitación y rendición compatibles, lo que dificulta una respuesta coherente y oportuna.

El proceso de investigación identificó, además, que las personas afectadas tienen una desconfianza significativa hacia las instituciones públicas, lo que exige que las autoridades no solo adapten sus procedimientos, sino también su cultura de atención y comunicación.

### Mapa de autoridades y sus competencias

Actor	Rol en el ecosistema
<b>Autoridades de Protección de Datos (APDs)</b>	Supervisión de los derechos recogidos en el RGPD. Competencia para investigar, ordenar medidas correctoras y sancionar. Pueden actuar de oficio.
<b>Defensor del Pueblo / Síndic de Greuges</b>	Supervisión de la actuación de las administraciones públicas. Puede investigar el uso de IA en servicios públicos (SEPE, servicios sociales, policía predictiva). No tiene poder sancionador pero si gran capacidad de influencia.
<b>Inspección de Trabajo y Seguridad Social</b>	Supervisión del cumplimiento del Estatuto de los Trabajadores, en concreto las disposiciones de la Ley Rider. Condiciones de trabajo en entornos de gestión algorítmica y de IA.
<b>Autoridad de supervisión del AI Act (AESIA)</b>	Supervisión del cumplimiento del Reglamento de IA, especialmente sistemas de alto riesgo. En proceso de constitución. Competencias a determinar en coordinación con APDs.

### Tribunales de Justicia

Litigio estratégico para casos de daño algorítmico. No son mecanismo de acceso fácil, pero generan precedentes de alto impacto sistémico. Reparación a través de la vía administrativa, administrativa-contenciosa, civil o social.

## Hoja de ruta para autoridades

Fase	Nombre y actores principales	Qué se hace
<b>F0</b> 1-2 meses	<b>Diagnóstico interno</b> <i>Dirección + equipo técnico-jurídico</i>	Mapeo de reclamaciones actuales relacionadas con IA. Análisis de brechas de capacidad técnica. Identificación de casos sin resolver por falta de conocimiento. Revisión del marco legal aplicable.
<b>F1</b> 3-6 meses	<b>Formación y sensibilización</b> <i>Todo el personal de atención + responsables técnicos</i>	Formación en funcionamiento de sistemas de IA, sesgos algorítmicos y marcos legales. Sesiones con personas afectadas para entender la perspectiva de quién reclama. Visitas a organizaciones sociales que trabajan en el ámbito.
<b>F2</b> 3-6 meses	<b>Adaptación de procedimientos</b> <i>Equipo jurídico + equipo técnico + participación de personas usuarias</i>	Diseño de procedimientos específicos para reclamaciones algorítmicas: admisión simplificada, inversión de la carga de la prueba y establecimiento de plazos urgentes en casos de daños graves. Desarrollo de formularios en lenguaje claro y accesible, con testeo con personas usuarias para garantizar su comprensión, usabilidad y eficacia.
<b>F3</b> Continuo	<b>Coordinación inter-institucional</b> <i>Responsables institucionales</i>	Firma de protocolos de derivación con otras autoridades. Integración en la ventanilla única (Modulo 1). Creación de grupo de trabajo inter-institucional sobre IA y derechos.
<b>F4</b> Continuo	<b>Monitoreo proactivo</b> <i>Equipo técnico especializado</i>	Análisis sistemático de sectores de alto riesgo (servicios sociales, empleo, policía, crédito, etc.). Investigaciones de oficio. Publicación de informes de vigilancia. Coordinación con investigación académica.

## Adaptación de procedimientos

### Admisión y tramitación simplificada

Los procedimientos actuales de reclamación ante las APDs u otras autoridades requieren que la persona que reclama sea capaz de identificar la infracción legal concreta, lo que resulta imposible sin conocimientos jurídicos y técnicos. Un procedimiento adaptado debería:

- Aceptar reclamaciones basadas en la descripción del daño sufrido, sin necesidad de identificar la norma infringida.
- Disponer de personal de atención capaz de ayudar a la persona reclamante a articular su caso y recolectar/certificar evidencias.
- Ofrecer un formulario guiado en lenguaje sencillo, tanto en formato digital como presencial.
- Garantizar acuse de recibo con información clara sobre los próximos pasos y plazos.
- Si el caso no corresponde a la autoridad receptora, ser capaces de derivar de manera eficiente y coordinada hacia la autoridad competente, evitando que la persona quede desatendida o perdida entre distintos organismos.

### Inversión de la carga de la prueba

La investigación señaló de manera unánime que la carga individual de la prueba es una de las principales barreras. Las autoridades deberían adaptar sus procedimientos para que, una vez aportados indicios razonables de daño algorítmico, sea la entidad que desplegó el sistema quien deba demostrar que este funciona de manera equitativa y conforme a la ley.

### Monitoreo proactivo y actuación de oficio

Más allá de la respuesta reactiva a reclamaciones individuales, las autoridades deberían desarrollar capacidad de monitoreo proactivo: identificar sectores o sistemas con alto potencial de daño y actuar de oficio, sin esperar a que las personas afectadas presenten reclamaciones individuales. Esta capacidad requiere:

- Equipos técnicos especializados con acceso a herramientas de auditoría de algoritmos e IA.
- Cooperación con investigación académica y organizaciones de la sociedad civil que documentan casos.
- Registros públicos de sistemas de IA que faciliten el monitoreo.
- Protocolos de actuación de oficio cuando se detectan patrones de daño sistémico.

El monitoreo proactivo debe activarse desde el momento mismo en que una administración pública o entidad privada con impacto público despliega un nuevo sistema. Las autoridades deberían solicitar de inmediato la **documentación mínima de explicabilidad**: *model cards* que describan el proceso de decisión y los datos utilizados, gráficos de causalidad que permitan identificar puntos críticos de fallo o discriminación, y métricas de equidad (paridad demográfica, igualdad de oportunidad) junto con las métricas de rendimiento habituales. La ausencia de esta documentación debería considerarse un incumplimiento exigible por sí misma. La transparencia no puede depender de la existencia de una reclamación previa.

Además, es crítico garantizar el **mantenimiento continuo de los modelos de IA**: un sistema puede funcionar correctamente al desplegarse, pero degradarse posteriormente si no se monitoriza y reentrena. Los contratos de despliegue deberían especificar explícitamente quién es responsable del mantenimiento, cómo se monitoriza el rendimiento y qué protocolos se activan si el modelo se degrada.

