



ACCIÓN ESPECÍFICA DE LA UNIÓN 2024 FSI

ISF/2024/SA/3.4.1 – AILE – Innovación: Inteligencia artificial para la aplicación de la ley

La convocatoria se lanza de conformidad con el Programa de Trabajo del Mecanismo Temático 2023-2025 y será gestionado por la Dirección General de Migración y Asuntos de Interior (DG HOME) de la Comisión Europea.

La convocatoria cubre el tema: ISF/2024/SA/3.4.1 – AILE – Innovación: Inteligencia artificial para la aplicación de la ley.

La inteligencia artificial (IA) es una tecnología versátil que ya se ha vuelto indispensable en la caja de herramientas de los organismos encargados de hacer cumplir la ley. Puede mejorar las capacidades existentes, proporcionar nuevas herramientas y mejorar el desempeño y la eficiencia de los organismos encargados de hacer cumplir la ley en un panorama delictivo que cambia y evoluciona rápidamente. De este modo, ayuda a los organismos encargados de hacer cumplir la ley a dar una respuesta eficaz al crimen organizado y al terrorismo.

Esta nueva tecnología puede tener muchos beneficios para la seguridad interna de la UE, pero también entraña grandes riesgos si se utiliza de forma indebida. Los delincuentes también están explotando los beneficios de la innovación con fines maliciosos, para facilitar y ampliar sus actividades delictivas.

Al mismo tiempo, el uso de IA en el sector de la seguridad interna también genera preocupaciones y temores debido a la percepción de falta de transparencia de la tecnología de IA, su uso y el impacto general de estas tecnologías en los derechos fundamentales.

El 18 de julio de 2024, la presidenta de la Comisión Europea, Ursula von der Leyen, presentó ante el Parlamento Europeo Directrices políticas para la próxima Comisión Europea 2024-2029.

En estas directrices, la Comisión describe un plan integral para posicionar a Europa como líder mundial en innovación en inteligencia artificial (IA).

Además, como se afirma en la Estrategia de la Unión de la Seguridad de la UE 2020-2025, la inteligencia artificial podría actuar como una herramienta poderosa para prevenir y combatir la delincuencia grave y organizada, incluido el terrorismo, impulsando las capacidades de investigación, por ejemplo, analizando grandes cantidades de información e identificando patrones y anomalías. También puede proporcionar herramientas concretas para ayudar a identificar contenido terrorista en línea o descubrir transacciones sospechosas, identificar la venta de productos ilícitos y facilitar la recopilación de información.

La Estrategia señala que para materializar este potencial es necesario reunir la investigación, la innovación y los usuarios de la inteligencia artificial con la gobernanza y la infraestructura técnica adecuadas, involucrando activamente al sector privado, el mundo académico y los tecnólogos.



También significa garantizar los más altos estándares de cumplimiento de los derechos fundamentales, contribuyendo al mismo tiempo de manera efectiva a un alto nivel de seguridad interna.

La aplicación práctica de este enfoque también forma parte de la Estrategia de la UE para luchar contra la delincuencia organizada 2021-2025, en el que la Comisión se compromete a apoyar a los Estados miembros en relación con proyectos piloto sobre soluciones de inteligencia artificial que ayudarían a fomentar la adopción de innovación por parte de la comunidad policial.

Las fuerzas de seguridad, la industria y el mundo académico deberían cooperar entre sí, con el apoyo de la financiación de la UE, para desarrollar herramientas y soluciones a nivel de la UE que respondan a las necesidades de las fuerzas de seguridad de la UE, apoyando así también la labor de Europol en la prestación de servicios y soluciones técnicas a las fuerzas de seguridad de la UE. Este enfoque colaborativo debería garantizar la sostenibilidad de los proyectos de Horizonte Europa y del Fondo de Seguridad Interior y apoyar a Europol en esa labor, respetando el acervo pertinente y salvaguardando los derechos fundamentales.

