fundaciónHermes
derechos de ciudadanía digital

10 Aniversario

Nuestros derechos también en el entorno digital

Ocho propuestas para la próxima legislatura

Fundación Hermes · Elecciones generales 2026

Ocho propuestas sobre derechos en el entorno digital

Fundación Hermes ante las elecciones generales del 29 de noviembre de 2026

Pedir una cita médica, solicitar una ayuda, buscar empleo o acompañar a niños y adolescentes en internet son situaciones cotidianas en las que la tecnología puede facilitarnos la vida. Para que ese avance beneficie a todas las personas, necesitamos poder utilizarla con confianza, comprender las decisiones que nos afectan y contar con ayuda cuando la necesitamos.

Cuando utilizamos la tecnología, somos más que usuarios de un servicio: somos ciudadanos y ciudadanas con derechos. En Fundación Hermes trabajamos para que la ciudadanía conserve y pueda ejercer, también en el entorno digital, los derechos que ya tiene reconocidos fuera de él.

Con motivo de las próximas elecciones generales, ofrecemos a todas las candidaturas ocho propuestas para la próxima legislatura, con medidas, plazos y compromisos cuyo cumplimiento pueda comprobarse. Las presentamos con voluntad de diálogo y abiertas a las aportaciones de las formaciones y a la adhesión de personas y entidades.

Un impulso inicial compartido. Invitamos al Gobierno que resulte de las urnas a impulsar durante los primeros cien días desde su toma de posesión las iniciativas pendientes, aprovechando el trabajo realizado y buscando el máximo consenso, con respeto a los plazos específicos de cada propuesta.

1. Comprender las decisiones y poder pedir una revisión humana

Cuando una Administración utiliza inteligencia artificial o sistemas automatizados en decisiones sobre ayudas, becas, sanciones u otros derechos o intereses legítimos, la persona afectada debe poder comprenderlas y solicitar su revisión.

Aprobar un marco de garantías durante el primer año. Reconocer el derecho a saber que se ha utilizado un sistema automatizado, recibir una explicación comprensible y solicitar una revisión humana efectiva, gratuita y con plazo de respuesta definido. La información debe ofrecerse en lenguaje claro y en la lengua oficial que la persona pueda elegir conforme a la normativa aplicable.

Registrar los sistemas y evaluar su impacto. Disponer de un registro público de los sistemas de la Administración General del Estado en ese mismo plazo, contado desde la toma de posesión del Gobierno. Exigir evaluaciones previas del impacto sobre los derechos fundamentales, proporcionadas al riesgo de cada sistema.

Permitir auditorías y corregir errores. Incluir en la contratación pública cláusulas que permitan auditar los sistemas, también cuando el proveedor invoque el secreto empresarial, con las debidas garantías de confidencialidad. Asegurar decisiones revisables y corregibles, responsables identificados y trazabilidad. El Gobierno informará anualmente a las Cortes sobre la aplicación de estas garantías.

2. Garantizar entornos digitales seguros para niños y adolescentes

La protección de los menores empieza en el diseño de los servicios. Las plataformas deben ofrecer garantías adecuadas a su edad y acreditar que evalúan y reducen los riesgos.

Retomar la protección legislativa de los menores. Recuperar el proyecto de ley orgánica de protección de menores en los entornos digitales, en coherencia con el Reglamento de Servicios Digitales y la propuesta europea EU KIDS Act. Las reglas de acceso por edades deberán ajustarse al marco europeo que finalmente se apruebe.

Establecer garantías desde el diseño. Exigir cuentas de menores privadas por defecto y sin publicidad basada en su comportamiento. Prohibir los mecanismos de diseño adictivo que les afecten, como el desplazamiento infinito, la reproducción automática sin pausas, las notificaciones nocturnas y los asistentes conversacionales que fomenten la dependencia emocional.

Acreditar el cumplimiento y proteger la capacidad de elección. Exigir a las plataformas que acrediten ante las autoridades competentes el cumplimiento de sus obligaciones y la evaluación y reducción de los riesgos del diseño adictivo. Proteger también a las personas adultas frente a diseños manipulativos que exploten sus vulnerabilidades o dificulten elegir libremente.

3. Comprobar la edad respetando la privacidad

Proteger a los menores y preservar la privacidad son objetivos que deben avanzar juntos. Comprobar la edad no debe exigir una identificación innecesaria ni permitir el seguimiento de la actividad digital.

Acreditar únicamente la edad necesaria. Exigir que cualquier sistema de verificación de edad, público o privado, acredite solo que se supera la edad exigida, sin revelar la identidad al proveedor del servicio ni exigir entregar datos biométricos a proveedores o terceros.

Evitar el seguimiento y ofrecer alternativas. Impedir el seguimiento entre servicios y la creación de historiales centralizados de uso. Ofrecer alternativas accesibles a quienes no dispongan de un dispositivo compatible o no quieran utilizar una aplicación.

Desplegar una identidad digital voluntaria y con garantías. Implantar la cartera europea de identidad digital, cuyo despliegue está previsto para finales de 2026, con carácter voluntario. Permitir compartir únicamente los atributos necesarios y someterla a auditorías independientes de seguridad y privacidad.

4. Ofrecer apoyo y respuestas rápidas frente a la violencia digital

Quien sufra la creación o difusión de imágenes íntimas sin consentimiento, reales o generadas con inteligencia artificial, necesita protección, acompañamiento y vías de respuesta urgentes.

Reforzar una protección penal proporcionada. Mejorar la respuesta penal frente a la creación y difusión no consentidas de deepfakes sexuales, es decir, imágenes o vídeos íntimos falsificados mediante tecnología, y frente a las suplantaciones gravemente lesivas, atendiendo a la gravedad de cada conducta.