## Ejemplos y referencias

APDCAT (Autoritat Catalana de Protecció de Dades): mencionada en el proceso como ejemplo de autoridad de protección de datos que ha avanzado en el monitoreo proactivo de sistemas algorítmicos. Su enfoque de análisis sectorial (no solo respuesta a reclamaciones individuales) es un modelo a seguir.

Defensor del Pueblo neerlandés y el caso SyRI: el recurso judicial que derribó el SyRI fue posible en parte gracias a la intervención de organizaciones de la sociedad civil, pero el Defensor del Pueblo neerlandés había documentado previamente los efectos del sistema. La articulación entre supervisión institucional y litigio estratégico es un modelo replicable.

NYC Local Law 144 (Nueva York, 2023): primera ley que exige auditorías anuales independientes de sesgos en sistemas de IA utilizados en procesos de contratación laboral. A diferencia del Reglamento Europeo de IA, su escala acotada y sus obligaciones concretas (plazos fijos, auditorías independientes, publicación de resultados), la hacen directamente aplicable y verificable. Referente de regulación concreta y exigible para organizaciones en fases iniciales de implementación.

Observatorio de Ética en Inteligencia Artificial de Catalunya (OEIAC): observatorio vinculado a la Universidad de Girona, con criterios de evaluación de sistemas más rigurosos que la clasificación estándar de riesgos del EU AI Act. Modelo de observatorio distribuido y cercano al territorio que puede complementar a las grandes agencias de supervisión nacional.

Modelo PIO (OEIAC): metodología de autoevaluación previa al despliegue cuya primera pregunta es ¿es la IA realmente la mejor solución para este problema?. Incorpora criterios de impacto social, ambiental y de derechos desde la fase de diseño, y actualmente se aplica con un nivel de exigencia superior a la clasificación de riesgos estándar.

MÓDULO

3

## Organizaciones de la sociedad civil

Acompañamiento · Alfabetización · Articulación

El tercer bloque temático aborda cómo garantizar la participación real de las personas afectadas y de la sociedad civil en el diseño, la evaluación y la gobernanza de los sistemas algorítmicos. La participación es entendida no como un requisito formal, sino como una condición para que los sistemas sean justos y legítimos.

### El rol de las organizaciones en el ecosistema

Las organizaciones de la sociedad civil, ONG de derechos digitales, sindicatos, redes comunitarias, asociaciones de personas usuarias, etc. ocupan un lugar clave en el ecosistema de reclamaciones algorítmicas/IA. Son el punto de contacto más próximo y de mayor confianza para muchas de las personas afectadas, y tienen la capacidad de traducir los problemas concretos de las personas en demandas jurídicas, políticas y comunicativas. Este papel de intermediarias es fundamental para personas que no accederán directamente a ningún organismo institucional por desconocimiento del idioma, vulnerabilidad económica o desconfianza histórica hacia las instituciones.

La investigación mostró que las organizaciones no solo acompañan casos individuales: identifican patrones sistémicos de daño, generan evidencia que puede usarse en litigios estratégicos, contribuyen a la alfabetización algorítmica de las comunidades y conectan a las personas afectadas con el ecosistema más amplio de actores.

### Hoja de ruta para organizaciones

Fase	Nombre y actores principales	Qué se hace
<b>F0</b> 1-2 meses	<b>Mapeo y posicionamiento</b> <i>Equipo de la organización</i>	Análisis de casos de IA que afectan a las comunidades con las que trabajas. Identificación de alianzas con otras organizaciones, clínicas jurídicas y sindicatos. Definición del rol de la organización en el ecosistema (acompañamiento individual, alfabetización, litigio estratégico...).
<b>F1</b>	<b>Formación interna</b>	Formación básica en derechos digitales, funcionamiento de sistemas de IA y marcos legales (RGPD, AI Act, etc.).

2-3 meses	<i>Equipo técnico y de atención</i>	Desarrollo de protocolos de identificación y documentación de casos de daño algorítmico/IA.
<b>F2</b> Continuo	<b>Alfabetización comunitaria</b> <i>Equipo de la organización + comunidad</i>	Talleres y sesiones de sensibilización con las comunidades. Materiales en lenguaje accesible. Formación de personas de las propias comunidades como agentes de primera atención ( <i>peer educators</i> ).
<b>F3</b> Continuo	<b>Acompañamiento de casos</b> <i>Equipo jurídico y de apoyo</i>	Recepción y documentación de casos. Orientación jurídica. Derivación a autoridades competentes o clínicas jurídicas. Acompañamiento durante el proceso. Documentación de patrones de daño.
<b>F4</b> Continuo	<b>Articulación con el ecosistema</b> <i>Responsables de la organización</i>	Participación en la ventanilla única (Modulo 1). Coordinación con autoridades (Modulo 2). Contribución a procesos de litigio estratégico. Comunicación pública de casos con consentimiento.
<b>F5</b> Continuo	<b>Incidencia</b> <i>Toda la organización</i>	Uso de los casos documentados para incidencia. Participación en consultas públicas. Propuestas de mejora de mecanismos de reclamación basadas en evidencia. Identificación de patrones y posibilidad de acciones conjuntas entre personas afectadas de las comunidades.

## Acompañamiento comunitario efectivo

### Protocolo de primera atención

El protocolo de primera atención es el instrumento que permite a cualquier persona de la organización recibir un caso de posible daño algorítmico/IA, aunque no sea especialista en la materia. Debe incluir:

- Preguntas de identificación del daño: ¿Qué pasó? ¿Qué decisión te afectó? ¿Quién la tomó? ¿Cuándo te enteraste?
- Preguntas de documentación: ¿Tienes alguna comunicación escrita (carta, email, notificación)? ¿Sabes si fue una decisión automática o tomada por una persona?
- Orientación sobre los próximos pasos: derivación interna o externa, según el caso.

- Registro del caso en formato estandarizado para facilitar la identificación de patrones.
- Información clara sobre qué puede esperar la persona: plazos, posibilidades de resolución, apoyo disponible.

## Documentación de patrones de daño

Más allá del caso individual, las organizaciones tienen un papel clave en la documentación de patrones de daño sistémico que puedan fundamentar acciones colectivas o de oficio. Cada caso debe registrarse de manera que permita identificar:

- El tipo de sistema algorítmico implicado (gestión laboral, acceso a prestaciones, crédito, policía predictiva...).
- El sector o entidad que lo despliega.
- El tipo de daño (discriminación, privación de un derecho, pérdida económica, daño reputacional...).
- El perfil de las personas afectadas (para identificar si hay patrones de discriminación sistemática).
- El resultado del proceso de reclamación (resuelto, derivado, sin resolución...).