Otro elemento clave es la regulación integral del uso de sistemas de inteligencia artificial a través del Reglamento de la UE sobre inteligencia artificial (AI Act) que entró en vigor el 1 de agosto de 2024. El Reglamento proporciona orientación y claridad jurídica a los desarrolladores e implementadores de sistemas de IA sobre cómo “mitigar eficazmente los riesgos para la salud, la seguridad y los derechos fundamentales”. Clasifica casos de uso específicos de IA según su riesgo potencial en cuatro niveles: riesgo inaceptable, riesgo alto, riesgo limitado y riesgo bajo o mínimo. Se prohíbe el uso de casos de uso que impliquen un riesgo inaceptable. En casos de "alto riesgo", los desarrolladores e implementadores (usuarios) deben cumplir con obligaciones detalladas que garanticen el uso adecuado de los sistemas de IA y mitiguen el riesgo que el sistema pueda generar. Dichos sistemas deben entrenarse utilizando conjuntos de datos sólidos y amplios para mejorar la eficacia, evitar sesgos y disminuir los resultados falsos positivos. La Ley de IA también es aplicable en el ámbito jurídico.

Los proyectos de investigación financiados por la UE han estado investigando el uso de la IA para la aplicación de la ley con resultados prometedores, al tiempo que estudian los desafíos que deben abordarse desde perspectivas jurídicas, éticas y sociales, como por ejemplo garantizar que los sistemas de IA salvaguarden los derechos fundamentales y se basen en los principios de responsabilidad y confiabilidad.

Las barreras y los desafíos a menudo obstaculizan la adopción de la innovación en el sector de la seguridad civil y su aplicación en las fuerzas del orden. Algunos ejemplos de estos desafíos son:

- La falta de financiación y vías de desarrollo dedicadas a fomentar la adopción de tecnologías y métodos innovadores, por ejemplo financiando desarrollos de última milla,

- Una comprensión limitada de cómo la contratación pública puede utilizarse como catalizador para la adopción de la innovación o,
- La visibilidad y trazabilidad limitadas de los resultados de investigaciones exitosas.

La financiación de la UE es necesaria para esta acción específica, dados los desafíos mencionados para la adopción de innovación, nuevos conocimientos, tecnologías, metodologías y asimilación de principios éticos y legales en el campo del uso de la inteligencia artificial para fines de aplicación de la ley y para apoyar el fortalecimiento de las capacidades de los Estados miembros en relación con la prevención y la lucha contra la delincuencia grave y organizada, incluido el terrorismo.

Además, hay un fuerte valor añadido de la UE en la promoción de las innovaciones europeas, ya que conducen al fortalecimiento de las capacidades existentes y al desarrollo de nuevas capacidades de aplicación de la ley. Estos instrumentos también pueden apoyar, por un lado, a los proveedores de tecnología en la industrialización y comercialización de productos innovadores, así como a las empresas creación y ampliación y, por otro lado, las autoridades competentes en la realización de pruebas o validaciones adicionales y la implementación de soluciones innovadoras.

Las sinergias entre la investigación y la innovación (I+i) financiadas por la Unión y el Fondo de Seguridad Interior pueden maximizar el impacto de la financiación a las fuerzas y cuerpos de seguridad aprovechando los resultados de investigación satisfactorios, prestando apoyo para probar, validar o implementar nuevos métodos y tecnologías derivados de acciones de I+i respaldadas por los principios de ética, transparencia y fiabilidad, y salvaguardando los derechos fundamentales.

1. El objetivo de esta acción específica es brindar apoyo financiero a los Estados miembros para facilitar la adopción (es decir, probar, validar, realizar más pruebas y/o implementar) de tecnologías y herramientas de IA confiables, éticas y transparentes por parte de las fuerzas del orden para una policía moderna y eficiente para prevenir y combatir la delincuencia grave y organizada, incluido el terrorismo.

