Revista Científica
DE LA FACULTAD DE DERECHO
Y CIENCIAS SOCIALES
Y POLÍTICAS - UNNE

El Reglamento de Inteligencia Artificial de la Unión Europea y su impacto en los derechos de las personas migrantes: Un análisis crítico

The European Union's Artificial Intelligence Act and its impact on the human rights of migrants: a critical analysis

Daiana Estefanía Yovan
Instituto de Justicia y Derechos Humanos,
Universidad Nacional de Lanús, Argentina
daiana.yovan@gmail.com
ORCID: https://orcid.org/0000-0001-6333-5885
Licenciada en Ciencia Política de la Universidad de Buenos Aires (UBA), Argentina
Especialista en Gobierno Abierto, Organización de Estados Americanos (OEA).
Doctoranda, Derechos Humanos de la Universidad Nacional de Lanús (UNLa)
Becaria del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)

Recepción: 6 de marzo de 2025
Aceptación: 14 de mayo de 2025

Resumen

Este artículo examina críticamente el reciente Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (en adelante, RIA o Reglamento de Inteligencia Artificial) de la Unión Europea (UE) desde la perspectiva de los derechos humanos, con especial énfasis en su impacto sobre las personas migrantes y en movilidad. A través de un análisis detallado del marco regulatorio y sus excepciones, se argumenta que la legislación establece un régimen diferenciado que podría comprometer los derechos fundamentales de las poblaciones

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

vulnerables, particularmente en el contexto de la migración y el control fronterizo. El estudio revela cómo las excepciones y exenciones incorporadas en el reglamento, especialmente en materia de seguridad nacional y control migratorio, podrían facilitar prácticas de vigilancia discriminatoria y socavar las protecciones previstas para otros ámbitos de aplicación, generando tensiones con otros marcos normativos europeos como los de interoperabilidad y protección de datos.

Palabras clave: Inteligencia Artificial, Regulación, Derechos Humanos, Migración, Vigilancia, Unión Europea, Interoperabilidad, Sesgo Algorítmico

Abstract

This article critically examines the recent European Union (EU) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (hereinafter, AI Act or Artificial Intelligence Regulation) from a human rights perspective, with a particular focus on its impact on migrants and people in mobility. Through a detailed analysis of the regulatory framework and its exceptions, it is argued that the legislation establishes a differentiated regime that could compromise the fundamental rights of vulnerable populations, especially in the context of migration and border control. The study reveals how the exceptions and exemptions incorporated into the law, particularly concerning national security and migration control, could facilitate discriminatory surveillance practices and undermine protections intended for other areas of application, creating tensions with other European regulatory frameworks such as those for interoperability and data protection.

Keywords: Artificial Intelligence, Regulation, Human Rights, Migration, Surveillance, European Union, Interoperability, Algorithmic Bias

1. Introducción

La aprobación del Reglamento de Inteligencia Artificial (RIA) de la UE el 13 de marzo de 2024 representa un momento decisivo en la historia de la regulación tecnológica global. Como primera legislación integral en esta materia, el reglamento establece un precedente significativo que probablemente influirá en futuras regulaciones en otras jurisdicciones. Sin embargo, mientras el texto ha sido ampliamente celebrado como un avance pionero, un análisis más detallado revela preocupaciones significativas sobre su aplicación en el ámbito de la migración y el control fronterizo.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Si bien la legislación introduce un marco regulatorio basado en riesgos que busca equilibrar la innovación tecnológica con la protección de los derechos fundamentales, este equilibrio parece inclinarse significativamente cuando se trata de la gestión migratoria y la seguridad fronteriza, áreas donde las excepciones y derogaciones abundan. Cabe señalar que el RIA emerge en un contexto de creciente tecnificación del control migratorio europeo, caracterizado por la proliferación de bases de datos interoperables (SIS II, VIS, Eurodac - véase el Reglamento (UE) 603/2013) y sistemas de vigilancia fronteriza. Esta digitalización de la frontera (Broeders, 2007), que se apoya en marcos como los establecidos por el Reglamento (UE) 2019/817 y el Reglamento (UE) 2019/818 para la interoperabilidad, se enmarca en un proceso más amplio de securitización de la migración (Bigo, 2002), donde la movilidad humana es construida como un problema de seguridad que requiere soluciones tecnológicas. En este contexto, el RIA podría permitir el uso de sistemas de Inteligencia Artificial que podrían ser perjudiciales cuando se usen para la seguridad nacional, la vigilancia biométrica en las fronteras y allanar el camino para el uso de la Inteligencia Artificial por parte de la policía en determinadas circunstancias. Surge así una cuestión clave sobre la coherencia entre los objetivos de eficiencia y seguridad promovidos por los reglamentos de interoperabilidad y las salvaguardias de derechos fundamentales que el RIA pretende, pero parece debilitar en el contexto migratorio.

Este artículo examina estas tensiones y sus implicaciones para los derechos humanos de las personas en movilidad. El presente análisis se fundamenta en una perspectiva crítica de los derechos humanos, entendiendo estos como indivisibles y universales, principios que deberían aplicarse independientemente del estatus migratorio de las personas. La metodología empleada combina el análisis jurídico documental con una perspectiva crítica de la migración, prestando especial atención a cómo las tecnologías de control pueden reforzar y amplificar desigualdades estructurales existentes. Este enfoque permite examinar no solo el contenido formal de la legislación, sino también sus efectos prácticos sobre las poblaciones más vulnerables.

2. El marco de la excepción

La teoría de la securitización, desarrollada por la Escuela de Copenhague (Buzan, Wæver y de Wilde, 1998), es clave para comprender cómo la migración ha sido discursivamente construida como una amenaza a la seguridad en Europa. Este marco teórico ayuda a entender cómo el RIA refuerza esta tendencia al legitimar prácticas de control y vigilancia a través de la tecnología. El Artículo 2.3 del Reglamento establece una amplia exención para los sistemas de IA utilizados exclusivamente con fines de seguridad nacional (una cuestión justificada en parte por el legislador en considerandos como el Cdo. 33, pero criticada por organizaciones de derechos digitales por su potencial de abuso, ver

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

EDRi, 2023), creando una laguna jurídica que resulta particularmente preocupante en el contexto migratorio. Según este artículo, las normas del reglamento no se aplican a sistemas desarrollados o empleados con fines militares, de defensa o de seguridad nacional, independientemente de si estos son operados por entidades públicas o privadas.

