# Informe de conclusiones y líneas de investigación sobre los aspectos jurídicos de la ciberseguridad

Jornadas sobre Aspectos Jurídicos de la Ciberseguridad

Sesión del 6 de febrero de 2026

Facultad de Derecho ─ Universidad de Oviedo.

Dra. Luisa Fernanda Rodríguez Hevia

Vicedecana de Business & Tech
Universidad Alfonso X el Sabio (UAX)



Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
Plan de Recuperación, Transformación y Resiliencia
incibe_ Instituto Nacional de Ciberseguridad

# Índice





Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 1. Resumen Ejecutivo

El presente informe tiene por objeto sistematizar y desarrollar las principales conclusiones derivadas de las Jornadas sobre Aspectos Jurídicos de la Ciberseguridad, celebradas los días 5 y 6 de febrero de 2026 en la Universidad de Oviedo, en el marco de la Actividad 12 del proyecto de investigación PECIEE, orientada a la potenciación de la investigación en el ámbito jurídico de la ciberseguridad.

El encuentro reunió a especialistas del ámbito jurídico, académico y tecnológico procedentes de distintas universidades, configurándose como un espacio de reflexión interdisciplinar en el que se identificaron los principales retos jurídicos del entorno digital, así como las lagunas en la aplicación de los marcos normativos vigentes.

Como premisa transversal, el análisis parte de la consideración de que los principales desafíos de la ciberseguridad jurídica no derivan de la insuficiencia normativa, sino de las dificultades en la detección del ilícito y en la atribución de responsabilidad en entornos digitales complejos.

El informe se articula en torno a cinco líneas de investigación: (i) cibercriminalidad y Derecho penal, (ii) robótica social e inteligencia artificial física, (iii) protección de datos y seguridad, (iv) legal design y arquitectura contractual y (v) dimensión jurídico-pública de las redes sociales.

En conjunto, el informe concluye que el reto principal de la ciberseguridad jurídica no es normativo, sino de aplicación efectiva, coordinación institucional y adaptación a la complejidad tecnológica.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 2. Introducción

La aceleración de la transformación digital ha modificado profundamente las bases sobre las que se articulan las relaciones sociales, económicas e institucionales, generando nuevos escenarios de riesgo que tensionan los marcos jurídicos tradicionales. La digitalización de procesos, la automatización mediante inteligencia artificial y la circulación masiva de datos han incrementado tanto las oportunidades como las vulnerabilidades del entorno digital.

En este contexto, la ciberseguridad deja de ser una cuestión exclusivamente técnica para convertirse en un eje central en la protección de los derechos fundamentales, la estabilidad de los mercados y la confianza en las instituciones.

Las jornadas celebradas en la Universidad de Oviedo constituyen el punto de partida del presente informe. Su objetivo es transformar las aportaciones realizadas en un marco analítico estructurado que permita evaluar la adecuación del ordenamiento jurídico vigente y definir líneas de investigación futuras.

El carácter interuniversitario del proyecto refuerza el valor de las conclusiones alcanzadas, al integrar perspectivas diversas y enfoques complementarios en el análisis de la ciberseguridad jurídica.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 3. Marco Conceptual y Normativo

La ciberseguridad jurídica puede definirse como el conjunto de mecanismos normativos, organizativos y de gobernanza orientados a prevenir, detectar y responder a amenazas digitales, garantizando al mismo tiempo la protección de los derechos fundamentales.

En el ámbito europeo, este marco se articula en torno al Reglamento General de Protección de Datos (RGPD), la Directiva NIS2 y el Reglamento de Inteligencia Artificial, junto con su desarrollo en el ordenamiento jurídico español.

Este entramado normativo configura un entorno complejo en el que confluyen distintas ramas del Derecho —penal, administrativo, civil y constitucional—, generando en ocasiones solapamientos, tensiones interpretativas y dificultades de aplicación práctica.

En este sentido, uno de los principales retos consiste en avanzar hacia modelos integrados de interpretación y aplicación normativa que permitan mejorar la eficacia de las medidas de ciberseguridad.

# 4. Metodología

El informe adopta una metodología cualitativa de carácter exploratorio basada en:

- El análisis de las intervenciones realizadas durante las jornadas
- La clasificación temática de los problemas jurídicos identificados
- La contrastación con el marco normativo europeo y nacional

El enfoque es interdisciplinar, integrando análisis jurídico con condicionantes tecnológicos y organizativos.

