ANEXO II

RESUMEN EJECUTIVO

Título
Riesgos para los derechos fundamentales en tratamientos biométricos no identificantes mediante inteligencia artificial: límites del Reglamento de IA y papel del RGPD

Autora
Leire Escajedo San-Epifanio

1. Objetivo / hipótesis

El objetivo del trabajo es identificar y evaluar los riesgos específicos para los derechos y libertades de las personas derivados de tratamientos biométricos no identificantes basados en sistemas de inteligencia artificial, así como analizar en qué medida dichos riesgos quedan adecuadamente abordados por el Reglamento (UE) 2024/1689 de Inteligencia Artificial. La hipótesis de partida sostiene que determinadas modalidades de captación biométrica no identificante pueden generar riesgos elevados que no siempre activan los mecanismos de protección reforzada previstos en el Reglamento de IA, lo que hace necesaria una aplicación especialmente exigente del principio de responsabilidad proactiva del Reglamento General de Protección de Datos.

2. Justificación de la investigación

El uso creciente de sistemas de inteligencia artificial capaces de captar y procesar señales corporales, atencionales o conductuales en tiempo real, sin finalidad identificante, se ha normalizado en entornos digitales, comerciales y de interacción cotidiana. Aunque estas prácticas no persiguen la identificación de las personas, pueden incidir de manera relevante en la autonomía personal, la igualdad material y la autodeterminación informativa, al permitir inferencias situacionales y ajustes dinámicos del entorno de interacción. Sin embargo, el marco europeo de gobernanza de la inteligencia artificial tiende a abordarlas de forma fragmentaria, atendiendo a categorías y contextos de uso específicos, lo que justifica la necesidad de un análisis autónomo desde la óptica de la protección de datos y de la gestión preventiva del riesgo.

3. Diseño y metodología

El estudio adopta una metodología jurídico-técnica aplicada, orientada a la evaluación ex ante de riesgos para los derechos fundamentales. Se basa en el análisis sistemático del marco normativo europeo aplicable, en particular del RGPD y del Reglamento de IA, en el examen de arquitecturas técnicas de reconocimiento biométrico no identificante y en la identificación de riesgos conforme a los criterios derivados del principio de responsabilidad proactiva. La metodología incorpora elementos propios de las evaluaciones de impacto en protección de datos y de la protección de datos desde el diseño y por defecto, con el objetivo de articular un enfoque de análisis y gestión del riesgo susceptible de aplicación práctica.

4. Resultados principales

El trabajo pone de manifiesto que determinadas modalidades de biometría no identificante, en particular aquellas basadas en inferencias emocionales, atencionales o

conductuales en tiempo real, pueden generar riesgos elevados para los derechos y libertades de las personas, pese a no activar los umbrales clásicos asociados a la identificación biométrica. Asimismo, se constata que el Reglamento de IA no aborda estos riesgos de forma integral ni sistemática, lo que desplaza en la práctica el control preventivo hacia los instrumentos del RGPD y refuerza el papel de las Autoridades de Protección de Datos como garantes de una evaluación material del riesgo.

5. Novedad y aplicabilidad

La principal aportación del estudio consiste en sistematizar los tratamientos biométricos no identificantes como un ámbito autónomo de riesgo desde la perspectiva de la protección de datos y de los derechos fundamentales. Sobre esta base, se formulan criterios operativos para su evaluación y gestión mediante el principio de responsabilidad proactiva, permitiendo traducir los principios del RGPD en decisiones concretas de diseño, despliegue y supervisión de sistemas de inteligencia artificial que operan sobre señales biométricas no identificantes.

6. Conclusiones

El trabajo concluye que la protección efectiva frente a los riesgos derivados de la biometría no identificante exige reforzar el uso de las herramientas preventivas del RGPD, en particular la identificación sistemática de riesgos, la realización de evaluaciones de impacto cuando proceda y la aplicación de medidas de protección de datos desde el diseño y por defecto. En este contexto, la responsabilidad proactiva se configura como el principal instrumento operativo actualmente disponible para garantizar los derechos y libertades de las personas, como complemento necesario —pero no sustitutivo— del marco establecido por el Reglamento de IA.

Executive summary

Title
Risk assessment of non-identifying biometric processing through artificial intelligence: limits of the AI Act and the role of the GDPR

Author
Leire Escajedo San-Epifanio

1. Aim and hypothesis

The aim of this study is to identify and assess the specific risks to individuals' rights and freedoms arising from non-identifying biometric processing based on artificial intelligence systems, and to examine the extent to which such risks are adequately addressed by the AI Act (Regulation (EU) 2024/1689). The underlying hypothesis is that certain forms of non-identifying biometric processing may give rise to high risks that do not consistently trigger the enhanced safeguards provided by the AI Act, thereby requiring a particularly demanding application of the accountability principle under the General Data Protection Regulation.

2. Rationale of the research

The increasing deployment of artificial intelligence systems capable of capturing and processing bodily, attentional or behavioural signals in real time, without an identifying purpose, has become normalised in digital, commercial and everyday interaction environments. Although these practices are not intended to identify individuals, they may significantly affect personal autonomy, substantive equality and informational self-determination by enabling situational inference and adaptive modulation of interaction environments. The European framework for AI governance, however, tends to address such practices in a fragmented and context-dependent manner, structured around predefined categories and specific contexts of use. This fragmentation justifies the need for a dedicated analysis from a data protection and preventive risk management perspective.

3. Design and methodology

The study adopts an applied legal-technical methodology focused on ex ante risk assessment. It is based on a systematic analysis of the European regulatory framework applicable to non-identifying biometric processing, in particular the GDPR and the AI Act, combined with the examination of technical architectures used for biometric inference without identification. The analysis identifies and assesses risks in line with the requirements of the accountability principle. The methodology incorporates key elements of data protection impact assessments, as well as data protection by design and by default, with the aim of developing a practically applicable approach to risk analysis and governance.

4. Main findings

The study shows that certain forms of non-identifying biometric processing, particularly those based on real-time emotional, attentional or behavioural inference, may entail high risks to individuals' rights and freedoms, despite not meeting the traditional thresholds associated with biometric identification. It further indicates that the AI Act does not address these risks in a comprehensive or systematic manner, which in practice shifts

preventive control towards the instruments of the GDPR and reinforces the supervisory and preventive role of Data Protection Authorities.

5. Novelty and applicability

The main contribution of the study lies in conceptualising non-identifying biometric processing as an autonomous domain of risk from a data protection and fundamental rights perspective. On this basis, the study proposes operational criteria for assessing and managing such risks through the accountability principle, enabling GDPR requirements to be translated into concrete decisions regarding the design, deployment and oversight of artificial intelligence systems that operate on non-identifying biometric signals.

6. Conclusions

The study concludes that effective protection against the risks associated with non-identifying biometric processing requires a strengthened use of the GDPR's preventive tools, in particular systematic risk identification, the performance of data protection impact assessments where appropriate, and the implementation of data protection by design and by default measures. In this context, accountability emerges as the primary operational mechanism for safeguarding individuals' rights and freedoms, as a necessary complement to—rather than a substitute for—the regulatory framework established by the AI Act.