Esta disposición podría permitir a los Estados miembros utilizar sistemas de IA para el control migratorio, invocando la seguridad nacional para evitar cumplir con salvaguardias como evaluaciones de impacto en derechos fundamentales, estándares técnicos estrictos o requisitos contra la discriminación (Molnar & Gill, 2022). Esto abre la puerta a prácticas de vigilancia masiva en las fronteras bajo el pretexto de seguridad nacional, sin realizar una evaluación de impacto sobre los derechos fundamentales y sin garantizar que el sistema de IA cumpla altos estándares técnicos y no discrimine a ciertos grupos.

3. Arquitectura legal de un régimen diferenciado

El sistema de clasificación de riesgos

El Reglamento de Inteligencia Artificial de la Unión Europea es una legislación clave que regula el uso de los sistemas de IA dentro de la UE, basándose en un enfoque de evaluación de riesgos. Esta normativa clasifica los sistemas de IA según el nivel de riesgo que representan para la salud, la seguridad y los derechos fundamentales de las personas, lo que permite establecer distintos niveles de regulación y requisitos dependiendo del impacto potencial de cada sistema.

La clasificación de riesgos se divide en cuatro categorías: prácticas prohibidas, alto riesgo, riesgo limitado y riesgo mínimo. En cuanto a las prácticas prohibidas, se incluyen aquellas tecnologías que presentan un alto potencial de violación de derechos fundamentales, como técnicas subliminales para manipular el comportamiento, la explotación de grupos vulnerables, la categorización biométrica para inferir datos sensibles, la calificación social por entidades públicas o privadas, y el reconocimiento biométrico en tiempo real en espacios públicos (con excepciones). Estas prácticas están vedadas debido a su capacidad para vulnerar derechos fundamentales, como la privacidad y la no discriminación.

Los sistemas de alto riesgo son aquellos que pueden tener un impacto significativo en los derechos fundamentales y abarcan áreas como la biometría, infraestructura crítica, educación, empleo, servicios esenciales, aplicación de la ley, migración y administración de justicia (la inclusión de la migración como alto riesgo, reflejada en el Cdo. 60, fue un punto clave del debate legislativo, aunque persisten críticas sobre si la clasificación es suficientemente protectora; ver Ryan & Leufer, 2023). Estos sistemas deben cumplir con rigurosos requisitos de evaluación y registro (detallados en parte en considerandos como

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

el Cdo. 73, que enfatizan la necesidad de documentación técnica y sistemas de gestión de riesgos; véase Veale & Zuiderveen Borgesius, 2021, para un análisis de estos requisitos).

Por otro lado, los sistemas de riesgo limitado presentan un menor impacto y están sujetos a requisitos de transparencia, como la obligación de informar a los usuarios de que están interactuando con un sistema de IA. Finalmente, los sistemas de riesgo mínimo no están sujetos a requisitos específicos bajo la legislación, ya que su impacto potencial se considera insignificante.

El ámbito migratorio y la excepcionalidad de la clasificación de riesgos

En el contexto migratorio, el Anexo III, punto 7, clasifica como de alto riesgo los sistemas de IA utilizados en "la gestión de la migración, el asilo y el control de fronteras". Sin embargo, esta clasificación resulta insuficiente, ya que las tecnologías de vigilancia migratoria son cada vez más diversas y comunes, y muchas de ellas deberían considerarse prohibidas por su impacto negativo sobre los derechos fundamentales (Access Now, 2023). Este fenómeno refleja una contradicción en la ley: si bien se reconoce el peligro de ciertos sistemas, al mismo tiempo se desactivan las alarmas y mecanismos de control, lo que institucionaliza un régimen diferenciado de vigilancia tecnológica. Este enfoque podría profundizar las dinámicas de discriminación y control sobre las poblaciones migrantes, exponiéndolas a riesgos adicionales.

La definición de un sistema de alto riesgo se basa en la autoevaluación realizada por el productor del sistema, tal como se establece en el Artículo 43. Si el proveedor considera que un sistema de IA listado en el Anexo III no es de alto riesgo, deberá documentar su evaluación antes de comercializarlo o ponerlo en servicio. Esta evaluación debe registrarse en la base de datos pública creada por la Unión Europea (cuya gestión por la Comisión se detalla en el Cdo. 131, aunque la efectividad de esta base de datos para la rendición de cuentas ha sido cuestionada; Smuha et al., 2021), pero las sanciones por una clasificación errónea se limitan a una multa. Aunque la normativa debería exigir una evaluación externa, en el caso de los sistemas de IA en el ámbito migratorio, la falta de esta medida aumenta los riesgos.

La legislación establece un régimen diferenciado para el ámbito migratorio a través de varias disposiciones clave. El Artículo 49.4 establece que para los sistemas de IA de alto riesgo en las áreas de aplicación de la ley, migración y control fronterizo, el registro se realizará en una sección no pública de la base de datos de la UE. Esto limita considerablemente la transparencia y el escrutinio público de estos sistemas, generando una opacidad institucionalizada que restringe la capacidad de supervisión (una limitación que contrasta con la necesidad de autoridades de vigilancia independientes y con poderes efectivos, como se sugiere en el Cdo. 159; ver Hoofnagle et al., 2019, sobre los desafíos de la supervisión algorítmica). En

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

concreto, el Artículo 49.4 establece que "El registro se realizará en una sección no pública de la base de datos de la UE, accesible únicamente para las autoridades competentes y los organismos notificados".

De manera similar, el Artículo 50 introduce excepciones significativas a los requisitos de transparencia para sistemas utilizados en la prevención, investigación o persecución de delitos, incluyendo los implementadores de sistemas de reconocimiento de emociones o categorización biométrica. Teniendo en cuenta la creciente criminalización de la migración, estas excepciones podrían tener un impacto desproporcionado sobre las personas migrantes. La criminología crítica y los estudios sobre *crimigración* (Stumpf, 2006; De Giorgi, 2010) aportan un marco teórico clave para comprender cómo la implementación de sistemas de IA para la persecución del delito puede afectar a los migrantes, generando efectos adversos sobre su derecho a no ser discriminados y creando un *chilling effect* que limita sus libertades fundamentales.

La tecnificación del control migratorio y la cuestión de la coherencia normativa

El Reglamento de Inteligencia Artificial establece un marco normativo que regula la implementación de diversos sistemas tecnológicos aplicados al control migratorio. Entre estos sistemas se encuentran el perfilado automatizado de personas en función de múltiples variables, la categorización de individuos según criterios de riesgo, el uso de evaluaciones algorítmicas para determinar la probabilidad de que alguien represente una amenaza, y la interoperabilidad entre bases de datos de diferentes organismos estatales y supranacionales (regulada en parte por los Reglamentos (UE) 2019/817 y (UE) 2019/818). Asimismo, esta legislación facilita la incorporación de herramientas de análisis biométrico avanzado, como los sistemas de reconocimiento facial y la detección de emociones, que pueden utilizarse en aeropuertos, pasos fronterizos y otros espacios de control migratorio. Estas tecnologías, aunque presentadas como mecanismos para optimizar la eficiencia y seguridad de la gestión migratoria, generan preocupaciones significativas debido a sus efectos discriminatorios y a las posibles vulneraciones de derechos fundamentales que pueden derivarse de su implementación.