Como criterio metodológico adicional, las Jornadas contaron con la participación de profesorado universitario e investigadores con trayectoria acreditada en las respectivas líneas abordadas, pertenecientes a distintas universidades y equipos de investigación. Las aportaciones realizadas se apoyan en líneas de trabajo previamente desarrolladas en el ámbito del Derecho penal, la protección de datos, la inteligencia artificial, la ciberseguridad y el Derecho constitucional digital, lo que garantizó la coherencia académica y la solidez de los contenidos tratados, en línea con los objetivos establecidos.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

# 5. Premisa Jurídica

La premisa central del informe es que el principal desafío de la ciberseguridad jurídica no reside en la insuficiencia normativa, sino en las dificultades de detección del ilícito y atribución de responsabilidad.

Aunque el Derecho penal vigente es materialmente adecuado, su aplicación se ve limitada por:

- la anonimización de las comunicaciones
- la transnacionalidad de las infraestructuras
- la volatilidad de la prueba digital

En consecuencia, los retos se sitúan principalmente en el plano operativo, probatorio y de cooperación internacional

# 6. Desarrollo Analítico de las Líneas de Investigación

A partir del marco conceptual y de la premisa jurídica central expuestos, el presente apartado desarrolla de forma sistemática las principales líneas de investigación identificadas durante las jornadas. Cada subepígrafe combina una breve presentación del contexto de la línea con la descripción de los problemas jurídicos detectados, un análisis de las tensiones normativas y prácticas que se derivan de ellos y, finalmente, la formulación de propuestas y prioridades de investigación futura.

## 6.1. Derecho penal, cibercriminalidad y nuevas tecnologías

Las jornadas dedicaron una parte central al análisis del tratamiento penal de la cibercriminalidad, coordinado por el profesor Javier Fernández Teruelo y su equipo de investigación de la Universidad de Oviedo. Esta línea aborda cómo los delitos tradicionales se proyectan sobre un entorno digital caracterizado por la deslocalización de las conductas, la intermediación tecnológica y la creciente sofisticación de los modus operandi de los ciberdelincuentes.

Entre los problemas jurídicos más relevantes identificados destacan, en primer lugar, los fraudes en sistemas de banca online y otros servicios financieros digitales, donde las estafas informáticas complejas generan importantes dificultades de calificación y de delimitación de responsabilidades entre entidades, proveedores de servicios y usuarios. En segundo lugar, la criminalidad organizada y el blanqueo de capitales en contextos transnacionales plantean retos específicos en términos de trazabilidad de las operaciones, obtención de evidencia digital y coordinación entre autoridades de distintos Estados. Asimismo, se subrayó el impacto de la ingeniería social y de las redes de “muleros” en la



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

canalización de fondos ilícitos, así como la especial gravedad de los delitos contra la indemnidad sexual de menores en entornos online, que exigen obligaciones proactivas reforzadas para los proveedores de servicios de internet.

Desde una perspectiva analítica, esta línea confirma la premisa general de suficiencia material del Derecho penal, pero pone de manifiesto que la evolución tecnológica altera profundamente las condiciones de imputación y prueba. La anonimización de usuarios, el uso de infraestructuras distribuidas, la rápida desaparición o modificación de rastros digitales y la intervención de múltiples intermediarios privados complican la atribución individualizada de responsabilidad y la aplicación de los estándares probatorios clásicos. Además, la coexistencia de marcos regulatorios sectoriales (por ejemplo, en servicios de pago o prevención de blanqueo) con el Derecho penal sustantivo y procesal obliga a articular mejor las relaciones entre compliance, supervisión administrativa y persecución penal.

Como líneas de investigación prioritarias, se propone, en primer lugar, el desarrollo de estudios dogmáticos y empíricos sobre la calificación penal de las distintas tipologías de fraude online, incluyendo el papel de las medidas de ciberseguridad exigibles a las entidades financieras y plataformas de pago. En segundo lugar, se plantea profundizar en los mecanismos de obtención, conservación y cadena de custodia de la prueba digital en contextos transnacionales, así como en las herramientas de cooperación judicial y policial internacional más adecuadas para estos supuestos. Finalmente, se considera necesario avanzar en la delimitación de la responsabilidad de intermediarios y proveedores de servicios digitales, especialmente en materia de prevención de delitos contra la indemnidad sexual de menores y de colaboración en la persecución de redes de blanqueo de capitales.