A continuación, se facilitan los principales datos de la convocatoria extraídos de la misma.

2. Tipos de solicitantes a los que se dirige la convocatoria, siendo entidades legales como:

- personas jurídicas (organismos públicos o privados);
- las organizaciones internacionales son elegibles;

- otros entes podrán participar en otras funciones del consorcio, como socios asociados, subcontratistas, terceros que aporten contribuciones en especie, etc;
- las personas físicas NO son elegibles (con la excepción de los trabajadores por cuenta propia, es decir, cuando la empresa no tiene personalidad jurídica distinta de la de la persona física);
- los entes sin personalidad jurídica con arreglo a su legislación nacional podrán participar excepcionalmente, siempre que sus representantes tengan la capacidad de asumir obligaciones jurídicas en su nombre, y ofrecer garantías de protección de los intereses financieros de la UE equivalentes a las ofrecidas por las personas jurídicas;
- los organismos de la UE NO pueden formar parte del consorcio;
- asociaciones y agrupaciones de interés — Las entidades compuestas por miembros pueden participar como “beneficiarios únicos” o “beneficiarios sin personalidad jurídica” (si la acción será implementada por los miembros, también deben participar, ya sea como beneficiarios o como entidades afiliadas, de lo contrario, sus costos NO serán elegibles);
- países que actualmente negocian acuerdos de asociación: los beneficiarios de países con negociaciones en curso pueden participar en la convocatoria y pueden firmar subvenciones si las negociaciones concluyen antes de la firma de la subvención (con efecto retroactivo, si así lo establece el acuerdo).

3. Condiciones geográficas:

Los solicitantes (beneficiarios y entidades afiliadas) deben estar establecidos en cualquiera de los países elegibles:

- Todos los Estados miembros de la UE, excepto Dinamarca, o en un país o territorio de ultramar vinculado a éstos.
- Países no pertenecientes a la UE (no sean Estados miembros) que tengan un acuerdo operativo con Europol.

4. Actividades que se financiarán en el marco de la convocatoria de propuestas:

El apoyo se centrará en cofinanciación técnica, organizativa y/o social de soluciones con elementos innovadores obligatorios, en particular sobre cómo aplicar la nueva legislación de la UE (Ley IA).

Las propuestas de proyectos deben basarse en los resultados de la investigación y la innovación en materia de seguridad, especialmente retomando los resultados de las actividades financiadas por la UE, con el fin de garantizar algunos de los siguientes aspectos:

- Probar, validar, probar y/o implementar herramientas y sistemas de IA relevantes para la aplicación de la ley, basándose en los resultados de proyectos de investigación e innovación financiados por la UE.
- Mejorar la comprensión, los conocimientos y las prácticas en materia de IA en todas las autoridades educativas locales para promover el uso responsable de la IA basado en sólidas garantías jurídicas y éticas, incluido el logro del cumplimiento de la nueva Ley de IA;
- Mayor experiencia y capacidad de los organismos encargados de hacer cumplir la ley para contrarrestar la IA explotada para usos delictivos, incluidos, entre otros, la facilitación de delitos cibernéticos o ciberdependientes, por ejemplo, la generación delictiva de deepfakes o fraudes en línea.

La acción específica puede incluir, entre otras, actividades como:

- adopción y prueba de herramientas derivadas de programas de investigación financiados por la UE,
- validación y difusión de dichas herramientas,
- acciones operativas transfronterizas,
- mecanismos para intercambiar información a través de las fronteras,
- Capacitación y alfabetización en inteligencia artificial para las autoridades educativas locales.

En todos los casos, esto debería incluir capacitación en alfabetización en IA, así como orientación para las autoridades educativas locales.