Aquí surge una tensión fundamental respecto a la coherencia con los marcos de interoperabilidad y bases de datos específicas como Eurodac y PNR. Los Reglamentos (UE) 2019/817 y 2019/818 buscan crear un ecosistema de información integrado para mejorar la gestión de fronteras y la seguridad, estableciendo (al menos formalmente) salvaguardias en materia de protección de datos y derechos fundamentales. Sin embargo, el RIA, con sus amplias excepciones para seguridad nacional (Art. 2.3) y las limitaciones a la transparencia para sistemas de IA en migración y aplicación de la ley (Art. 49.4, Art. 50), podría permitir que sistemas de IA operen dentro de esta infraestructura interoperable con

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

un nivel reducido de escrutinio y rendición de cuentas (Beduschi, 2021). Por ejemplo, un sistema de evaluación de riesgos clasificado como de alto riesgo según el Anexo III del RIA, pero cuyos detalles técnicos y evaluación de impacto no son públicamente accesibles, podría alimentarse de datos de Eurodac (Reglamento (UE) 603/2013) o del SIS (integrado en el marco de interoperabilidad) y generar resultados potencialmente discriminatorios sin que exista una supervisión externa efectiva. De manera similar, los sistemas de análisis de datos PNR (Directiva (UE) 2016/681), que ya han sido criticados por su potencial discriminatorio, podrían incorporar herramientas de IA sujetas a las reglas menos estrictas del RIA cuando se aplican en contextos de seguridad o control migratorio. Esta falta de alineación podría socavar los principios de protección de datos y necesidad/proporcionalidad que supuestamente rigen estos sistemas de información a gran escala, creando un escenario donde la eficiencia tecnológica habilitada por la interoperabilidad se prioriza sobre la protección efectiva de los derechos de las personas migrantes (Guild, 2023).

El uso de inteligencia artificial en el control migratorio no es un fenómeno aislado, sino que debe entenderse dentro de un contexto más amplio de vigilancia masiva y *datificación* de la movilidad humana. Para analizar críticamente este fenómeno, recurrimos a los estudios críticos de vigilancia (Lyon, 2019; Dencik et al., 2019), que permiten examinar cómo estas tecnologías refuerzan regímenes de control estatal y producen nuevas formas de exclusión. En este sentido, la noción de capitalismo de vigilancia (Zuboff, 2019) resulta particularmente útil, ya que explica cómo la recopilación masiva de datos sobre los movimientos de las personas no solo responde a objetivos gubernamentales de seguridad, sino que también se vincula con modelos de negocio basados en la explotación de información personal. Este marco conceptual permite situar la expansión de la IA en el control migratorio dentro de un esquema más amplio de gobernanza digital, donde la automatización de la vigilancia se entrelaza con intereses comerciales y estrategias geopolíticas de control territorial.

Además de estos enfoques, el concepto de discriminación algorítmica (Eubanks, 2018) aporta una perspectiva clave para analizar cómo los sistemas de IA pueden reproducir desigualdades preexistentes en la sociedad. A través del uso de datos históricos y criterios de categorización que reflejan sesgos estructurales, estos sistemas pueden generar evaluaciones desproporcionadamente negativas para ciertos grupos de migrantes, especialmente aquellos provenientes de regiones estigmatizadas o sujetos a perfiles raciales específicos. De manera similar, la noción de racismo automatizado (Benjamin, 2019) advierte sobre cómo la automatización de decisiones en contextos de frontera puede reforzar dinámicas de exclusión racial, al operar bajo lógicas que, aunque presentadas como objetivas y neutrales, perpetúan prácticas discriminatorias de larga data. En conjunto, estos marcos teóricos nos permiten problematizar el impacto de la inteligencia artificial en el control

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

migratorio, destacando sus riesgos en términos de justicia social, derechos humanos y acceso equitativo a la movilidad transnacional.

El Artículo 5(1)(d) del RIA autoriza el uso de sistemas de identificación biométrica remota en espacios públicos con fines policiales, siempre que su empleo sea considerado estrictamente necesario. Esta disposición se justifica en tres escenarios específicos: la búsqueda de víctimas potenciales de delitos, lo que podría incluir casos de trata de personas, desapariciones forzadas o explotación laboral; la prevención de una amenaza específica, sustancial e inminente para la vida o seguridad física de las personas, como operativos antiterroristas o respuestas inmediatas a posibles atentados o crímenes violentos; y la detección, localización, identificación o enjuiciamiento de perpetradores o sospechosos de delitos penales, permitiendo a las autoridades el reconocimiento automatizado de individuos que se encuentren en bases de datos policiales o que sean requeridos en investigaciones criminales.

Si bien la ley establece estos límites, su aplicación en el control migratorio suscita preocupaciones importantes, especialmente debido a la posibilidad de que estas herramientas se utilicen de manera desproporcionada y sin garantías suficientes para los derechos fundamentales de las personas migrantes. Los sistemas de reconocimiento biométrico operan mediante la captura y análisis de características físicas únicas de los individuos, tales como huellas dactilares, patrones faciales, iris, voz o incluso la forma de caminar. Estas tecnologías utilizan algoritmos de aprendizaje automático para comparar los datos capturados con bases de datos preexistentes, permitiendo identificar o verificar la identidad de una persona en tiempo real. En el ámbito del control migratorio, se han implementado en aeropuertos, pasos fronterizos y centros de detención con el argumento de mejorar la eficiencia en la gestión de flujos migratorios y reforzar la seguridad.