## 6.2. Robótica social e inteligencia artificial física

Una segunda línea de trabajo de las jornadas se centró en la robótica social y la inteligencia artificial integrada en dispositivos físicos, impulsada por el equipo de investigación de la Universidad de las Islas Baleares liderado por María Isabel Montserrat y Thomas Woiczyk. El foco se situó en aquellos entornos especialmente sensibles —como la asistencia a personas mayores, la atención a pacientes oncológicos pediátricos o la interacción cotidiana en el ámbito doméstico— en los que los sistemas de IA física asumen funciones de cuidado, apoyo o toma de decisiones con impacto directo sobre la integridad física y moral de las personas usuarias.

Los problemas jurídicos identificados giran en torno a la atribución de responsabilidad por daños derivados del funcionamiento anómalo, defectuoso o inseguro de estos sistemas. La progresiva autonomía de los robots sociales y la complejidad de sus algoritmos plantean dudas sobre la aplicación de los esquemas clásicos de responsabilidad civil y penal, basados en la acción humana directa, en la previsibilidad del daño y en la existencia de un nexo causal claramente identificable. Además, se



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

subrayó el riesgo añadido asociado a eventuales ciberataques (hijacking de dispositivos) que alteren la programación o el comportamiento del robot, convirtiéndolo en un vector de daño intencionado frente al que las personas afectadas tienen una capacidad de control muy limitada.

Desde una perspectiva analítica, esta línea pone de relieve la necesidad de repensar las categorías tradicionales de imputación en contextos donde confluyen fabricantes de hardware, desarrolladores de software, proveedores de servicios en la nube, entidades que despliegan los dispositivos y usuarios finales. La cadena de valor tecnológica se traduce en una cadena de potenciales responsables jurídicos, en la que no siempre resulta evidente qué estándar de diligencia corresponde a cada actor, ni cómo deben articularse las obligaciones de diseño seguro, actualización, supervisión humana y ciberseguridad. Además, la irrupción del futuro Reglamento europeo de Inteligencia Artificial introduce nuevas exigencias de evaluación de riesgos, transparencia y gobernanza que deberán coordinarse con los regímenes existentes de responsabilidad por productos defectuosos y por prestación de servicios.

En este contexto, se proponen varias líneas de investigación prioritarias. En primer lugar, avanzar en modelos de distribución de responsabilidad que, sin crear ficciones de subjetividad para los sistemas de IA, permitan asignar de forma clara obligaciones y consecuencias jurídicas a cada eslabón de la cadena técnico-organizativa, especialmente en sectores de alto riesgo. En segundo lugar, profundizar en el diseño de marcos de ciberseguridad específicos para la robótica social, que integren requisitos de seguridad desde el diseño, mecanismos de actualización segura y protocolos de respuesta ante incidentes de secuestro o manipulación remota de dispositivos. Finalmente, se considera necesario promover estudios interdisciplinarios que combinen la perspectiva jurídica con la ingeniería, la ética y la sociología, a fin de capturar adecuadamente el impacto de estos sistemas en la autonomía personal, la confianza de los usuarios y la delimitación de los derechos fundamentales afectados.

## 6.3. Protección de datos y controles de seguridad

La tercera línea de investigación, presentada por Raquel Sánchez, se centró en la interacción entre la normativa de protección de datos personales y los marcos de ciberseguridad y seguridad institucional, con especial referencia al RGPD, la LOPDGDD y el Esquema Nacional de Seguridad (ENS). El objetivo fue analizar cómo las obligaciones derivadas de la privacidad y las derivadas de la seguridad de la información se cruzan en la práctica, generando en ocasiones fricciones, solapamientos o aparentes contradicciones.

El problema jurídico de partida reside en la tensión estructural entre el principio de minimización de datos y de limitación de la finalidad, por un lado, y la necesidad de desplegar medidas de monitorización, registro de eventos y análisis de comportamiento para garantizar la ciberseguridad, por otro. La implantación de controles de acceso,



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

sistemas de detección de intrusiones, soluciones de monitorización continua o servicios gestionados de seguridad implica, en muchos casos, tratamientos intensivos de datos personales que deben mantenerse dentro de los márgenes permitidos por el RGPD. A ello se añade la coexistencia de evaluaciones de impacto en protección de datos, análisis de riesgos de seguridad de la información y auditorías ENS, que pueden generar cargas duplicadas y dificultades de coordinación dentro de las organizaciones.