Como resultado, los proyectos seleccionados deberán lograr uno o más de los siguientes objetivos:

- Mejorar la seguridad de los ciudadanos de la UE proporcionando a las fuerzas del orden herramientas de inteligencia artificial de vanguardia adaptadas a sus necesidades operativas.
- Facilitar la adopción rápida y eficaz de soluciones de IA para fines de aplicación de la ley, especialmente las procedentes de programas de investigación e innovación en materia de seguridad financiados por la Unión.
- Aumentar el uso seguro y responsable de las tecnologías de IA por parte de las autoridades educativas locales, es decir, promoviendo mecanismos para su implementación social, legal y ética.
- Aumentar la autonomía estratégica abierta europea mediante la implementación de soluciones desarrolladas en proyectos de investigación europeos.

Los proponentes deben centrarse en un tema en particular: Adopción de tecnología/tecnologías (probar, validar, pilotar y/o implementar más). No es obligatorio, pero bienvenido, abordar los avances relacionados con soluciones y métodos sociales y organizacionales innovadores para una IA confiable en la aplicación de la ley, incluidos nuevos conocimientos, recomendaciones y/o directrices adicionales.

Las acciones propuestas deben basarse en los resultados de proyectos de investigación e innovación anteriores. Algunos ejemplos de tales iniciativas incluyen, entre otros, los siguientes proyectos financiados por la UE:

- **STARLIGHT** es un proyecto que está reforzando las operaciones de investigación y ciberseguridad de las fuerzas de seguridad de la UE con herramientas basadas en IA que son transparentes, resistentes y explicables. Los avances técnicos del proyecto STARLIGHT tienen en cuenta los resultados de popAI y ALIGNER que se enumeran a continuación. Estos dos proyectos proporcionaron los principios necesarios para mejorar los esfuerzos de colaboración al tiempo que se salvaguardan los derechos fundamentales:
 - **popAI** Trabajó en un conjunto de recomendaciones para el uso ético de la IA por parte de las autoridades educativas locales y proporcionó una caja de herramientas éticas prácticas.
 - **ALIGNER** reúne a actores europeos para identificar conjuntamente cómo mejorar la seguridad protegiendo al mismo tiempo los derechos fundamentales.
- **TRACE** exploró el aumento y la propagación de los delitos cibernéticos y los flujos financieros ilícitos.
- **AIDA** centrado en el cibercrimen y el terrorismo abordando cuestiones específicas relacionadas con los (LEAs) utilizando métodos pioneros de aprendizaje automático e inteligencia artificial.
- **TENSOR** proporcionará a las autoridades policiales y a los institutos forenses una plataforma que podrán utilizar para facilitar la extracción, el intercambio y el almacenamiento de pruebas biométricas en entornos transfronterizos.
- **GRACE** se aplicaron técnicas probadas de aprendizaje automático a la derivación y elaboración de análisis, gestionando al mismo tiempo adecuadamente los desafíos técnicos, éticos y legales propios de la lucha contra la explotación sexual infantil.
- **TENACITY** desarrolla un Marco de Gobernanza de Inteligencia de Viajes que facilita la gestión y el acceso a los datos para ayudar a las fuerzas de seguridad a gestionar la inteligencia en las investigaciones de terrorismo y delincuencia grave y organizada.
- **VIGILANT** está desarrollando una plataforma que busca herramientas y tecnologías avanzadas de identificación y análisis de desinformación.
- **APPRAISE** es una solución integrada de inteligencia de amenazas para proteger el entorno de las ciudades aumentadas. Realiza un monitoreo continuo de fuentes en línea y sensores físicos para identificar amenazas potenciales y mejorar las estrategias de protección de objetivos blandos (como centros comerciales y estadios).

- **FERMI** proporcionará un conjunto de herramientas para detectar y monitorear la propagación de desinformación y noticias falsas e identificar sus fuentes, así como material de capacitación personalizado para autoridades policiales y judiciales, ciudadanos de la UE y otras partes interesadas relevantes.

