“LÍNEAS TEMÁTICAS 2026/2027”

Este documento recoge nuestras líneas prioritarias para el próximo año en relación con la Red de grupos de excelencia en investigación sobre privacidad, protección de datos y tecnologías emergentes. Estas líneas reflejan áreas estratégicas en las que consideramos fundamental impulsar proyectos, colaboraciones, debates y resultados concretos que fortalezcan el impacto colectivo de la Red.

No se trata de un listado cerrado: es una **invitación a la co-creación**. Os animamos a que, además de alinear vuestras propuestas con estas prioridades, nos hagáis llegar aquellas líneas o temas emergentes que consideréis relevantes para el avance de la Red. Nuestro objetivo es que este proceso sea bidireccional, flexible y enriquecedor para todos.

Líneas temáticas en el área legal

Título	Código de línea	Problema encontrado/Interés en la línea específica
Fuentes, legalidad y posición de la autoridad de control	L1	Potestad normativa de la Agencia Española de Protección de Datos y límites derivados del principio de legalidad: Análisis del alcance de la capacidad de la Agencia para dictar circulares e instrucciones, especialmente tras la doctrina del Tribunal Constitucional de 2019, que limita su posible función de colaboración normativa con la ley. El reto principal reside en determinar hasta qué punto puede concretar o desarrollar obligaciones sin invadir la reserva de ley, en ámbitos como el estatuto del delegado de protección de datos o el uso de datos biométricos.
	L2	Naturaleza jurídica y efectos de guías, notas técnicas y otros instrumentos de *soft law* de la autoridad de control: Delimitación del valor jurídico de estos instrumentos a partir del RGPD, la LOPDGDD y el estatuto de la AEPD. El problema central radica en su utilización práctica como criterios cuasi vinculantes, especialmente en el ámbito sancionador, lo que plantea tensiones con los principios de tipicidad y seguridad jurídica.
	L3	Principio de legalidad en el tratamiento de datos por el sector público y reacción de las autoridades ante normas habilitantes insuficientes: Supuestos en los que la base normativa del tratamiento no cumple plenamente las exigencias de legalidad, ya sea por falta de rango o por insuficiencia de garantías. Se plantea qué margen tiene la autoridad de control para reaccionar ante normas defectuosas desde la perspectiva del RGPD.
Derecho sancionador de protección de datos: Análisis comparativo en el contexto internacional y con otras normas nacionales en las que se	L4	Configuración del ilícito administrativo en protección de datos - concurso de infracciones y principio non bis in idem: Delimitación de infracciones en el marco del RGPD y la LOPDGDD, con especial atención a la posible sobrefragmentación de conductas. El reto consiste en determinar cuándo varias vulneraciones pueden reconducirse a un número más reducido de tipos sancionadores.

prevé multa administrativa pero no están previstas otro tipo de medidas correctivas	L5	Aplicación del derecho sancionador en materia de brechas de seguridad/ de datos personales y evolución de los criterios de imputación: Análisis de la evolución reciente en la calificación de infracciones, la graduación de sanciones y la valoración de atenuantes y agravantes, incluyendo el impacto de medidas correctoras adoptadas tras la brecha.
	L6	Aplicación del principio de responsabilidad proactiva (*accountability*) en el ámbito sancionador y sus límites derivados del principio de culpabilidad: La exigencia de demostrar el cumplimiento no puede implicar inversión de la carga de la prueba ni responsabilidad objetiva. El reto es compatibilizar la responsabilidad proactiva con los principios de culpabilidad, tipicidad y presunción de inocencia.
Interacción con otros marcos regulatorios	L7	Concurrencia de regímenes sancionadores entre el RGPD y el Reglamento de Inteligencia Artificial: Análisis de los riesgos de doble sanción derivados de la aplicación simultánea de ambos marcos normativos sobre un mismo tratamiento. Análisis de los riesgos y oportunidades involucrados en la existencia de dos autoridades de supervisión diferentes.
Inteligencia artificial y tratamientos algorítmicos	L8	Tratamiento de datos en el ámbito laboral mediante inteligencia artificial y papel de la negociación colectiva: Análisis de las posibilidades de los convenios colectivos para regular el uso de IA en el tratamiento de datos de empleados.
	L9	Uso de categorías especiales de datos en sistemas de inteligencia artificial y tensión con la mitigación de sesgos: Estudio de la utilización de datos sensibles para cumplir requisitos técnicos de los sistemas de IA y su compatibilidad con el RGPD.
Principios del RGPD y modelos de negocio basados en datos	L10	Modelos de pago o consentimiento en servicios digitales y validez del consentimiento en contextos de desequilibrio: Análisis de la licitud de modelos que condicionan el acceso a servicios al pago o a la aceptación del tratamiento de datos.
	L11	Anonimización y seudonimización de datos personales: estándares y límites prácticos: Estudio de las condiciones para considerar efectiva la anonimización y el riesgo de reidentificación.
	L12	Impacto económico de la protección de datos en organizaciones y sectores económicos: Estudio del efecto del cumplimiento del RGPD en términos de costes, competitividad y organización empresarial.
Salud y espacios de datos de alta sensibilidad	L13	Tratamiento de datos de personas mayores en contextos sociosanitarios, especialmente en residencias: Análisis de los riesgos derivados de la vulnerabilidad del colectivo y del entorno institucional.
Sectores y contextos específicos	L14	Relación entre protección de datos y transparencia pública: conflictos y criterios de armonización: Estudio de la colisión entre acceso a la información pública y protección de datos. Análisis de casos como los relativos al principio de minimización en contextos de revelación pública, por ejemplo, de datos sobre la situación de baja de los trabajadores.