Desde un punto de vista analítico, esta línea muestra que la clave no está en optar entre privacidad o seguridad, sino en construir marcos integrados de gestión del riesgo que alineen ambos conjuntos de obligaciones. Ello exige articular metodologías que permitan, por ejemplo, que una única matriz de riesgos alimente tanto la evaluación de impacto en protección de datos como el análisis de riesgos exigido por el ENS y la Directiva NIS2, evitando incoherencias y redundancias. Asimismo, se hace necesario clarificar la base jurídica y los límites de determinados tratamientos realizados con fines de seguridad, así como los criterios de proporcionalidad y necesidad aplicables a técnicas avanzadas de monitorización y correlación de eventos.

Como líneas de investigación prioritarias se plantean, en primer lugar, el diseño de modelos de evaluación integrada de riesgos que unifiquen, en la medida de lo posible, las exigencias del RGPD, el ENS y NIS2, especialmente en organizaciones públicas y operadores esenciales. En segundo lugar, el desarrollo de catálogos de medidas de seguridad "jurídicamente robustas" que, además de reforzar la protección técnica de los sistemas, incorporen desde el inicio garantías específicas para los derechos de las personas afectadas (información, ejercicio de derechos, minimización y conservación limitada de registros). Finalmente, se propone estudiar con mayor detalle los modelos de gobernanza interna —comités de seguridad, delegados de protección de datos, responsables de sistemas de información— que resultan más eficaces para asegurar una coordinación real entre privacidad y ciberseguridad en la práctica organizativa diaria.

## 6.4. Arquitectura contractual y legal design en productos digitales

La cuarta línea de investigación, presentada por Patricia Aira, se centró en la arquitectura contractual de los productos y servicios digitales y en el potencial del legal design como herramienta preventiva en materia de ciberseguridad. El punto de partida es la constatación de que los términos y condiciones, políticas de privacidad y demás instrumentos contractuales que acompañan al software y a los servicios en línea suelen tratarse como un trámite formal al final del desarrollo, pese a constituir el núcleo de la relación jurídica entre proveedor y usuario.

Entre los principales problemas detectados destaca la desconexión entre el diseño técnico del producto y su diseño jurídico. La arquitectura de permisos, flujos de datos, mecanismos de autenticación o modelos de negocio (freemium, publicidad segmentada, tratamiento masivo de datos) se define a menudo sin integrar de forma temprana las implicaciones legales, lo que conduce a contratos opacos, poco comprensibles y, en



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ocasiones, difícilmente compatibles con los requerimientos de protección de datos, ciberseguridad o defensa de consumidores. Esta falta de alineación puede generar vulnerabilidades jurídicas que se traducen en riesgos reputacionales, sanciones regulatorias y menor eficacia de las propias medidas de seguridad.

Desde una perspectiva analítica, la línea subraya que el legal design no se limita a hacer más "amigables" los textos legales, sino que supone incorporar criterios jurídicos y de protección de derechos desde la fase cero del diseño del producto. Esto implica repensar los contratos como parte de la arquitectura del servicio, de modo que las decisiones sobre qué datos se recogen, cómo se tratan, qué obligaciones de seguridad asume cada parte o qué mecanismos de notificación de incidentes se prevén queden reflejadas de manera clara, coherente y operativa. En el ámbito de tecnologías emergentes, como los contratos inteligentes en entornos blockchain, este enfoque resulta especialmente relevante para evitar que el automatismo técnico consolide errores de diseño jurídico difíciles de corregir ex post.

Entre las líneas de investigación prioritarias, se propone, en primer lugar, el desarrollo de estudios empíricos sobre modelos de términos y condiciones que resulten simultáneamente comprensibles para los usuarios y adecuados desde el punto de vista de la ciberseguridad y la protección de datos. En segundo lugar, la elaboración de guías de buenas prácticas de legal design aplicadas a diferentes tipos de servicios digitales (plataformas, apps, servicios en la nube, dispositivos conectados), que integren requisitos normativos y de usabilidad. Finalmente, se plantea explorar la extensión de estas metodologías al ecosistema contractual de tecnologías emergentes, con especial atención a los smart contracts y a los sistemas automatizados de ejecución, donde la coordinación entre código y norma jurídica resulta particularmente crítica.

## 6.5. Dimensión jurídico-pública de las redes sociales

La quinta línea de investigación, dirigida por Leonardo Álvarez, se centró en la dimensión jurídico-pública de las redes sociales como infraestructuras de debate y formación de opinión en las sociedades democráticas. Las plataformas dejan de ser meros espacios privados de interacción para adquirir una relevancia constitucional creciente, en la medida en que condicionan el ejercicio efectivo de derechos fundamentales como la libertad de expresión, de información y de participación política.