Actualmente, nuevos desafíos que plantea la inmensa cantidad de datos, sin embargo, al mismo tiempo la disponibilidad y escasez de datos de alta calidad para entrenar herramientas basadas en inteligencia artificial en el contexto de la aplicación de la ley constituyen un obstáculo importante para la innovación en el campo de la seguridad interna. Por lo tanto, se alientan las propuestas para explorar más formas de facilitar el acceso de las fuerzas del orden a datos de alta calidad y, al hacerlo, se espera que se creen sinergias con:

- **LAGO** creará un ecosistema confiable de datos de investigación de la UE para facilitar la colaboración en materia de investigación orientada a los datos entre las fuerzas de seguridad del Estado, los profesionales de la seguridad, las agencias pertinentes de la UE, los investigadores y los responsables políticos.
- **TESSERA** tiene como objetivo realizar el trabajo preparatorio para la creación de conjuntos de datos a gran escala, confiables y compartibles de alta calidad basados en casos de uso operativos identificados, apoyando así el Espacio Europeo de Datos de Seguridad para la Innovación.

Puede encontrarse más información sobre la investigación y la innovación financiadas por la Unión en tecnologías y métodos de seguridad interior en:

- Portal de financiación y licitaciones de la UE (para temas y convocatorias pasadas, actuales y futuras),
- el Servicio Común de Información sobre Investigación y Desarrollo (CORDIS) (paraproyectos actuales y pasados),
- El panel de Horizon (para búsquedas agregadas por país, socio y tema),
- a través de la Comunidad Europea de Investigación e Innovación en Seguridad (CERIS), y
- de los puntos de contacto nacionales (PCN) para la investigación en materia de seguridad de la UE en cada Estado miembro,
- de la Unidad de Investigación en Innovación y Seguridad de la DG HOME.

La compra de productos y servicios que estén disponibles comercialmente, a menos que sean una parte muy menor y complementaria del esfuerzo de integración en una solución innovadora, no están respaldadas por esta acción. La compra de tecnología disponible en el mercado es posible en el marco de otros instrumentos de financiación del FSI o de otros instrumentos de financiación de la UE, por ejemplo, los programas de los Estados miembros del FSI y el FEDER (Fondo Europeo de Desarrollo Regional).

La acción específica puede incluir, entre otras, actividades como:

- pruebas, validación y/o pruebas piloto adicionales (incluso en grupos de Estados miembros) en un entorno real,
- evaluación de herramientas de IA para la madurez operativa,
- instalación e integración en sistemas heredados,
- despliegue,
- capacitación práctica sobre el uso de las nuevas soluciones.

Se fomenta la cooperación con Europol en cualquiera de estos elementos, especialmente la utilización del repositorio de herramientas de Europol, ya que podría potenciar la calidad y el impacto de las propuestas. Cuando sea pertinente para el desarrollo de sus propuestas, también se anima a los estados miembros a que tengan en cuenta la lista de cumplimiento para IA (CC4AI). Esta herramienta web, creada por Europol, ayuda a los profesionales a evaluar el cumplimiento de los sistemas y herramientas de IA con los requisitos y obligaciones de la Ley de IA.

El artículo 5 del Reglamento del FSI establece que esta financiación no será elegible para:

- acciones limitadas al mantenimiento del orden público a nivel nacional;
- acciones con fines militares o de defensa;
- equipos cuyo objetivo principal sea el control aduanero;
- equipo coercitivo, incluidas armas, municiones, explosivos y porras antidisturbios, excepto para fines de entrenamiento; (...).

Si se prevén gastos para la adquisición de equipos o medios de transporte o la construcción de edificios o instalaciones relacionados con la seguridad y se selecciona la propuesta de proyecto, la autoridad de gestión del FSI del Estado miembro debe asegurarse de que el gasto se incluirá en el cálculo del Programa del FSI para el umbral del 35 % estipulado en el artículo 13 del Reglamento del FSI.

Las propuestas deben explicar los planes para la futura implantación y/o ampliación de las nuevas tecnologías y/o métodos, en caso de que las actividades financiadas por esta acción específica tengan éxito. Se puede planificar una mayor implantación, utilización y/o ampliación operativa con el apoyo de la financiación nacional, de los programas de los Estados miembros del Fondo de Seguridad Institucional y/o de otros fondos públicos o privados.

Se acogerán especialmente con agrado las propuestas de proyectos que presenten un plan creíble y comprometido para una mayor adopción, ya que garantizarán un impacto en las capacidades de las autoridades competentes.

La convocatoria de manifestaciones de interés está abierta tanto a propuestas de proyectos nacionales como transnacionales. Sin embargo, en ambos casos, las propuestas deben exponer de forma clara y convincente Demostrar el impacto transnacional de sus esfuerzos.



En el caso de una propuesta de proyecto transnacional, el Estado miembro principal deberá asegurarse de que la autoridad de gestión del FSI de cada Estado miembro participante firme debidamente el «formulario de declaración de asociación». En el formulario de solicitud, se debe enumerar a cada beneficiario del proyecto en cada Estado miembro participante y se debe indicar la parte que recibirá cada Estado miembro del importe adicional asignado, si la propuesta de proyecto resulta aceptada. Sobre la base de este acuerdo común, cada socio tendrá un papel y las consiguientes responsabilidades en la ejecución del proyecto y en el cumplimiento de sus objetivos.

Las acciones específicas propuestas no deben centrarse en actividades relacionadas con la investigación, sino que deben apoyar la adopción y el uso de soluciones innovadoras derivadas del pasado de investigación. Por lo tanto, las nuevas tecnologías abordadas en las propuestas de proyecto (que no son necesariamente las únicas tecnologías involucradas, pero deberían ser las principales) deben tener un nivel de preparación tecnológica (TRL) no inferior a 8 al inicio del proyecto. Se valorará la presentación de pruebas del nivel de TRL de la(s) tecnología(s) seleccionada(s).

Esta acción específica se enmarca específicamente en el apartado (e) del Anexo III del Reglamento ISF, en lo relativo al apoyo a:

e) «acciones que desarrollen métodos innovadores o desplieguen nuevas tecnologías con potencial de transferibilidad a otros Estados miembros, en particular proyectos destinados a probar y validar los resultados de proyectos de investigación en materia de seguridad financiados por la Unión»; Los Estados miembros pueden proponer tanto proyectos ejecutados íntegramente a nivel nacional como proyectos ejecutados transnacionalmente por un grupo de Estados miembros. En el primer caso, los Estados miembros proponentes deben explicar el valor añadido específico de su enfoque transnacional.

5. El presupuesto disponible es de 2.000.000 EUR.

La DG Home se reserva el derecho de no otorgar todos los fondos disponibles o de redistribuirlos entre los temas de la convocatoria, en función de las propuestas recibidas y los resultados de la evaluación.



6. Calendario y plazos:

- Fecha de inicio: 1 de septiembre de 2024.
- Fecha límite de remisión: 14 de febrero de 2024.
- Firma del Acuerdo de Subvención: abril de 2025.

7. Duración: los proyectos deben completarse antes del 31 de diciembre de 2027.

8. El presupuesto para cada proyecto aprobado será de entre 200.000 y 1.000.000 euros (siendo el presupuesto total de 2.000.000 de euros, teniendo en cuenta que se pueden aprobar varios proyectos a la vez).