Sin embargo, el uso de estos sistemas plantea múltiples riesgos, entre ellos la posibilidad de errores en la identificación, sesgos algorítmicos que afectan desproporcionadamente a ciertos grupos raciales o étnicos, y la falta de transparencia en los procesos de recopilación y almacenamiento de datos biométricos. Estudios como los realizados por el Instituto Nacional de Estándares y Tecnología de EE.UU. (NIST) han encontrado que las tasas de falsos positivos (identificar incorrectamente a dos personas diferentes como la misma) pueden ser entre 10 y 100 veces mayores para rostros de personas asiáticas y afroamericanas en comparación con los caucásicos, dependiendo del algoritmo específico utilizado (NIST, 2019). Por su parte, la investigación Gender Shades del MIT (Buolamwini & Gebru, 2018) demostró que sistemas comerciales de clasificación de género tenían tasas de error de hasta el 34% para mujeres de piel oscura, mientras que eran casi perfectos (menos del 1% de error) para hombres de piel clara. Estos hallazgos evidencian que los sistemas de reconocimiento facial tienden a ser menos precisos cuando se aplican

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

a personas *racializadas* y mujeres, aumentando la probabilidad de identificaciones erróneas y potenciales vulneraciones de derechos. Además, el empleo de sistemas biométricos en contextos de movilidad humana refuerza la vigilancia sobre los migrantes, quienes ya se encuentran en una posición de mayor exposición frente a los controles estatales. La interoperabilidad de bases de datos entre distintos países y agencias gubernamentales facilita el seguimiento transnacional de personas en situación de migración, lo que puede derivar en efectos adversos como la criminalización de la movilidad, ya que la vinculación de datos biométricos con antecedentes penales o perfiles de riesgo puede generar una presunción de culpabilidad sobre las personas migrantes, afectando su derecho al debido proceso y a la presunción de inocencia; la exclusión y restricciones en el acceso a servicios, dado que en algunos casos la exigencia de autenticación biométrica se ha extendido a trámites administrativos como la solicitud de asilo o la regularización migratoria, lo que puede dificultar el acceso a derechos básicos; y la falta de mecanismos efectivos de supervisión, ya que la recopilación y uso de datos biométricos por parte de Estados y empresas privadas no siempre está regulada con la debida transparencia, lo que incrementa el riesgo de uso indebido o filtraciones de información sensible.

A pesar de que el RIA establece restricciones formales sobre el uso de estas tecnologías, su implementación en el control migratorio sigue siendo un tema de preocupación, especialmente en lo que respecta a la protección de los derechos de las personas en movimiento y la posible ampliación de regímenes de vigilancia masiva bajo el pretexto de la seguridad fronteriza.

Otro aspecto particularmente preocupante del RIA es la disposición transitoria que permite que los sistemas de IA utilizados en grandes bases de datos de la Unión Europea, como Eurodac (Reglamento (UE) 603/2013), el Sistema de Información de Schengen (SIS) y el Sistema Europeo de Información y Autorización de Viajes (ETIAS), continúen operando hasta 2030 sin cumplir completamente con los nuevos requisitos de protección de datos y transparencia algorítmica. Esta prórroga implica que, a pesar de la adopción de regulaciones más estrictas sobre inteligencia artificial, la UE seguirá utilizando tecnologías de recolección y análisis de datos que fueron diseñadas bajo normativas previas, lo que deja abierta la posibilidad de que se perpetúen prácticas discriminatorias y se consolide un modelo de vigilancia migratoria basado en la automatización del control. La extensión temporal de estas disposiciones, como señala Broeders (2007), refuerza la creación de una "frontera digital" europea, un sistema en el que la exclusión y marginalización de los migrantes no se basa únicamente en barreras físicas o en la normativa migratoria tradicional, sino en el uso de bases de datos interoperables (facilitadas por los Reglamentos (UE) 2019/817 y (UE) 2019/818) que pueden restringir el acceso y la movilidad de ciertos grupos en función de criterios automatizados. Esta falta de aplicación

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

retroactiva inmediata de las salvaguardias del RIA a sistemas ya integrados en la arquitectura de interoperabilidad agudiza las preocupaciones sobre la coherencia normativa y la protección efectiva de derechos (Statewatch, 2023).

Para comprender mejor las implicaciones de esta disposición, es fundamental analizar el concepto de interoperabilidad en el contexto del control migratorio. La interoperabilidad de bases de datos se refiere a la capacidad de diferentes sistemas y plataformas de compartir, cruzar y procesar información de manera integrada, permitiendo que datos biométricos, antecedentes migratorios, historiales de solicitudes de asilo y registros de seguridad puedan ser accesibles en tiempo real por múltiples agencias y Estados. En la Unión Europea, este principio ha sido promovido como una estrategia para reforzar la gestión de fronteras y mejorar la cooperación entre los distintos Estados miembros. La Comisión Europea ha impulsado activamente la interconexión de bases de datos como una forma de optimizar la seguridad, pero esta estrategia plantea serios riesgos en términos de protección de derechos, ya que permite que los datos de las personas migrantes sean utilizados de manera extensiva sin su consentimiento explícito y, en muchos casos, sin mecanismos efectivos de supervisión y control.

Entre los sistemas más relevantes en este entramado interoperable se encuentra Eurodac, una base de datos que almacena huellas dactilares de solicitantes de asilo y migrantes en situación irregular con el propósito de facilitar la aplicación del Reglamento de Dublín, que determina qué Estado miembro es responsable de tramitar una solicitud de protección internacional. Sin embargo, con la creciente automatización del control migratorio, Eurodac ha evolucionado de ser una base de datos de gestión de solicitudes de asilo a un sistema que también puede ser consultado por fuerzas de seguridad y organismos policiales, ampliando su función hacia fines de vigilancia. De manera similar, el Sistema de Información de Schengen (SIS) permite a los Estados miembros intercambiar información sobre personas buscadas, objetos robados y alertas migratorias, lo que refuerza la capacidad de rastreo de personas en movimiento dentro del espacio Schengen. La interoperabilidad entre estas bases de datos y el Sistema Europeo de Información y Autorización de Viajes (ETIAS), que recopilará información previa sobre viajeros exentos de visa antes de su entrada a la UE, amplía significativamente las capacidades de predicción y categorización de individuos, generando una infraestructura de datos que opera como un filtro digital de movilidad.

Uno de los principales problemas de este modelo es que la interoperabilidad no solo facilita el acceso compartido a datos entre distintas agencias, sino que también permite la propagación de errores y sesgos a gran escala. Si un individuo es categorizado erróneamente en una de estas bases de datos, la interconexión de los sistemas puede hacer que esta información se replique automáticamente en otras plataformas, dificultando su

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

corrección y afectando gravemente la vida de la persona implicada. Este fenómeno es particularmente problemático para los migrantes, quienes muchas veces no tienen acceso a mecanismos efectivos para impugnar decisiones automatizadas o corregir información incorrecta en bases de datos estatales. Además, la integración de estos sistemas con tecnologías de inteligencia artificial plantea interrogantes sobre la capacidad de los Estados para garantizar que las decisiones automatizadas no refuercen dinámicas de exclusión y criminalización.