El problema jurídico principal identificado radica en la tensión entre el carácter privado de las plataformas y las funciones cuasi públicas que desempeñan. Las políticas de moderación de contenidos, el diseño algorítmico de la visibilidad de mensajes y la gestión de cuentas y perfiles pueden generar fenómenos de censura, discriminación o desinformación que producen un efecto desaliento (chilling effect) sobre el ejercicio de la libertad de expresión. Al mismo tiempo, la ausencia de estándares claros de transparencia y rendición de cuentas dificulta el control democrático sobre decisiones que impactan directamente en el espacio público digital.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Desde una perspectiva analítica, esta línea pone de relieve la necesidad de replantear los marcos regulatorios aplicables a las plataformas, combinando la autorregulación con obligaciones legales más exigentes en materia de transparencia, neutralidad y garantías procedimentales. Se abre aquí el debate sobre hasta qué punto deben imponerse deberes análogos a los de los poderes públicos —por ejemplo, en términos de respeto a estándares constitucionales, motivación de decisiones o mecanismos de recurso— a entidades privadas que ejercen un control estructural sobre el discurso público. Asimismo, la ciberseguridad se proyecta sobre la integridad de los procesos de comunicación, incluyendo la protección frente a campañas coordinadas de desinformación, manipulación automatizada de contenidos o ataques dirigidos a colectivos vulnerables.

Entre las líneas de investigación prioritarias se propone, en primer lugar, profundizar en la delimitación de los límites y posibilidades de la autorregulación de las grandes plataformas tecnológicas a la luz de los principios constitucionales y del emergente Derecho europeo de servicios digitales. En segundo lugar, avanzar en el diseño de obligaciones de transparencia algorítmica y de sistemas de supervisión independientes que permitan evaluar el impacto de las decisiones de moderación y recomendación de contenidos sobre los derechos fundamentales. Finalmente, se considera necesario estudiar la articulación entre las políticas de ciberseguridad de las plataformas y la protección efectiva de la ciudadanía frente a campañas de desinformación, injerencias externas y dinámicas de acoso u odio en línea, con especial atención a los grupos en situación de vulnerabilidad.

## 7. Conclusiones

El análisis desarrollado a partir de las jornadas permite confirmar que el reto principal de la ciberseguridad jurídica no reside tanto en la ausencia de normas como en la eficacia de su aplicación práctica. En materia penal, de protección de datos, seguridad de la información, responsabilidad civil y garantías constitucionales existe ya un entramado normativo considerable, pero su articulación y ejecución presentan todavía importantes déficits.

En primer lugar, se constata que el Derecho penal resulta, en términos generales, materialmente suficiente para tipificar las principales conductas asociadas a la cibercriminalidad, pero encuentra dificultades notables en la obtención y valoración de la prueba digital, la atribución de autoría en entornos anonimizados y la cooperación judicial y policial internacional. Estas limitaciones procesales y organizativas reducen la capacidad disuasoria y protectora del sistema, incluso cuando el marco tipificador es adecuado.

En segundo lugar, la irrupción de la inteligencia artificial y de la robótica social en entornos sensibles pone de manifiesto la necesidad de adaptar los modelos clásicos de imputación, distribución de responsabilidades y gestión del riesgo. La complejidad de la



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

cadena técnico-organizativa en la que intervienen fabricantes, desarrolladores, proveedores de servicios y usuarios exige enfoques más finos que permitan atribuir obligaciones claras a cada actor sin generar vacíos ni solapamientos.

En tercer lugar, la interacción entre el RGPD, la LOPDGDD, el ENS, la Directiva NIS2 y el emergente Reglamento de IA evidencia la importancia de avanzar hacia marcos integrados de gestión del riesgo que concilien privacidad y seguridad. La falta de articulación entre evaluaciones de impacto, análisis de riesgos y auditorías puede derivar en cargas duplicadas, incoherencias y, en última instancia, en una menor eficacia de las medidas de ciberseguridad adoptadas.

Finalmente, el estudio pone de relieve que el diseño jurídico temprano de los productos digitales y el reconocimiento de las redes sociales como espacios de relevancia pública son piezas clave para la consolidación de un ecosistema digital seguro y respetuoso con los derechos fundamentales. Integrar el legal design en el ciclo de desarrollo y reforzar las obligaciones de transparencia y rendición de cuentas de las plataformas se revela, así, como una condición necesaria para garantizar la confianza ciudadana en el entorno digital.