9. Seguimiento y evaluación

La DG HOME evaluará las propuestas presentadas por los Estados miembros. Para que una propuesta sea considerada admisible, deberá:

1. presentarse dentro de la fecha límite al buzón funcional de acciones específicas de la ISFHOME-ISF-SPECIFIC-ACTIONS@ec.europa.eu,
2. consistente en el formulario oficial de Solicitud ISF/2024/SA/3.4.1 adjunto a esta Nota junto con sus anexos, que deben ser legibles y completos (se rellenan todos los campos necesarios para la evaluación),
3. ser presentado por la autoridad de gestión en nombre de la entidad del Estado miembro que será responsable de la ejecución de la acción específica,
4. identificar un beneficiario del proyecto (una entidad) que será responsable de la implementación de la acción específica en el Estado miembro (a cargo de la acción),
5. en caso de un proyecto transnacional: incluir formularios de declaración de asociación firmados por las autoridades de gestión de todos los Estados miembros participantes.

La DG HOME evaluará las propuestas admisibles basándose en los siguientes criterios:

A. Relevancia (30 puntos –Puntuación mínima: 15 puntos)

1. Claridad de la solución propuesta, su correspondencia con los objetivos y alcance de esta convocatoria de manifestación de interés, y su contribución hacia los indicadores de resultados y productos enumerados en el Anexo VIII del Reglamento del FSI (véase el Anexo 4).

2. Innovación de la solución propuesta (de mín. TRL 8) en comparación con las herramientas de última generación disponibles.

B. Calidad y contenido (30 puntos –Puntuación mínima: 15 puntos)

1. Madurez de la propuesta; idoneidad del diseño y planificación implementación, considerando las actividades previstas; metodología (incluyendo gestión operativa y financiera); organización del trabajo y estrategia para la gestión y seguimiento de proyectos; medidas adoptadas o previstas para mitigar los riesgos identificados.
2. Rentabilidad, complementariedad y sostenibilidad: la propuesta debe presentar la distribución del apoyo financiero solicitado y su adecuación en relación con la escala y el tipo de las actividades previstas (personal, viajes, formación, etc.). También debe demostrar la relación coste-eficacia y la relación calidad-precio generales, así como la complementariedad con otras fuentes de financiación de la UE (programas del FSI de los Estados miembros, convocatorias de propuestas del FSI en el marco de las acciones de la Unión, programas de subvenciones de EUROPOL EMPACT, etc.). Por último, debe explicarse el modelo de sostenibilidad, incluido un plan creíble para futuros despliegues y/o ampliación una vez finalizada la duración de esta acción.

C. Impacto (40 puntos –Puntuación mínima: 20 puntos)

1. Valor añadido de la UE: los beneficios concretos y los resultados cuantificados del proyecto para el Se deberá demostrar la existencia de un acuerdo de colaboración entre la Unión Europea y el Estado o los Estados miembros interesados, así como su potencial de transferibilidad.
2. Impacto de la solución propuesta de desarrollo de capacidades y/o mejora de una capacidad/sistema existente basado en IA para el cumplimiento de la ley.
3. Participación y cooperación con entidades competentes de los Estados miembros (autoridades competentes, entidades privadas y públicas, por ejemplo, organizaciones de investigación, industria) y entidades pertinentes de la UE (por ejemplo, Europol, CEPOL) cuando corresponda, y explicaciones sobre cómo se logrará esto.
4. Difusión y comunicación estrategia, incluida la transferibilidad de la solución a otros Estados miembros, y su relación y/o contribución a Autonomía estratégica europea.

Los Estados miembros deben garantizar el respeto de los principios horizontales descritos en el artículo 9 del Reglamento (UE) 2021/1060, incluido el respeto de los derechos fundamentales y el cumplimiento de la Carta de los Derechos Fundamentales de la Unión Europea, así como del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680 (20).

Además, los Estados miembros también deben garantizar que las acciones previstas no se vean afectadas por un dictamen motivado emitido por la Comisión con respecto a un procedimiento de infracción con arreglo al artículo 258 del Tratado de Funcionamiento de la Unión Europea (TFUE) que ponga en duda la legalidad y regularidad del gasto o la ejecución de las acciones (artículo 8, apartado 5, del Reglamento (UE) 2021/1149).