En este sentido, la extensión del uso de estas bases de datos hasta 2030 sin la plena aplicación de los estándares de la nueva legislación sobre inteligencia artificial no solo representa una laguna normativa, sino que también refuerza la dependencia de la UE en un modelo de gobernanza migratoria basado en el uso intensivo de datos biométricos y registros automatizados. Este tipo de infraestructura digital, al estar diseñada bajo lógicas de securitización y prevención de riesgos, tiende a priorizar el control sobre la protección de derechos, lo que agrava la situación de vulnerabilidad de las personas migrantes. La interoperabilidad, en lugar de facilitar la regularización o la protección de quienes buscan asilo, se ha convertido en una herramienta que refuerza la selectividad y exclusión en la gestión de fronteras, consolidando un régimen en el que la movilidad de ciertos grupos está condicionada por evaluaciones algorítmicas y perfiles de riesgo generados a partir de bases de datos automatizadas.

Asimismo, otro eje relevante refiere a los sistemas predictivos y de evaluación de riesgos. El Anexo III del RIA se refiere específicamente a los sistemas de evaluación de riesgos utilizados en el contexto migratorio. Estos sistemas de IA están diseñados para asistir a las autoridades competentes en la evaluación de los riesgos que una persona podría presentar para la seguridad, con el objetivo de determinar el riesgo de entrada o estancia irregular en los Estados miembros. Aunque estos sistemas pretenden ser herramientas de gestión eficientes, su uso puede acentuar la discriminación al basarse en datos que no siempre reflejan una amenaza real, sino patrones de comportamiento previamente establecidos que pueden ser racialmente sesgados.

Los sistemas de evaluación de riesgos y predicción en el control migratorio, regulados en el Anexo III del RIA, representan una de las aplicaciones más controvertidas de la IA en la gestión de fronteras. Estas tecnologías están diseñadas para asistir a las autoridades en la determinación del riesgo que una persona podría representar en términos de seguridad o irregularidad migratoria. Su implementación busca optimizar los procesos de control mediante la automatización del análisis de perfiles y la identificación temprana de posibles amenazas. Sin embargo, el uso de estos sistemas plantea preocupaciones fundamentales, ya que se basan en modelos algorítmicos que, en muchos casos, dependen de conjuntos de datos que pueden estar sesgados, replicando y reforzando patrones discriminatorios preexistentes.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Por otro lado, el Anexo III de la ley clasifica estos sistemas como "alto riesgo", en virtud de su capacidad para influir en decisiones que pueden afectar de manera significativa los derechos y libertades de las personas migrantes. La regulación establece que su implementación debe cumplir con estrictos requisitos de transparencia, explicabilidad y supervisión humana, aunque en la práctica persisten dudas sobre la efectividad de estos mecanismos de control. La recopilación masiva de información sobre ciertas poblaciones migrantes, combinada con la interoperabilidad de bases de datos como Eurodac, el Sistema de Información de Schengen (SIS) y ETIAS, genera un circuito de retroalimentación en el que los mismos perfiles de riesgo se replican constantemente. Un ejemplo de esto es la categorización de ciertos grupos nacionales o étnicos como más propensos a la "migración irregular" en función de datos históricos de detenciones o rechazos en frontera. Dado que las decisiones de control migratorio previas han estado marcadas por prejuicios raciales y nacionalidades específicas han sido desproporcionadamente vigiladas, los sistemas predictivos tienden a perpetuar y amplificar estas tendencias, estableciendo un sesgo estructural en la toma de decisiones automatizada.

El problema central radica en que estos sistemas no operan en un vacío técnico, sino que están condicionados por los datos con los que han sido entrenados. Los algoritmos de evaluación de riesgos se alimentan de bases de datos interoperables, cruzando información de registros biométricos, antecedentes de viajes, historial de solicitudes de asilo y otras fuentes, como redes sociales o información obtenida en entrevistas con autoridades migratorias. A partir de esta información, los modelos de IA asignan puntuaciones de riesgo a individuos o grupos, clasificándolos según su supuesta probabilidad de involucrarse en actividades ilícitas o de permanecer en un país sin autorización. En este sentido, estas tecnologías no solo buscan detectar casos de ingreso irregular, sino que también se utilizan para predecir comportamientos futuros basados en patrones estadísticos, lo que introduce un elemento de pre-criminalización y vigilancia preventiva.

Un caso paradigmático de este problema es el uso de inteligencia artificial en el análisis de perfiles de pasajeros aéreos a través del sistema de Registro de Nombres de Pasajeros (PNR), regulado por la Directiva (UE) 2016/681. Este sistema, utilizado en la UE y otros países, recopila datos de pasajeros antes de su llegada a un territorio determinado para evaluar el riesgo de cada viajero en función de sus patrones de viaje, método de pago del billete o incluso el tipo de equipaje registrado. Si bien se presenta como una herramienta de seguridad, diversos estudios han señalado que su implementación ha llevado a la discriminación de ciertos grupos étnicos y religiosos, reforzando la asociación entre movilidad y sospecha criminal (ver Hayes, 2019). En este contexto, los sistemas de evaluación de riesgos no solo afectan a quienes intentan cruzar fronteras, sino que también impactan la experiencia de viaje y movilidad de poblaciones específicas, generando un trato diferenciado basado en

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

criterios opacos y difíciles de impugnar. La aplicación del RIA a los algoritmos utilizados dentro del sistema PNR podría estar sujeta a las mismas limitaciones de transparencia y excepciones si se consideran dentro del ámbito de la aplicación de la ley o la seguridad, manteniendo la falta de claridad sobre cómo se realizan estas evaluaciones de riesgo.

Además del sesgo algorítmico, otra preocupación clave es la falta de transparencia y mecanismos efectivos de supervisión sobre el uso de estos sistemas. En muchos casos, las personas afectadas no tienen acceso a información clara sobre cómo se generó su perfil de riesgo ni sobre las razones por las que pueden ser sometidas a controles más estrictos o rechazadas en la frontera. La opacidad en el funcionamiento de estos algoritmos limita el derecho a la defensa y al debido proceso, ya que las decisiones automatizadas pueden tener consecuencias directas sobre la vida de las personas migrantes sin posibilidad de apelación efectiva. La falta de explicabilidad de los modelos de IA utilizados en el control migratorio refuerza la asimetría de poder entre los Estados y las personas en movilidad, consolidando un régimen en el que la vigilancia algorítmica actúa como un filtro invisible pero determinante en la gestión fronteriza.