Líneas temáticas en el área científico-técnica

Título	Código de línea	Problema encontrado/Interés en la línea específica
Prueba de conocimiento cero (ZKP)	CT1	Las soluciones actuales para verificación de atributos y análisis de datos suelen requerir la revelación de datos personales, lo que implica diferentes amenazas para la privacidad. Las pruebas de conocimiento cero (ZKP) permiten verificar atributos y afirmaciones (por ejemplo "soy mayor de edad" o "tengo un título universitario") sin revelar los datos subyacentes, pero su implementación práctica en entornos reales sigue siendo limitada: Análisis de casos de uso reales que podemos encontrar validados en sectores regulados (salud, banca, administración pública) y propuestas prácticas de implementación.
Unlearning en modelos de inteligencia artificial	CT2	Los modelos de IA entrenados con datos personales (modelos de lenguaje, modelos de recomendación o toma de decisiones, modelos predictivos) no permiten eliminar selectivamente la influencia de datos específicos sin reentrenar el modelo desde cero. Esto dificulta el cumplimiento del derecho al olvido (Artículo 17 RGPD) y expone a los titulares de los datos a amenazas como la vinculación, la identificación, la revelación de información o la falta de transparencia o de control: Estudio de métodos eficientes para *unlearning* en modelos complejos (*transformers*, redes neuronales profundas) y también para la validación de dicho *unlearning*.
Revocación de credenciales para la EUDI Wallet	CT3	La EUDI Wallet permite a los ciudadanos europeos solicitar, almacenar y presentar credenciales digitales (permisos de conducir, títulos académicos, etc.). Sin embargo, los mecanismos actuales de revocación de credenciales pueden comprometer la privacidad al permitir la vinculación de transacciones (*linkability*) o la identificación del usuario: Propuesta de técnicas de revocación eficiente con privacidad fuerte (por ejemplo, sin revelar la identidad del usuario o su historial de transacciones).
Servicios que implican el tratamiento de datos genéticos en tratamientos distintos a la asistencia sanitaria sometida a la normativa sectorial, investigación científica en salud, o en el marco de la Ley 7/2021	CT4	Los datos genéticos y los marcadores de ADN se han utilizado en el ámbito de servicios a usuarios finales para dar información sobre posibles ancestros o tendencias a enfermedades fuera del ámbito del análisis clínico. También se están viendo mensajes de utilización de ADN como sistemas biométricos de identificación: Análisis de productos y servicios para el usuario final que impliquen tratamientos de datos genéticos (fuera de casos clínicos, de investigación o de uso por FyCSE).
Criptografía post-cuántica y PETs en tratamientos de datos personales	CT5	La llegada de la computación cuántica amenaza con romper los algoritmos criptográficos actuales (como RSA o ECC), lo que podría comprometer la seguridad de los datos personales. Es necesario anticiparse a este escenario para garantizar que los tratamientos de datos sigan siendo seguros en la era post-cuántica: Análisis de las PETs más prometedoras para proteger datos personales en un entorno post-cuántico, necesidad de adaptaciones, propuesta de estrategias de migración, etc.