## Herramientas de alfabetización algorítmica

La alfabetización algorítmica es una condición previa para que las personas puedan reconocer cuando están siendo afectadas por un sistema de IA y activar sus derechos. El objetivo no es formar técnicamente a las personas, sino dotarlas del vocabulario y los conceptos mínimos para identificar el daño y saber qué hacer.

Además, debemos tener en cuenta que el daño algorítmico puede producirse a través del diseño de formularios, la selección de variables o los criterios de un sistema, sin que ninguna decisión esté automatizada. Reconocer el daño no requiere identificar una “decisión automatizada”.

### Contenidos clave de un taller de alfabetización algorítmica

1. ¿Qué es un sistema de IA y cómo se usa en tu vida cotidiana? Ejemplos concretos: redes sociales, búsqueda de empleo, acceso a crédito, servicios públicos, trabajo en plataformas.
2. ¿Cómo puede un sistema de IA afectarte negativamente? Discriminación, opacidad, error sin posibilidad de corrección.

3. ¿Qué derechos tienes? Derecho a explicación, derecho a impugnar, derecho a no ser objeto de decisiones automatizadas en determinados contextos, derecho a indemnización, etc.
4. ¿Cómo puedes identificar si una decisión que te afectó fue automática? Indicios y preguntas qué hacer.
5. ¿A dónde puedes ir a reclamar? Mapa de actores y mecanismos disponibles en tu contexto.
6. ¿Cómo documentar lo que te pasó para poder reclamar? Conservar evidencias, plazos, formato de la reclamación.

Los talleres deben desarrollarse en espacios de confianza para la comunidad, en el idioma de las personas participantes, con metodologías participativas que partan de las experiencias concretas de las personas (no de definiciones abstractas), y con materiales visuales y en lectura fácil. La duración recomendada es de 2 a 3 horas, con un máximo de 15-20 personas por sesión.

## Ejemplos y referencias

Sindicato de Manteros o Fundación Secretariado Gitano: organizaciones de base con alta confianza comunitaria de personas que enfrentan múltiples barreras de acceso a derechos. Ejemplos de cómo organizaciones arraigadas en la comunidad pueden actuar como intermediarias de primer acceso para personas que no se acercarían a ningún organismo institucional. Capaces de generar estadísticas y evidencia sobre discriminación sistémica que de otro modo quedaría invisible.

Formación específica, como la que ofrece FUNDAE: las personas técnicas que diseñan e implementan sistemas algorítmicos o de IA, como científicos/as de datos, ingenieros/as, necesitan formación específica en equidad, privacidad y explicabilidad, comparable a las formaciones FUNDAE en otras áreas. La alfabetización algorítmica debe alcanzar también a quienes construyen los sistemas, no solo quienes los usan.

## RECOMENDACIONES FINALES

Los resultados de este informe evidencian que los mecanismos de reclamación constituyen una pieza clave para que la regulación de los sistemas algorítmicos y de la inteligencia artificial sea realmente efectiva. Sin vías accesibles para denunciar, impugnar y obtener reparación frente a daños concretos, los derechos reconocidos en los distintos marcos normativos corren el riesgo de quedar en un plano meramente declarativo. En este sentido, los mecanismos de reclamación operan como el eslabón que conecta la regulación abstracta con la tutela real y cotidiana de los derechos humanos en contextos digitales. No obstante, para que esta conexión sea completa y los mecanismos de reclamación desplieguen todos sus efectos para la protección de derechos, es necesaria la ejecución por diferentes actores clave de una serie de acciones complementarias.

Por un lado, los **tomadores de decisiones** pueden:

- **Accionar normas que contemplen las vulneraciones de derechos derivadas del uso de algoritmos e IA desde el prisma de la reparación individual**, contemplando un daño que vaya más allá de la protección de datos personales, de la lógica de vigilancia del mercado y seguridad del producto y de los destinatarios de servicios de plataformas digitales.
- En paralelo a lo anterior, **tramitar las normas que adaptan las diferentes normativas europeas** (RSD a través del Proyecto de Ley 121/000068 y RIA a través del Anteproyecto de Ley para el Buen Uso y la Gobernanza de la IA), alcanzando los consensos necesarios para su pronta aprobación.
- **Conocer e interiorizar las buenas prácticas y casos de estudio replicables** en torno a los mecanismos de reclamación, algunos de los cuales se contemplan en este informe.

Por otro lado, las **autoridades de vigilancia y control** pueden:

- **Simplificar y mejorar la accesibilidad de los procesos de reclamación**, acompañando a las personas afectadas que sufren un daño, aunque no conozcan la norma que resulta aplicable a su caso, adaptando a lenguaje claro los materiales puestos a disposición de la ciudadanía, o formando a personal para la atención directa, entre otras cuestiones.

Finalmente, las **organizaciones de la sociedad civil** que actúan como punto de contacto con comunidades afectadas, pueden:

- **Reforzar sus capacidades y protocolos de respuesta** para el acompañamiento a personas o grupos sociales afectados por decisiones algorítmicas y de IA, generando evidencias y documentando los daños producidos.

- **Fomentar la alfabetización algorítmica** entre sus comunidades y con otras organizaciones de la sociedad civil, mejorando la detección de los daños por sistemas algorítmicos y de IA e incrementando la capacidad de reacción y, en su caso, reclamación ante los mismos.

## **SOBRE LA INVESTIGACIÓN**

### **Licencia y derecho de uso:**

Este documento es resultado de la investigación “Co-creación de mecanismos de reclamación ante vulneraciones de derechos por sistemas algorítmicos e inteligencia artificial” (Convenio c-38/23-ot), cuyos resultados son propiedad conjunta de La Fundación Salvador Soler - Political Watch y de la Entidad Pública Empresarial Red.es, de acuerdo con el Real Decreto Legislativo 1/1996, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

### **Investigadoras:**

Mireia Orra i De Salsas, Alex Haché y Eva Cruells López de ALIA (Associació Cultural de Dones per a la Recerca i l'Acció).

### **Coordinación del proyecto:**

Political Watch con la colaboración de la Coalición IA Ciudadana.

### **Participantes:**

Arnau Monterde (Ayuntamiento de Barcelona); Bastien Le Querrec (La Quadrature du Net); Beatriz Martos Vergara (Amnistía Internacional España); Belen Luna Sanz; Carla Garcia (Ayuntamiento de Barcelona); Carlos Bajo Erro (Oxfam Intermón); Daniel Cruz Fuentes (CCOO de Catalunya); Esther Paniagua, periodista y analista tecnológica; Francesc Xavier Urios Aparisi (Autoritat Catalana de Protecció de Dades - APDCat); Gala Pin Ferrando; Javier Sáez del Álamo (Fundación Secretariado Gitano); José Varela Ferrío (UGT); Judith Membrives i Llorens (Lafede - Justícia Global); Karlos Castilla Juárez (Institut de Drets Humans de Catalunya, IDHC); Marta Cruells (Barcelona Supercomputing Center - BSC); Menta (nombre anonimizado, Fembloc); Pablo Jiménez Arandia; Pablo Martín Muñoz (Political Watch); Paula Llera Colunga (Political Watch); Raquel Bello Collado (SIE Digital, Servei d'Intervenció Especialitzada en Violències Masclistes Digitals); Rebeca -Beka- Iglesias (Fundació i2CAT); Virginia Álvarez (Amnistía Internacional España).

## ANEXOS

- **ANEXO I.** Aportaciones clave del ámbito internacional para el diseño de mecanismos de reclamación.
- **ANEXO II.** Aportaciones clave del ámbito europeo para el diseño de mecanismos de reclamación.
- **ANEXO III.** Proceso de reclamación en base a la LOPDGDD y el RGPD.
- **ANEXO IV.** Proceso de reclamación en base al RSD.
- **ANEXO V.** Proceso de reclamación en base al RIA.
- **ANEXO VI.** Aportaciones clave del ámbito español para el diseño de mecanismos de reclamación.
- **ANEXO VII.** Metodología y fuentes de la fase cualitativa; perfiles anonimizados de los participantes del proceso cualitativo.
- **ANEXO VIII.** Listas de verificación para la puesta en marcha del diagnóstico inicial y cada uno de los tres módulos.

## ANEXO I. Aportaciones clave del ámbito internacional para el diseño de mecanismos de reclamación.

Instrumento internacional	Qué exige	Cómo reclamar	Límites
Recomendación General número 36 - CERD <sup>33</sup>	La discriminación algorítmica puede existir <b>sin intención discriminatoria</b> , lo que exige mecanismos sensibles a daños estructurales y sistémicos.	Los Estados deben garantizar <b>recursos efectivos y accesibles</b> , incluso frente a tecnologías complejas y opacas.	<b>Soft law</b> : su eficacia depende de la <b>capacidad institucional</b> y de su traducción a procedimientos nacionales.
Informe ONU Empresas y DDHH - Sector tecnológico (A/HRC/50/56) <sup>34</sup>	Las <b>empresas</b> tecnológicas tienen <b>responsabilidad directa de respetar los derechos humanos</b> en todo el ciclo de vida de los sistemas.	Los mecanismos de reclamación deben <b>combinar vías judiciales, administrativas y empresariales</b> , sin exclusiones.	Los mecanismos empresariales pueden fallar por <b>falta de independencia, transparencia y carácter vinculante</b> .
Informe ONU sobre adquisición e implantación de IA (A/HRC/59/53) <sup>35</sup>	Los Estados <b>no pueden delegar su responsabilidad</b> en proveedores tecnológicos mediante contratación pública.  Importancia de los <b>mecanismos internos</b> .	Deben existir mecanismos de reclamación desde la fase de adquisición, no solo tras el despliegue. = <b>Ciclo completo</b> .	Riesgos de <b>opacidad contractual y dependencia técnica</b> que bloquean reclamaciones efectivas.
Recomendación UNESCO sobre la Ética de la IA <sup>36</sup>	La protección de derechos exige integrar <b>evaluaciones de impacto, rendición de</b>	Promueve <b>canales accesibles de denuncia</b> , auditorías independientes y	Falta de procedimientos exigibles: requiere <b>concreción normativa</b>

<sup>33</sup> Comité para la Eliminación de la Discriminación Racial (CERD). (2020). *Recomendación general núm. 36 (2020), sobre la prevención y combate del perfilado racial por parte de las fuerzas del orden* [Recomendación general]. Consultado el 26 de diciembre de 2025. Disponible en: <https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-recommendation-no-36-2020-prevention-and>

<sup>34</sup> Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR). (2022). *A/HRC/50/56: La aplicación práctica de los Principios Rectores sobre las Empresas y los Derechos Humanos a las actividades de las empresas tecnológicas* [Informe]. Consultado el 26 de diciembre de 2025. Disponible en: <https://www.ohchr.org/es/documents/thematic-reports/ahrc5056-practical-application-guiding-principles-business-and-human>

<sup>35</sup> Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR). (2025). *A/HRC/59/53: Adquisición e implantación de tecnologías de inteligencia artificial: velar por su conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos* [Informe]. Consultado el 28 de diciembre de 2025. Disponible en: <https://www.ohchr.org/es/documents/thematic-reports/ahrc5953-artificial-intelligence-procurement-and-deployment-ensuring>

<sup>36</sup> UNESCO - Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2022). *Recomendación sobre la ética de la inteligencia artificial* [Recomendación]. Consultado el 26 de diciembre de 2025. Disponible en: <https://www.unesco.org/es/articulos/recomendacion-sobre-la-etica-de-la-inteligencia-artificial>

	<b>cuentas y sostenibilidad.</b>	participación de comunidades afectadas.	<b>nacional</b> para ser operativa.
Principios de la OCDE sobre IA <sup>37</sup>	La IA debe ser <b>responsable, transparente y centrada en las personas</b> , con supervisión humana.	Los marcos de gobernanza deben permitir <b>revisión de decisiones y respuesta ante impactos adversos</b> .	No reconoce derechos subjetivos ni vías directas de reclamación: depende de marcos jurídicos posteriores.
Recomendación CM/Rec(2020)1 – Consejo de Europa <sup>38</sup>	Los sistemas algorítmicos deben respetar <b>derechos procesales del CEDH</b> (arts. 6, 13 y 14).	Exige <b>remedios efectivos</b> , revisión imparcial y <b>contestabilidad</b> (derecho a ser oído).	No vinculante, pero con <b>alto valor interpretativo</b> para jueces y autoridades administrativas.
Convenio Marco sobre IA – Consejo de Europa (CETS 225) <sup>39</sup>	La tutela frente a la IA pasa de principios a <b>obligaciones jurídicas</b> vinculantes.	Obliga a garantizar <b>remedios efectivos, información e impugnación</b> , judicial y administrativa.	Su impacto dependerá de la <b>ratificación y transposición efectiva</b> por los Estados.