Por otro lado, la interconexión de los sistemas de evaluación de riesgos con bases de datos interoperables plantea interrogantes sobre la durabilidad y reutilización de la información migratoria. En la práctica, una persona clasificada como de alto riesgo por un sistema en particular puede ver replicada esta categorización en múltiples plataformas y en diferentes países, incluso si la información original fue errónea o basada en criterios subjetivos. Esto genera un problema de etiquetado permanente, donde los individuos quedan atrapados en una red de vigilancia digital que condiciona su movilidad a largo plazo. Esta interconexión de datos no solo es utilizada para rechazar solicitudes de ingreso o residencia, sino que también puede afectar procesos administrativos como la obtención de visas, la renovación de documentos o el acceso a servicios esenciales en los países de destino.

En última instancia, la aplicación de sistemas predictivos y de evaluación de riesgos en el control migratorio refuerza un paradigma de seguridad basado en la anticipación y prevención de amenazas, priorizando la vigilancia sobre la protección de derechos fundamentales. A pesar de que el RIA, en su Anexo III, establece la necesidad de garantías y supervisión en el uso de estos sistemas, la realidad es que su implementación en el contexto migratorio está marcada por una lógica de control que se articula con la infraestructura de datos y la interoperabilidad de bases de datos previamente establecidas. Esto no solo perpetúa desigualdades estructurales, sino que también consolida un modelo en el que la movilidad humana es gestionada a través de tecnologías que, lejos de ser neutrales, reflejan dinámicas de exclusión y marginación digitalizadas.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Implicaciones para los derechos fundamentales: la erosión de garantías

La normativa propuesta tiene un impacto directo sobre varios derechos fundamentales protegidos por la Carta de Derechos Fundamentales de la Unión Europea, incluyendo el derecho a la privacidad (Artículo 7), la protección de datos personales (Artículo 8), la no discriminación (Artículo 21) y el derecho de asilo (Artículo 18). Aunque el RIA establece ciertos límites y salvaguardias en el uso de inteligencia artificial (IA) en el ámbito migratorio, las excepciones y exenciones previstas ponen en riesgo la integridad de estos derechos esenciales, permitiendo la erosión progresiva de garantías fundamentales. Esta erosión se ve potenciada por la falta de coherencia con los principios de protección de datos que deberían regir la interoperabilidad de sistemas como Eurodac o SIS, donde el RIA podría legitimar el uso de IA con menores garantías.

El derecho a la privacidad (Artículo 7) es uno de los más afectados por la implementación de sistemas de IA en el control migratorio. La expansión de tecnologías de vigilancia biométrica, perfilado automatizado y monitoreo masivo ha introducido nuevos riesgos en la protección de la intimidad de las personas migrantes. La falta de transparencia y supervisión efectiva en el uso de estas herramientas dificulta que los individuos puedan conocer en qué medida su información está siendo recolectada, almacenada y utilizada por las autoridades. En este sentido, el uso de sistemas de reconocimiento facial en espacios públicos, la vigilancia predictiva y la interconexión de bases de datos migratorias pueden dar lugar a un régimen de control sin precedentes, en el que las personas en movilidad son sometidas a un escrutinio constante sin garantías claras de protección de su privacidad.

Además, la naturaleza de estos sistemas implica que la recopilación de datos biométricos se realice sin consentimiento explícito, en contravención de los principios establecidos en la legislación europea de protección de datos. Las imágenes, huellas dactilares y patrones biométricos de los migrantes pueden ser utilizados para rastrear sus movimientos dentro y fuera de la UE, generando un entorno de vigilancia ubicua que limita su autonomía y refuerza un trato diferencial basado en su estatus migratorio. La implementación de estas tecnologías sin una regulación clara sobre tiempos de retención, acceso a los datos y eliminación de registros, aumenta el riesgo de abuso y uso indebido de la información recopilada.

El principio de no discriminación (Artículo 21), que prohíbe cualquier forma de discriminación basada en origen étnico, religión, nacionalidad o cualquier otra característica protegida, también se ve seriamente amenazado. Los sistemas de perfilado y evaluación de riesgos utilizados en el control migratorio dependen de algoritmos que procesan grandes volúmenes de datos históricos, los cuales reflejan patrones previos de actuación de las autoridades migratorias. Como diversos estudios han señalado (Eubanks, 2018;

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Benjamin, 2019), cuando estos sistemas se basan en datos sesgados, terminan reforzando y amplificando desigualdades estructurales preexistentes.

Por ejemplo, si los registros históricos muestran que ciertas nacionalidades han sido desproporcionadamente sometidas a controles fronterizos más estrictos o a mayores tasas de rechazo de solicitudes de asilo, los algoritmos pueden interpretar estos datos como indicadores de "alto riesgo", perpetuando una discriminación indirecta que afecta desproporcionadamente a ciertos grupos. Este fenómeno no solo normaliza la racialización del control migratorio, sino que también debilita el principio de igualdad ante la ley, convirtiendo la IA en un mecanismo de exclusión digitalizada que restringe la movilidad de poblaciones específicas con base en supuestos riesgos de seguridad.

El derecho a la protección de datos personales (Artículo 8) es otro de los pilares fundamentales que se ven comprometidos por la nueva legislación. La normativa permite excepciones relacionadas con la seguridad nacional y el control fronterizo, las cuales amplían el margen de maniobra de las autoridades para recolectar, procesar y almacenar información personal sin requerir consentimiento explícito de los individuos afectados. Esta disposición plantea un desafío crucial para el modelo europeo de protección de datos, ya que podría socavar principios esenciales como la minimización de datos, la finalidad específica y la limitación en el tiempo de almacenamiento, entrando en tensión con los objetivos de protección de datos de los reglamentos de interoperabilidad (Reg. (UE) 2019/817 y 2019/818).

En la práctica, esto significa que la información biométrica y los datos personales de las personas migrantes pueden ser retenidos y reutilizados de manera indefinida dentro del ecosistema de bases de datos interoperables de la UE. Sistemas como Eurodac, el Sistema de Información de Schengen (SIS) y ETIAS funcionan como repositorios centralizados que permiten el acceso simultáneo a múltiples agencias de seguridad y control fronterizo, lo que aumenta el riesgo de que los datos sean empleados con finalidades distintas a las originalmente previstas. Además, la integración de la IA en estos sistemas puede facilitar la re-identificación y seguimiento de individuos a lo largo del tiempo, afectando su derecho a la privacidad y aumentando su exposición a medidas restrictivas de movilidad.