## 8. Limitaciones del Estudio

El presente informe se basa en una metodología cualitativa derivada de un único evento académico, las Jornadas sobre Aspectos Jurídicos de la Ciberseguridad celebradas en febrero de 2026, lo que condiciona de manera directa el alcance de sus conclusiones. Las líneas de análisis recogidas reflejan las prioridades y sensibilidades de los ponentes y participantes, sin constituir necesariamente una muestra exhaustiva de todos los enfoques posibles sobre la materia.

Asimismo, el estudio se centra fundamentalmente en el marco jurídico europeo y español, con especial atención al RGPD, la Directiva NIS2, el ENS y el emergente Reglamento de IA, por lo que sus resultados no son directamente extrapolables a otros contextos regulatorios. La ausencia de un enfoque comparado sistemático limita la capacidad del informe para valorar soluciones alternativas desarrolladas en otros ordenamientos.

Por otra parte, la naturaleza cualitativa y exploratoria del análisis implica que no se han incorporado datos empíricos extensivos sobre incidencia real de ciberataques, sanciones, resoluciones judiciales o prácticas organizativas en materia de ciberseguridad. En consecuencia, las conclusiones deben entenderse como un marco de reflexión y una agenda de preguntas más que como respuestas definitivas basadas en evidencia cuantitativa.

Finalmente, la rapidez con la que evoluciona tanto la tecnología como el marco normativo en este ámbito hace que algunas de las referencias regulatorias puedan quedar parcialmente desactualizadas en el corto plazo. Esta circunstancia refuerza la necesidad



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

de concebir el informe como un punto de partida dinámico, susceptible de ser revisado y actualizado a medida que se produzcan nuevos desarrollos legislativos y jurisprudenciales.

## 9. Líneas Futuras de Investigación

A partir de las reflexiones recogidas, se identifican diversas líneas futuras de investigación que pueden orientar trabajos académicos y proyectos aplicados en los próximos años. Estas propuestas se alinean con las cinco áreas temáticas estructurantes del informe y buscan profundizar en los principales retos detectados.

En el ámbito del Derecho penal y la cibercriminalidad, resulta prioritario desarrollar estudios sistemáticos sobre la prueba digital y la atribución de responsabilidad en entornos transnacionales, incluyendo el análisis del papel de los proveedores de servicios y de los mecanismos de cooperación internacional. Asimismo, se propone examinar empíricamente la eficacia de las medidas de ciberseguridad y de los programas de compliance en la prevención de fraudes online, blanqueo de capitales y delitos contra la indemnidad sexual de menores en línea.

En relación con la robótica social y la inteligencia artificial física, se plantea avanzar en modelos de distribución de responsabilidad adaptados a sistemas de alta autonomía, integrando los requerimientos del futuro Reglamento de IA con los regímenes de responsabilidad por productos y servicios. También se considera necesario estudiar marcos específicos de ciberseguridad para estos dispositivos, que incorporen protocolos de actualización segura, respuesta ante incidentes y supervisión humana efectiva en entornos de alto riesgo.

En el campo de la protección de datos y los controles de seguridad, se propone investigar metodologías unificadas de evaluación de riesgos que permitan armonizar las exigencias del RGPD, el ENS y NIS2, especialmente en organizaciones públicas y operadores de servicios esenciales. Igualmente, se identifican como prioritarios los estudios sobre gobernanza interna de la ciberseguridad y la privacidad, analizando el papel de delegados de protección de datos, responsables de seguridad y órganos colegiados en la toma de decisiones.

En cuanto a la arquitectura contractual y el legal design, se abren líneas de trabajo orientadas al diseño y evaluación de modelos de términos y condiciones que integren, desde la fase de concepción del producto, obligaciones claras en materia de ciberseguridad, gestión de incidentes y reparto de responsabilidades entre las partes. De forma complementaria, se propone explorar la adaptación de estas metodologías al ámbito de los smart contracts y de las infraestructuras blockchain, donde la automatización contractual plantea desafíos específicos de control y corrección.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Finalmente, en la dimensión jurídico-pública de las redes sociales, se identifican como prioritarias las investigaciones sobre el equilibrio entre autorregulación y regulación pública, la transparencia algorítmica y los mecanismos de supervisión independientes de las decisiones de moderación de contenidos. También se considera esencial analizar el vínculo entre políticas de ciberseguridad de las plataformas, protección frente a campañas de desinformación y garantía efectiva de los derechos fundamentales en el espacio público digital, con especial atención a colectivos vulnerables.



Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD