

MANIFESTACIÓN DE INTERÉS DE LA ENTIDAD DE ACOGIDA

RETO DE ASESORAMIENTO CIENTÍFICO

Un **reto de asesoramiento científico** es una necesidad concreta de información, análisis o evidencia científica identificada por una administración pública para mejorar el diseño, implementación o evaluación de sus políticas, programas o servicios.

1. Nombre del departamento, órgano, organismo o entidad de derecho público de la Administración General del Estado

Ministerio para la Transformación Digital y de la Función Pública. Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA). Gabinete de la Secretaría de Estado.

2. Título abreviado del reto de asesoramiento científico para la web (Máximo 15 palabras)

Protección del contenido audiovisual en directo frente a piratería digital

3. Acrónimo del reto de asesoramiento científico

PROTEGE-LIVE

4. Título completo del reto de asesoramiento científico

Revisión de literatura regulatoria y técnica para una protección proporcionada de la propiedad intelectual de contenidos audiovisuales en directo en España y la Unión Europea

5. Descripción del reto de asesoramiento científico

5.1. Descripción de la política pública en la que se enmarca el reto de asesoramiento científico [Máximo 300 palabras]

El reto se enmarca en la política pública de impulso a la digitalización de la sociedad y la economía de forma respetuosa con los derechos individuales y colectivos, así como en la regulación de los servicios digitales, la economía digital, la comunicación audiovisual y la protección de la propiedad intelectual en internet. La piratería de retransmisiones en directo, especialmente deportivas y culturales, tensiona los instrumentos clásicos de tutela de derechos: la infracción se produce en ventanas temporales muy breves, se apoya en CDN, DNS, VPN, redes sociales, mensajería y *hosting* efímero, y puede desplazarse durante el propio evento. Las respuestas actuales (bloqueo dinámico de dominios o IP, retirada de contenidos, medidas contractuales y cooperación con intermediarios) deben ser efectivas, rápidas y trazables, pero también proporcionadas, reversibles y respetuosas con la neutralidad de red, la libertad de empresa, el acceso a información lícita, la protección de datos y la seguridad jurídica de terceros no infractores. La estancia apoyará al Gabinete de la Secretaría de Estado en la elaboración de criterio técnico-regulatorio nacional y europeo sobre protección de contenidos live, aplicación del Reglamento de Servicios Digitales, Recomendación (UE) 2023/1018, LSSI, propiedad intelectual y gobernanza de intermediarios digitales.

5.2. Justificación y objetivos del reto de asesoramiento científico [Máximo 300 palabras]

La necesidad surge de una brecha entre la velocidad de la piratería en directo y la capacidad de respuesta de los mecanismos jurídicos y técnicos disponibles. El objetivo general es producir evidencia útil para diseñar una respuesta pública que proteja el valor de los derechos audiovisuales sin generar sobrecargas, inseguridad jurídica ni incentivos técnicos contraproducentes. Objetivos específicos:

1. mapear el marco jurídico español y europeo aplicable a contenidos audiovisuales en directo, intermediarios y medidas cautelares dinámicas;
2. describir las arquitecturas técnicas usadas para piratear y para proteger el contenido en vivo;
3. evaluar proporcionalidad, eficacia, trazabilidad, reversibilidad y garantías de los bloqueos dinámicos por DNS, URL, dominio, IP, CDN, VPN o plataforma;
4. identificar buenas prácticas europeas y modelos de cooperación público-privada;
5. proponer un modelo de actuación con salvaguardas *ex ante* y *ex post*, métricas de daño y procedimientos de desbloqueo urgente;
6. formular opciones normativas, técnicas y organizativas para la Secretaría de Estado.

5.3. Resultados esperados [Máximo 300 palabras]

5.3.1. Entregables previstos orientados al apoyo a la política pública

Entregables previstos:

1. informe de diagnóstico jurídico-técnico del ecosistema de piratería de contenidos audiovisuales en directo; mapa comparado de soluciones europeas y nacionales.
2. matriz de riesgos y garantías para bloqueos dinámicos y otras medidas de *enforcement*.
3. propuesta de protocolo público de actuación proporcionada, con criterios de necesidad, precisión, trazabilidad, reversibilidad, auditoría y notificación a terceros afectados.
4. catálogo de soluciones técnicas recomendables (marcas de agua forenses, *fingerprinting*, monitorización en tiempo real, *notice-and-action*, API de evidencias, listas blancas, mecanismos de apelación y desbloqueo urgente).
5. cuadro de indicadores para medir eficacia, daño evitado, falsos positivos, tiempos de reacción y costes para intermediarios, titulares y usuarios legítimos.

5.3.2. Actividades previstas para presentar los resultados

Actividades previstas: reunión de arranque con el Gabinete y unidades competentes; entrevistas estructuradas con titulares de derechos, operadores, plataformas, CDN, expertos en ciberseguridad, entidades de consumidores y autoridades sectoriales; revisión de expedientes y documentación pública disponible; taller técnico-jurídico sobre bloqueo dinámico, CDN, DNS, VPN, ECH, *watermarking* y trazabilidad probatoria; sesiones quincenales de avance con la unidad de acogida; presentación intermedia de hallazgos y validación de escenarios; seminario interno en el Ministerio con conclusiones y opciones de política pública; entrega final de informe, resumen ejecutivo y presentación para decisores; y, si procede, preparación de una nota breve para coordinación interministerial o contribución a debates europeos.

5.3.3. Derechos de propiedad intelectual sobre los resultados generados

[marcar con una X la opción elegida]

- La entidad beneficiaria (universidad, centro de investigación, etc.) ostentará los derechos de propiedad intelectual sobre los resultados. [Opción que aparece en la convocatoria por defecto].
- La entidad de acogida (organismo público) solicita a la entidad beneficiaria la cesión de los derechos de propiedad intelectual sobre los resultados.
- Otra fórmula: la entidad beneficiaria conservará la titularidad de los resultados y concederá a la entidad de acogida una licencia no exclusiva, gratuita, indefinida y transferible dentro del sector público estatal para reproducir, adaptar, comunicar y reutilizar los entregables en el diseño,

ejecución, evaluación y coordinación de políticas públicas, citando la autoría cuando proceda y preservando la confidencialidad de la información no pública.

6. Perfil requerido de investigador/a

[Máximo 300 palabras]

6.1. Requisitos de formación [Indicar al menos el área/s de conocimiento del doctorado]

Esenciales: Doctorado en Derecho, Ingeniería Informática, Ingeniería de Telecomunicación, Ciencia de Datos, Comunicación Audiovisual, Economía Digital, Ciencias Políticas o áreas afines.

Complementarios: Se valorará especialmente formación mixta jurídico-técnica en propiedad intelectual, derecho digital, servicios de la sociedad de la información, regulación europea de plataformas, ciberseguridad, redes, distribución audiovisual OTT/IPTV, inteligencia artificial aplicada a detección de infracciones o gobernanza de datos. Imprescindible capacidad para comprender documentación normativa y técnica en español e inglés.

6.2. Requisitos de experiencia

Experiencia investigadora o profesional en al menos dos de los siguientes ámbitos: propiedad intelectual y derechos audiovisuales; aplicación del Reglamento de Servicios Digitales, LSSI, Directiva de Copyright, normativa audiovisual o medidas cautelares; análisis de piratería *online*, *streaming* no autorizado, IPTV, *cardsharing*, redes sociales o mensajería; funcionamiento de CDN, DNS, VPN, hosting, ECH, geobloqueo, *fingerprinting*, *watermarking* o monitorización de tráfico; elaboración de informes de política pública; análisis comparado europeo; interlocución con administraciones, reguladores, titulares de derechos, plataformas u operadores de telecomunicaciones. Se valorará experiencia en proyectos de evidencia para toma de decisiones públicas.

6.3. Requisitos de competencias

Competencias requeridas: pensamiento crítico e independencia analítica; capacidad para traducir problemas técnicos complejos a propuestas regulatorias accionables; conocimiento de principios de proporcionalidad, debido proceso, derechos fundamentales y protección de datos; manejo de evidencia empírica y diseño de indicadores; redacción clara de informes ejecutivos y jurídicos; solvencia para trabajar con información sensible o confidencial; capacidad de mediación entre actores con intereses contrapuestos; gestión de plazos cortos vinculados a eventos en directo; comunicación oral para presentaciones a altos cargos; y orientación a resultados aplicables, no meramente académicos.

CONDICIONES PARA LA RESOLUCIÓN DEL RETO

7. Unidad de acogida

7.1. Unidad de acogida

Gabinete de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

7.2. Sede y lugar de la unidad de acogida

Calle del Mármol, 2, 28005 Madrid. Ministerio para la Transformación Digital y de la Función Pública.

8. Incorporación

8.1. Plazo de incorporación. [Marcar con una X la opción deseada]

- Fecha a elección de la persona participante (dentro del plazo de 5 meses desde la resolución definitiva).
- En un plazo de 1 mes desde la resolución definitiva.
- Incorporación inmediata (dentro de los 10 días hábiles siguientes a la resolución definitiva).

8.2. Medidas formativas para la incorporación sobre las funciones y organización de la unidad de acogida

Durante la primera semana se facilitará una sesión de acogida sobre funciones, estructura y circuitos de trabajo del Gabinete; objetivos de la estancia; normas de confidencialidad y protección de datos; canales de coordinación con unidades del Ministerio; y acceso a documentación, normativa, expedientes públicos y fuentes técnicas. En las dos primeras semanas se programarán reuniones de contexto con las unidades competentes en regulación digital, audiovisual, datos y ciberseguridad, además de una introducción al procedimiento interno para elaborar notas, informes y posiciones institucionales. Se habilitará una persona de referencia para resolver dudas operativas y validar prioridades.

9. Régimen de presencialidad y horario

- 9.1. El participante desarrollará un mínimo del 60% de su estancia de forma presencial.
- 9.2. Horario: 9:00-17:30 de lunes a jueves y 9:00-14:30 los viernes, con flexibilidad para reuniones, sesiones técnicas y seguimiento de eventos en directo.

10. Uso de datos

La unidad de acogida se compromete a facilitar al/la participante el acceso a los datos disponibles en el Ministerio que sean pertinentes para el desarrollo del proyecto de asesoramiento científico, en cumplimiento con la normativa vigente sobre protección de datos y confidencialidad. El organismo público podrá establecer las condiciones específicas de acceso, uso y tratamiento de dichos datos, garantizando que su utilización se ajuste a los fines del proyecto y a los principios de legalidad, ética y seguridad.