El derecho de asilo (Artículo 18) también se ve afectado de manera indirecta por la implementación de estas tecnologías. El uso de sistemas de IA en la evaluación de solicitudes de protección internacional puede introducir criterios automatizados de selección que prioricen ciertos perfiles en detrimento de otros, lo que podría dar lugar a rechazos injustificados basados en inferencias algorítmicas. Asimismo, la vigilancia predictiva y el perfilado de riesgos pueden llevar a la criminalización de los solicitantes de asilo, al asociarlos con potenciales amenazas de seguridad sin pruebas concretas que respalden estas acusaciones.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Por otro lado, el uso de IA en la detección de fraudes en solicitudes de protección ha generado preocupaciones adicionales. Existen antecedentes de sistemas de IA que han sido entrenados para identificar supuestas inconsistencias en las narrativas de los solicitantes, lo que puede llevar a la denegación de refugio por motivos arbitrarios. La automatización de estos procesos, combinada con la falta de mecanismos efectivos de supervisión, crea un riesgo de exclusión digital para quienes no logren cumplir con los criterios predefinidos por los algoritmos, sin que puedan presentar pruebas adicionales o recurrir las decisiones de manera efectiva.

En última instancia, la erosión de estas garantías fundamentales genera un modelo de control migratorio cada vez más automatizado y menos transparente, donde las decisiones sobre la vida de las personas en movilidad dependen de sistemas algorítmicos opacos y difíciles de impugnar. A pesar de que la normativa reconoce ciertos riesgos y establece la necesidad de supervisión y auditoría de estos sistemas, las excepciones y lagunas regulatorias abren la puerta a la consolidación de un régimen de vigilancia que puede operar con bajos niveles de rendición de cuentas y escasa supervisión judicial.

Este escenario plantea un desafío crucial para la gobernanza de la inteligencia artificial en la UE: la necesidad de garantizar que la tecnología no solo optimice los procesos administrativos, sino que también respete y proteja los derechos fundamentales de todas las personas, incluidas aquellas en situación de movilidad. Sin medidas correctivas adecuadas, la creciente integración de la IA en la gestión migratoria podría derivar en un paradigma de exclusión digitalizada, donde las personas migrantes enfrentan no solo barreras físicas, sino también muros algorítmicos que limitan su acceso a la protección y su derecho a una movilidad segura y digna.

4. La respuesta de la sociedad civil: el movimiento #ProtectNotSurveil

En el marco de lo que Isin y Ruppert (2015) denominan “actos de ciudadanía digital” como forma de resistencia, la coalición #ProtectNotSurveil, conformada en febrero de 2023, ha sido especialmente crítica respecto a las deficiencias de la legislación en materia de control migratorio y el uso de la IA. Sus principales objeciones se centran en tres aspectos clave: la falta de prohibiciones efectivas para el uso de sistemas perjudiciales en el ámbito migratorio, la exclusión de tecnologías críticas de la categoría de alto riesgo, y la creación de un marco jurídico paralelo que otorga un tratamiento especial a las autoridades migratorias.

Siguiendo la perspectiva crítica de Noble (2018), quien afirma que “los algoritmos no son neutrales; reflejan y amplifican los sesgos existentes en la sociedad”, la coalición ha señalado que los sistemas de IA no solo reflejan, sino que pueden intensificar las desigualdades

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

sociales y raciales preexistentes. Este enfoque ha sido esencial para la argumentación de la sociedad civil contra los aspectos más problemáticos del RIA.

A través de un análisis exhaustivo del contexto migratorio, la coalición ha evidenciado que las prohibiciones impuestas en la legislación no se extienden al ámbito migratorio. Aunque se introducen algunas restricciones limitadas sobre el uso de la IA, los legisladores de la UE se han negado a prohibir sistemas particularmente nocivos, como aquellos utilizados para la evaluación de riesgos discriminatorios en el contexto migratorio o los análisis predictivos aplicados para facilitar las devoluciones forzadas. Además, la prohibición del reconocimiento de emociones non se aplica específicamente al ámbito migratorio, lo que deja fuera casos documentados de uso de tecnologías como los detectores de mentiras basados en IA en las fronteras (PICUM, 2023).

De manera alarmante, la lista de sistemas de alto riesgo excluye una serie de herramientas tecnológicas utilizadas en el control migratorio, las cuales, en última instancia, no estarán sujetas a las regulaciones del presente Reglamento. Entre estos sistemas se incluyen tecnologías como la identificación biométrica remota (más allá de las excepciones permitidas), los escáneres de huellas dactilares y las herramientas predictivas utilizadas para prever, restringir y controlar la migración, dejando expuesto el marco legislativo a la implementación de tecnologías invasivas y potencialmente discriminatorias.

5. Conclusiones

El análisis realizado revela que el Reglamento de Inteligencia Artificial de la Unión Europea, aunque constituye un paso significativo en la regulación de la IA, introduce un régimen asimétrico y excepcional en el ámbito migratorio que podría comprometer de manera estructural los derechos fundamentales de las personas en movilidad. Mientras que en otros sectores la normativa enfatiza la transparencia, la rendición de cuentas y la supervisión independiente, en el control migratorio se observan disposiciones más laxas, justificaciones amplias para el uso de IA con fines securitarios y una arquitectura legal que prioriza la gestión del riesgo sobre la protección de derechos.

Uno de los aspectos más preocupantes es la incorporación de excepciones y exenciones dentro de la legislación, particularmente en lo que respecta a la seguridad nacional y el control fronterizo. Estas disposiciones no solo establecen un marco jurídico paralelo en el que las salvaguardias son significativamente menores, sino que también abren la puerta a una expansión del uso de tecnologías intrusivas sin los niveles de supervisión requeridos en otros ámbitos. La existencia de lagunas normativas, como la autorización de sistemas de identificación biométrica remota sin una regulación específica sobre sus condiciones de uso, refuerza el riesgo de que estas herramientas se conviertan en instrumentos de vigilancia masiva con un impacto desproporcionado sobre las poblaciones migrantes.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Además, la falta de transparencia en los procesos de toma de decisiones algorítmicas introduce un desafío adicional: las personas en movilidad pueden ser sometidas a evaluaciones de riesgo, perfilamiento automatizado y restricciones de acceso al territorio europeo sin contar con mecanismos efectivos de impugnación. En este contexto, la aplicación de IA en la gobernanza migratoria podría dar lugar a un régimen de exclusión digitalizada, donde la movilidad de ciertos grupos se vea restringida por criterios automatizados opacos, sin posibilidad de escrutinio público ni control democrático efectivo.