Fuente: elaboración propia.

<sup>37</sup> Organisation for Economic Co-operation and Development (OECD). (2019/2024). *OECD AI Principles* [Recomendación]. Consultado el 26 de diciembre de 2025. Disponible en: <https://www.oecd.org/en/topics/ai-principles.html>

<sup>38</sup> Consejo de Europa, Comité de Ministros. (2020). *Recomendación CM/Rec(2020)1 del Comité de Ministros a los Estados miembros sobre los impactos de los sistemas algorítmicos en los derechos humanos* [Recomendación]. Consultado el 26 de diciembre de 2025. Disponible en: <https://search.coe.int/cm?i=09000016809e1154>

<sup>39</sup> Consejo de Europa, Tratado Serie No. 225. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* [Convenio]. Consultado el 26 de diciembre de 2025. Disponible en: <https://rm.coe.int/1680afae3c>

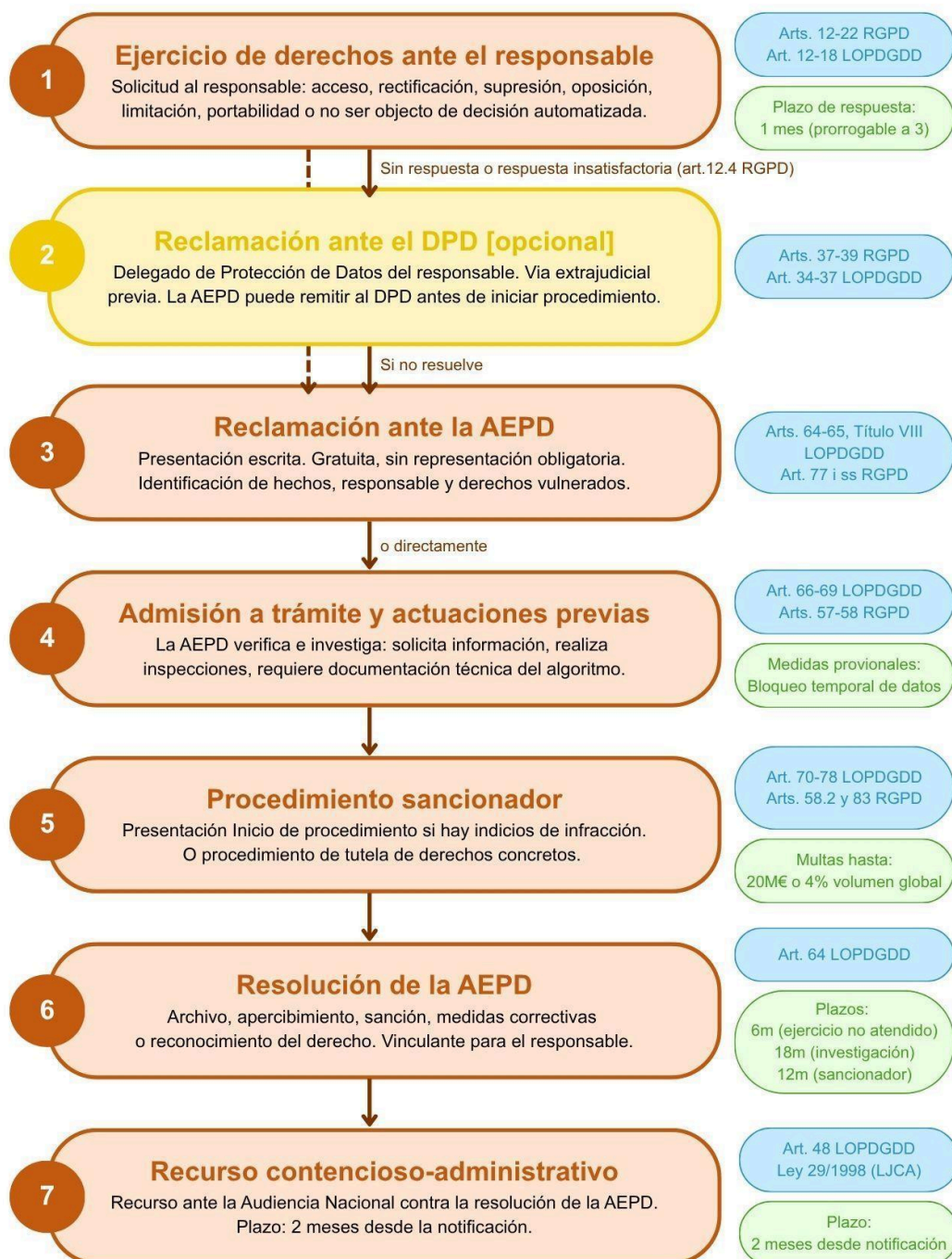
## ANEXO II. Aportaciones clave del ámbito europeo para el diseño de mecanismos de reclamación.

Elemento	RGPD (2016/679)	RSD (2022/2065)	RIA (2024/1689)
Lógica regulatoria principal	Protección de derechos fundamentales vinculados a datos personales.	Protección de derechos de los destinatarios del servicio y del entorno digital.	Seguridad del producto y vigilancia del mercado.
Sujeto central de protección	Persona interesada (titular de datos).	Destinatario del servicio (usuario).	Cumplimiento normativo del sistema de IA.
Existencia de derecho explícito de reclamación	Sí, derecho individual claro (art. 77).	Sí, derecho del destinatario del servicio (art. 53)	Sí, derecho a reclamar ante autoridad de vigilancia (art. 85).
Tipo de vía de reclamación	Administrativa ante autoridad de control + judicial.	Administrativa ante Coordinador de Servicios Digitales + mecanismos internos del proveedor.	Administrativa ante autoridad de vigilancia del mercado.
Rol de las autoridades administrativas	Autoridades de control independientes con funciones cuasi-jurisdiccionales.	Coordinadores nacionales con funciones de supervisión e inspección.	Autoridades de vigilancia del mercado con funciones de supervisión e inspección.
Capacidad de activar reparación individual	Alta: incluye indemnización por daños materiales e inmateriales (art. 82).	Media: derecho a indemnización reconocido (art. 54), condicionado al derecho nacional.	Baja: orientado a corrección del sistema, no a reparación individual directa.
Relación con otros recursos judiciales	Expresa y estructural (arts. 78 y 79).	Complementaria, sin exclusión de otras vías.	Subsidiaria y complementaria ("sin perjuicio de otros recursos").
Principales limitaciones prácticas	Dificultad de comprender lógicas algorítmicas; alcance limitado a datos personales.	Fragmentación procedimental y complejidad transfronteriza.	No concebido como vía de tutela individual; dependencia de capacidades técnicas.
Valor para la co-creación de mecanismos de reclamación	Modelo sólido de derechos individuales y procedimiento.	Modelo híbrido que combina derechos, supervisión y mecanismos internos.	Modelo de alerta y detección que debe complementarse con vías de derechos.

Fuente: elaboración propia.

## ANEXO III. Proceso de reclamación en base a la LOPDGDD y el RGPD.

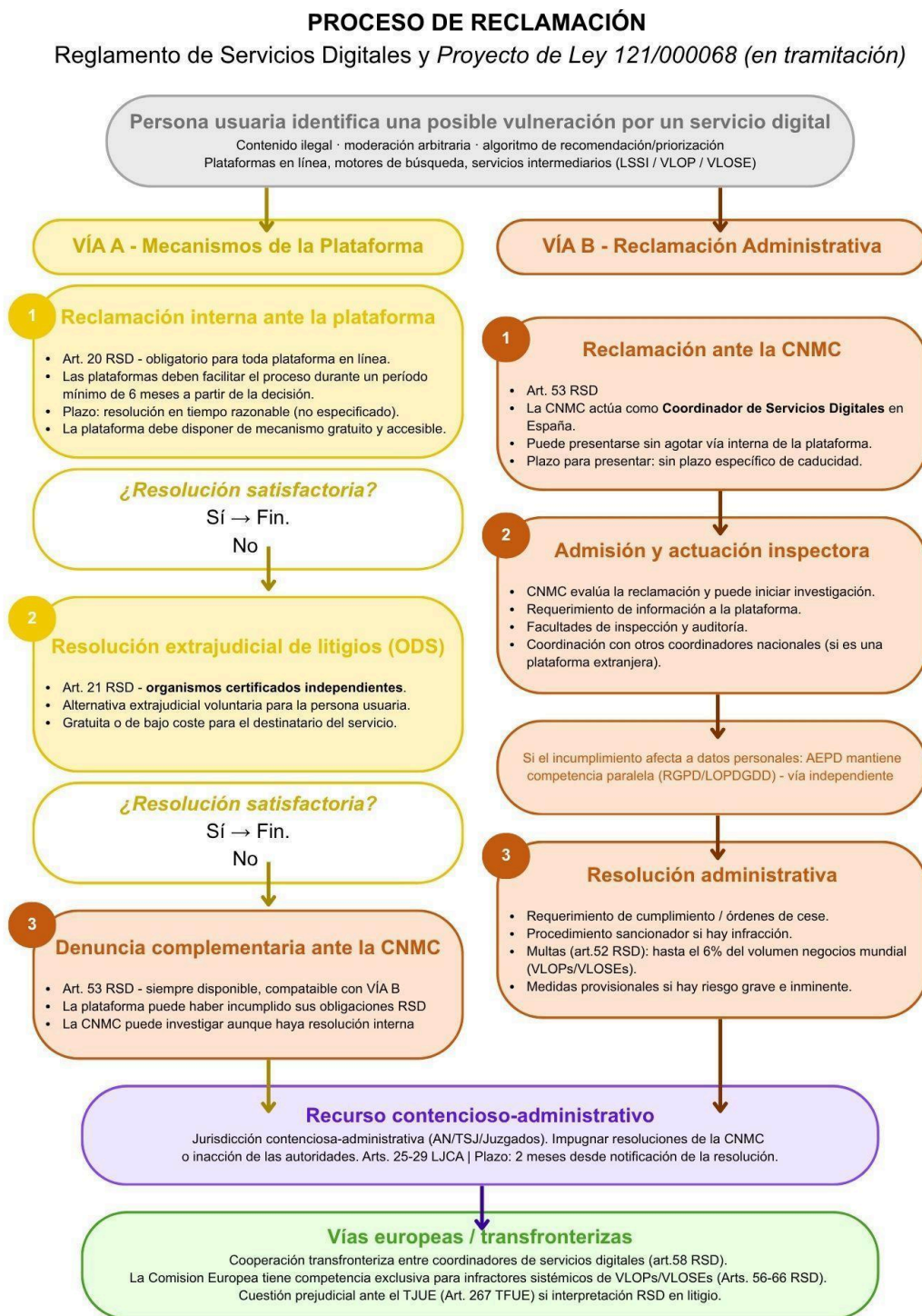
### PROCESO DE RECLAMACIÓN LOPDGDD · RGPD · Ante la AEPD



**\*LIMITACIÓN:** Este proceso aplica únicamente cuando el daño algorítmico/IA implica tratamiento de datos personales (art.4.1 RGPD). Daños sin datos identificables pueden quedar fuera de este marco.

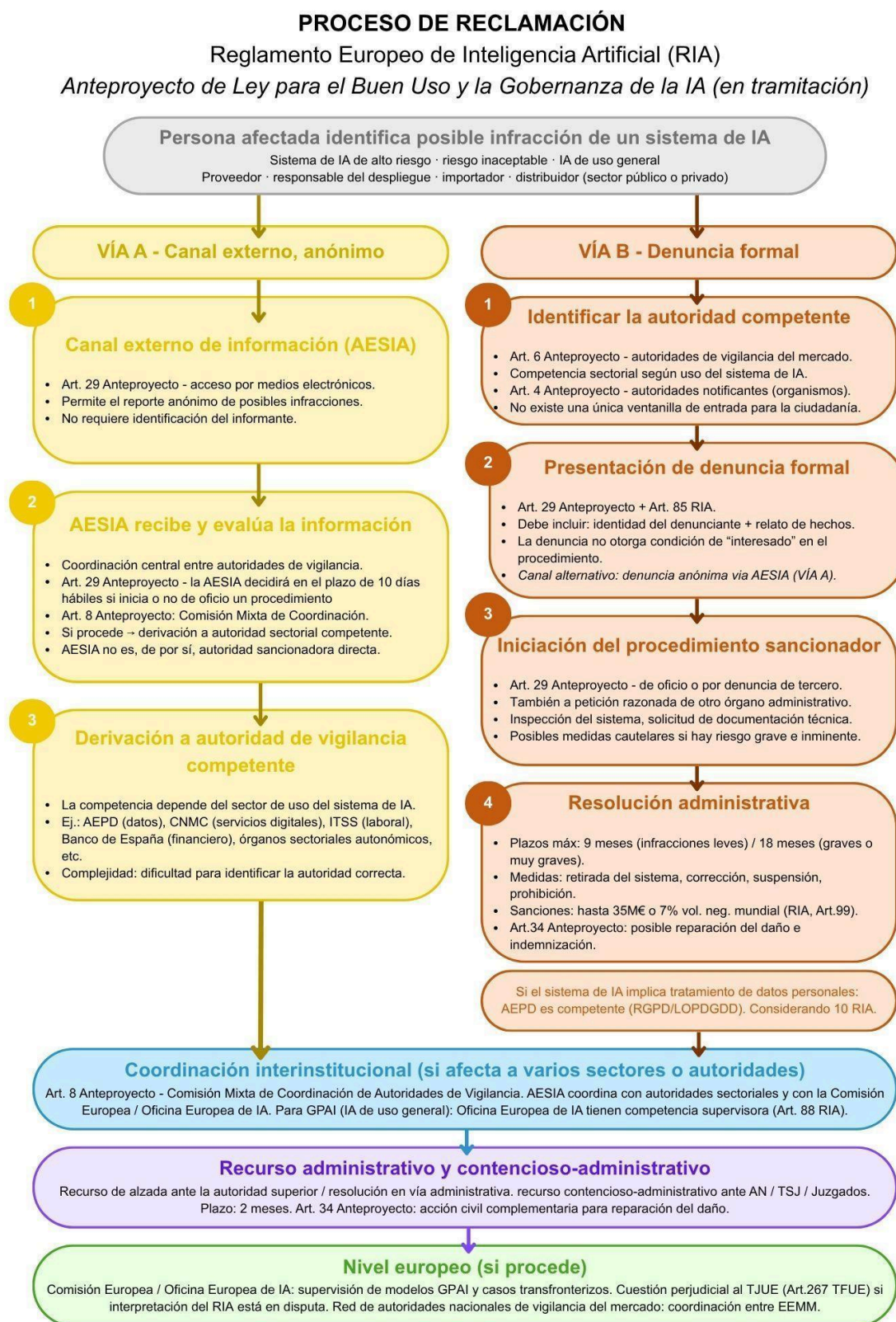
Fuente: elaboración propia.

## ANEXO IV. Proceso de reclamación en base al RSD.



Fuente: elaboración propia.

## ANEXO V. Proceso de reclamación en base al RIA.



Fuente: elaboración propia.

## ANEXO VI. Aportaciones clave del ámbito español para el diseño de mecanismos de reclamación.

Elemento	LOPDGDD (AEPD)	Proyecto Ley - RSD (CNMC)	Anteproyecto Gobernanza IA (AESIA)
		<u>En tramitación</u>	<u>En tramitación</u>
Autoridad principal	<b>AEPD</b> y autoridades autonómicas.	<b>CNMC</b> (Coordinador de Servicios Digitales).	Autoridades de vigilancia del mercado (sectoriales), con coordinación de <b>AESIA</b> .
Acceso al mecanismo	Reclamación directa de la persona afectada.	Reclamación del destinatario del servicio.	Denuncia de cualquier persona física o jurídica.
Activación del procedimiento	A instancia de parte; posible derivación previa a DPD o mecanismos extrajudiciales.	Denuncia ante CNMC que activa supervisión administrativa.	De oficio o por denuncia; canal externo incluso anónimo.
Condición de la persona reclamante	En principio parte interesada en el procedimiento, aunque no siempre es así.	Denunciante; no adquiere automáticamente condición de interesado.	Denunciante; no adquiere automáticamente condición de interesado.
Tipo de resolución	Resolución administrativa.	Resolución administrativa.	Resolución administrativa.
Efectos jurídicos	Medidas correctivas, sanciones, posible indemnización.	Órdenes de actuación, sanciones, coordinación europea.	Retirada, corrección del sistema, sanciones.
Capacidad reparadora	Baja, contempla indemnización, pero no indemniza directamente.	Baja, contempla indemnización, pero no indemniza directamente.	Muy baja.
Precedentes relevantes	Numerosas resoluciones AEPD	Aún incipientes (dependiente de implementación del RSD)	Inexistentes (norma en fase de anteproyecto)

Fuente: elaboración propia.

## ANEXO VII

### Metodología y fuentes de la fase cualitativa

Se realizaron nueve entrevistas individuales semiestructuradas en profundidad y dos grupos focales. Las entrevistas tuvieron una duración media de entre 60 y 90 minutos. Los grupos focales contaron con entre tres y siete personas participantes cada uno. El trabajo de campo fue grabado, transcrito y analizado mediante análisis temático cualitativo. Todos los perfiles han sido anonimizados y se identifican solo por su perfil profesional o activista genérico.

### Participantes del proceso (perfiles anonimizados)

Código	Perfil profesional/activista (anonimizado)
E1	Sindicalista / Responsable de digitalización en confederación sindical (sector servicios). Experto en negociación colectiva sobre algoritmos y gestión algorítmica en empresas.
E2	Activista y jurista en derechos digitales (organización de defensa de derechos civiles digitales). Especialista en litigio estratégico frente a sistemas de IA en la administración pública.
E3	Periodista especializado/a en inteligencia artificial y nuevas tecnologías. Autor/a de reportajes sobre opacidad algorítmica, regulación de la IA y sus impactos sociales.
E4	Investigador/a en derechos digitales, vigilancia algorítmica y justicia de datos. Ha trabajado en casos emblemáticos de discriminación algorítmica en Europa.
E5	Sindicalista / Persona experta en condiciones laborales y digitalización en confederación sindical. Especialista en economía de plataformas y derechos de trabajadores digitales.
E6	Responsable técnico/a-jurídico/a de autoridad regional de protección de datos. Persona experta en aplicación del RGPD a sistemas de decisión automatizada.
E7	Abogado/a y activista en litigio estratégico de derechos digitales. Especialista en acceso a la justicia, reparación colectiva e inversión de la carga de la prueba en contextos algorítmicos.
E8	Responsables de plataforma pública de participación democrática digital (co-entrevista con dos personas). Expertas en co-diseño de tecnología con metodologías participativas.
E9	Ingeniero/a senior especializado/a en DevOps y MLOps, con experiencia en orquestación de procesos, tecnología y equipos en proyectos críticos de I+D+i y sistemas interactivos complejos.
GF1	Grupo Focal 1: Representantes de organizaciones que trabajan en temas de derechos digitales, derechos humanos y participación. Muy enfocados en los daños y discriminaciones que provienen de la Administración Pública.
GF2	Grupo Focal 2: Actores de la sociedad civil, periodistas e instituciones públicas con experiencia en investigar y abordar daños en el entorno digital.
*S1	<i>Sesión con equipo experto en ingeniería inversa aplicada a entornos laborales y protección de datos. La sesión incluyó revisión de metodología, herramientas técnicas, resultados preliminares y discusiones sobre litigio estratégico y participación de trabajadores en experimentos de recopilación y análisis de datos.</i>

## ANEXO VIII

### Lista de verificación del diagnóstico inicial

Además, antes de iniciar el proceso, puede ser útil responder a las preguntas de diagnóstico previo para ajustar el módulo o módulos que mejor se adaptan a la situación diagnosticada. Con las respuestas a estas preguntas, podrás decidir por dónde empezar (ventanilla única, adaptación de autoridades u organizaciones), qué actores priorizar en el proceso participativo y qué ajustes son necesarios en la hoja de ruta.

#### Diagnóstico previo: preguntas clave

- ¿Qué **actores** del mapa anterior están activos en tu territorio o sector?
- ¿Qué colectivos y comunidades están siendo más afectados por sistemas algorítmicos en tu contexto? ¿Cuáles tienen menos capacidad de acceso a mecanismos de reclamación?
- ¿Existe voluntad institucional de los actores clave (autoridades, empleadores, etc.) para participar?
- ¿Existen ya **mecanismos** de reclamación sobre IA en tu contexto? ¿Cuáles son sus limitaciones principales?
- ¿Qué marcos legales son relevantes en tu contexto (RGPD, ET, AI Act, legislación nacional)?
- ¿Hay experiencias de procesos participativos previos sobre los que construir?
- ¿Se ha valorado si la inteligencia artificial es realmente la solución más adecuada para el problema identificado, o existen alternativas que puedan resolverlo con menores riesgos y mayor eficiencia?
- ¿Qué **recursos** (humanos, económicos, tecnológicos) están disponibles para el proceso?
- ¿Cuál es el nivel de alfabetización digital de las personas a las que quieres llegar?

### Lista de verificación de puesta en marcha del módulo 1 de ventanilla única

#### Lista de verificación: Ventanilla única

##### Fase 0 - Diagnóstico y alianzas

- Mapa de actores del ecosistema completado

- Análisis del marco legal aplicable (RGPD, AI Act, legislación nacional) realizado
- Al menos 3 actores del ecosistema comprometidos con el proceso (APD / AESIA / Defensor del Pueblo / organización social)
- Al menos 2 personas de comunidades directamente afectadas implicadas desde el inicio
- Recursos mínimos asegurados para el proceso (equipo, espacios, traducción si procede)

### **Fase 1 - Co-diseño**

- Al menos 2 talleres presenciales y 2 sesiones en línea de co-diseño realizadas
- Protocolo de atención co-diseñado con personas afectadas y actores del ecosistema
- Criterios de admisibilidad de reclamaciones definidos de manera participativa
- Acuerdos de derivación con al menos 2 actores competentes (APD, inspección de trabajo, clínica jurídica...)
- Mecanismos de seguimiento y comunicación con la persona reclamante definidos

### **Fase 2 - Diseño técnico e institucional**

- Formulario digital accesible diseñado y probado con personas usuarias reales
- Canal presencial operativo con espacios y personas formadas
- Acuerdos de colaboración firmados o formalizados con actores del ecosistema
- Equipo formado en: derechos digitales, comunicación inclusiva, protocolo de atención
- Sistema de trazabilidad de casos operativo

### **Fase 3 - Piloto**

- Al menos 10 casos piloto acompañados y documentados

- Registro de aprendizajes y propuestas de mejora
- Primera evaluación participativa realizada con personas usuarias y actores del ecosistema

## Lista de verificación de puesta en marcha del módulo 2 de adaptación de autoridad e instituciones

### Lista de verificación: Autoridades e instituciones

#### Diagnostico y formación

- Inventario de reclamaciones relacionadas con IA recibidas en los últimos 2 años realizado
- Análisis de brechas de capacidad técnica completado
- Al menos el 50% del personal de atención al público formado en derechos digitales básicos
- Al menos 2 personas técnicas con formación especializada en auditoria de sistemas algorítmicos y de IA
- Sesiones de escucha activa con personas afectadas y organizaciones de la sociedad civil realizada

#### Adaptación de procedimientos

- Formulario de reclamación sobre IA en lenguaje sencillo diseñado y publicado
- Protocolo de admisión simplificada de reclamaciones algorítmicas aprobado
- Procedimiento de inversión de carga de la prueba incorporado en el reglamento interno
- Plazos de urgencia para daños graves (suspensión de prestaciones, pérdida de empleo, etc.) establecidos
- Sistema de seguimiento activo del caso y comunicación periódica con la persona reclamante operativo

### **Coordinación y monitoreo**

- Protocolo de derivación firmado con al menos 2 otras autoridades competentes
- Integración o conexión con la ventanilla única (Modulo 1) formalizada
- Plan de monitoreo proactivo de sectores de alto riesgo aprobado
- Informe público anual de actividad en materia de IA comprometido
- Participación en grupo de trabajo inter-institucional sobre IA y derechos establecida

### **Lista de verificación de puesta en marcha del módulo 3 para organizaciones de la sociedad civil**

#### ***Lista de verificación: Organizaciones de la sociedad civil***

##### **Capacidad interna**

- Al menos 1 persona del equipo con formación básica en derechos digitales y sistemas de IA
- Protocolo de primera atención de casos de daño algorítmico elaborado
- Sistema de registro estandarizado de casos disponible
- Acuerdos de derivación con clínica jurídica o abogada especializada establecidos
- Política de confidencialidad y protección de datos de personas usuarias actualizada

##### **Alfabetización comunitaria**

- Talleres recurrentes de alfabetización algorítmica realizada con la comunidad
- Materiales en lenguaje accesible y en los idiomas de la comunidad disponibles

##### **Articulación**

- Conexión o acuerdo con la ventanilla única (Modulo 1) establecido
- Conocimiento de los procedimientos
- Participación en espacios de coordinación inter-organizacional
- Herramientas para documentar casos con patrón sistémico identificado y compartido con actores del ecosistema