Responder con urgencia y preservar las pruebas. Establecer procedimientos de notificación y retirada urgente, con una primera respuesta en un máximo de veinticuatro horas y medidas de preservación de pruebas. Coordinar la actuación con el canal prioritario de la Agencia Española de Protección de Datos cuando corresponda.

Acompañar a las víctimas y preservar las libertades. Garantizar asistencia gratuita y especializada, con especial atención a menores y mujeres. Transponer en plazo la Directiva europea sobre violencia contra las mujeres, incluidas sus disposiciones sobre violencia digital. Las medidas deben preservar la parodia, la crítica y la creación legítimas, respetando los derechos de terceros.

5. Garantizar servicios públicos accesibles y atención humana

Todas las personas debemos poder acceder a los servicios públicos, con independencia de nuestra edad, discapacidad, conocimientos digitales o dispositivos disponibles.

Reconocer por ley el derecho a la atención humana. Garantizar atención presencial o telefónica en todos los servicios públicos esenciales. Ofrecer atención presencial sin cita previa a las personas mayores de 65 años, a las personas con discapacidad que la necesiten y en situaciones de urgencia.

Eliminar barreras de acceso. Evitar que un trámite exija en la práctica disponer de un dispositivo o una aplicación concretos. Garantizar la accesibilidad de los servicios digitales públicos, también la cognitiva, con información que pueda comprenderse y utilizarse.

Conocer las dificultades para mejorar los servicios. Publicar anualmente indicadores de exclusión digital y abandono de trámites, desagregados por edad, territorio y discapacidad.

6. Proteger los derechos ante los algoritmos en el trabajo

Cuando un algoritmo interviene en la selección, evaluación, vigilancia o despido, las personas trabajadoras deben conocer los criterios que les afectan y poder solicitar revisión humana de las decisiones con efectos significativos.

Transponer prioritariamente la Directiva sobre trabajo en plataformas. Incorporar sus garantías a la legislación española, respetando el plazo europeo de transposición, que vence el 2 de diciembre de 2026.

Extender las garantías al conjunto de las personas trabajadoras. Asegurar información comprensible, supervisión humana y revisión de las decisiones automatizadas con efectos significativos, más allá del trabajo en plataformas. Contar con la representación legal de las personas trabajadoras en las evaluaciones de impacto de estos sistemas.

Proteger la intimidad en el ámbito laboral. Reforzar las garantías frente al tratamiento de datos sobre el estado emocional o psicológico y las conversaciones privadas, respetando las prohibiciones ya establecidas por la normativa europea.

7. Dotar a las instituciones de medios para proteger los derechos

Para ejercer un derecho necesitamos saber dónde acudir y contar con autoridades y organismos capaces de atender reclamaciones y cumplir eficazmente sus respectivas funciones.

Aprobar las medidas institucionales y de ciberseguridad en los primeros cien días. Aprobar, en ese plazo desde la toma de posesión del Gobierno, la legislación necesaria para que la Comisión Nacional de los Mercados y la Competencia ejerza plenamente como coordinador de servicios digitales. Completar en el mismo plazo la transposición de la Directiva de ciberseguridad NIS2.

Asegurar recursos y competencias claras. Dotar de medios suficientes a la Agencia Española de Supervisión de la Inteligencia Artificial, la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad, de acuerdo con sus respectivas funciones. Garantizar a las autoridades competentes autonomía de actuación y competencias claras.

Reforzar la respuesta y dar cuenta de los resultados. Mejorar la continuidad de las comunicaciones de emergencia ante apagones y fallos de red, con sistemas de respaldo y protocolos. Publicar cada año indicadores sobre reclamaciones, incidentes y tiempos de respuesta, respetando las exigencias de seguridad y confidencialidad.

8. Promover una campaña digital transparente

Una comunicación política transparente ayuda a la ciudadanía a formarse una opinión y participar con confianza. Invitamos a todas las candidaturas a asumir estos compromisos durante la campaña.

Hacer accesible la información sobre publicidad pagada. Publicar un registro de anuncios digitales pagados con el gasto, los intermediarios y los criterios utilizados para decidir a quién mostrarlos.

Identificar los contenidos generados o alterados con inteligencia artificial. Señalar de forma inequívoca los contenidos generados o sustancialmente alterados con estas tecnologías que puedan confundirse con hechos, imágenes o voces reales.

Asumir compromisos sobre contenidos y segmentación. No difundir deepfakes engañosos de personas candidatas ni utilizar datos personales sensibles, o inferencias que los revelen, para dirigir publicidad política. Declarar las colaboraciones remuneradas o con otras contraprestaciones con creadores de contenido.

Diálogo y participación

Diálogo con todas las candidaturas. Invitamos a las formaciones a compartir antes del 6 de noviembre de 2026 su valoración, los compromisos que podrían asumir y las aportaciones que consideren oportunas.

Seguimiento público de los compromisos. A los cien días desde la toma de posesión del Gobierno, y después anualmente, Fundación Hermes ofrecerá un seguimiento de los compromisos asumidos, basado en datos públicos y una metodología común.

Participación y adhesiones. Estas propuestas nacen de una carta abierta a la ciudadanía y mantienen su invitación a participar. Pueden adherirse personas a título individual, organizaciones de la sociedad civil, entidades académicas y asociaciones profesionales que compartan su contenido. Las adhesiones pueden comunicarse en **fundacion@fundacionhermes.org**

fundaciónHermes

derechos de
ciudadanía
digital