Otro punto crítico es la prolongación de períodos de transición para los sistemas existentes, lo que permite que tecnologías ya en funcionamiento continúen operando hasta 2030 sin cumplir plenamente con los nuevos requisitos de protección de datos y derechos fundamentales. Este aplazamiento no solo prolonga la vigencia de prácticas discriminatorias, sino que también consolida una infraestructura migratoria basada en la vigilancia tecnológica antes de que se implementen medidas de supervisión y rendición de cuentas adecuadas. Como resultado, en lugar de corregir los abusos previos y garantizar una migración más justa y transparente, el RIA podría terminar legitimando herramientas que ya han sido señaladas por organismos de derechos humanos como problemáticas. La tensión entre la necesidad de regular la IA y la decisión de permitir que sistemas integrados en la infraestructura de interoperabilidad (Reg. 2019/817 y 2019/818) operen bajo reglas antiguas subraya una incoherencia fundamental en el enfoque de la UE.

Frente a este panorama, la sociedad civil y los organismos de derechos humanos jugarán un papel crucial en el monitoreo de la implementación del reglamento y en la promoción de reformas necesarias. Iniciativas como la coalición #ProtectNotSurveil han advertido sobre los riesgos de destinar recursos públicos al desarrollo de tecnologías de vigilancia, en lugar de fortalecer mecanismos de protección para las personas migrantes. En este sentido, es imprescindible un debate público informado sobre los límites éticos y jurídicos de la IA en el control migratorio, así como una exigencia constante de transparencia y supervisión efectiva sobre las herramientas implementadas.

A pesar de los avances regulatorios que representa el RIA, su impacto en el ámbito migratorio pone en evidencia una contradicción fundamental dentro del modelo de gobernanza tecnológica de la UE. Mientras que en otros sectores la normativa se orienta hacia una IA ética y responsable, en el control de fronteras la lógica predominante sigue siendo la de seguridad, contención y riesgo. Esta dualidad no solo naturaliza la vigilancia diferenciada sobre ciertos grupos poblacionales, sino que también refuerza un modelo de gestión de la movilidad basado en la exclusión y la sospecha permanente.

Además, la normativa refuerza una asimetría en la protección de derechos: mientras que las personas dentro del territorio europeo tienen garantizados ciertos principios de privacidad y control sobre el uso de sus datos, las personas migrantes quedan sujetas a

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

mecanismos de control intrusivo y opaco, sin acceso a los mismos niveles de salvaguardias. Este régimen de excepción no solo es problemático desde una perspectiva jurídica, sino que también consolida un sistema de desigualdad estructural, en el que los avances tecnológicos no se distribuyen de manera equitativa, sino que se convierten en instrumentos de exclusión y control para poblaciones ya vulnerabilizadas.

En este sentido, el RIA no solo institucionaliza un régimen de vigilancia algorítmica, sino que también podría profundizar dinámicas preexistentes de discriminación y securitización en el control migratorio. Lejos de limitar el uso potencialmente nocivo de la IA, la normativa podría servir para sofisticar prácticas de exclusión que ya han sido denunciadas en el pasado. La creciente integración de tecnologías de perfilado, predicción de riesgos y reconocimiento biométrico en las fronteras refuerza un paradigma en el que las personas migrantes no son tratadas como sujetos de derecho, sino como objetos de gestión securitaria.

En última instancia, este análisis subraya la urgente necesidad de repensar la regulación de la inteligencia artificial desde una perspectiva genuinamente universal de derechos humanos. La gobernanza tecnológica no puede seguir operando bajo un esquema de doble estándar, donde ciertas poblaciones gozan de mayor protección mientras que otras son sometidas a tecnologías invasivas sin garantías efectivas. La implementación de IA en el ámbito migratorio debe someterse a los mismos estándares de transparencia, supervisión y control democrático que rigen en otros sectores, evitando la consolidación de un régimen de vigilancia permanente que, bajo la justificación de la seguridad, erosione los derechos fundamentales de las personas en movilidad.

Fuentes

- Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de la Unión Europea, C 326/391. https://www.europarl.europa.eu/charter/pdf/text_es.pdf.
- Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Artificial). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689.

- Reglamento (UE) 2019/817 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de las fronteras y los visados y por el que se modifican los Reglamentos (CE) n.° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 y (UE) 2018/1861 del Parlamento Europeo y del Consejo y las Decisiones 2004/512/CE y 2008/633/JAI del Consejo.
- Reglamento (UE) 2019/818 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, por el que se establece un marco para la interoperabilidad de los sistemas de información de la UE en el ámbito de la cooperación policial y judicial, el asilo y la migración y por el que se modifican los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816.
- Reglamento (UE) nº 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n° 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n° 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

Referencias

Access Now. (2023). *EU AI Act: Migration*. [Policy Brief]. https://www.accessnow.org/publication/eu-ai-act-migration/

Beduschi, A. (2021). International migration management in the age of artificial intelligence. *Migration Studies*, *9*(3), 1296-1317. https://doi.org/10.1093/migration/mnab006

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press.

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives*, *27*(1_suppl), 63-92. https://doi.org/10.1177/03043754020270S105

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Broeders, D. (2007). The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants. *International Sociology*, *22*(1), 71-92. https://doi.org/10.1177/0268580907070126

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, *81*, 1–15. http://proceedings.mlr.press/v81/buolamwini18a.html

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

De Giorgi, A. (2010). Immigration control, post-Fordism, and less eligibility: A materialist critique of the criminalization of immigration across Europe. *Punishment & Society*, *12*(2), 147-167. https://doi.org/10.1177/1462474509357378

Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring Data Justice: Conceptions, Applications and Directions. *Information, Communication & Society*, *22*(7), 873-881. https://doi.org/10.1080/1369118X.2018.1551423

EDRi (European Digital Rights). (2023). *National security exemption in the AI Act: A free pass for rights violations?* https://edri.org/our-work/national-security-exemption-in-the-ai-act-a-free-pass-for-rights-violations/

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Guild, E. (2023). *The EU's AI Act and its consequences for the Area of Freedom, Security and Justice*. CEPS Policy Brief. https://www.ceps.eu/ceps-publications/the-eus-ai-act-and-its-consequences-for-the-area-of-freedom-security-and-justice/

Hayes, B. (2019). *Automated suspicion: The EU's new travel surveillance initiatives*. Statewatch Analysis. https://www.statewatch.org/analyses/no-338-automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Isin, E., & Ruppert, E. (2015). *Being Digital Citizens*. Rowman & Littlefield International.

Lyon, D. (2019). Surveillance Capitalism, Surveillance Culture and Data Politics. En D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data Politics: Worlds, Subjects, Rights*. Routledge.

Molnar, P., & Gill, L. (2022). *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*. Citizen Lab Research Report No. 142. https://citizenlab.ca/2022/09/bots-at-the-gate-a-human-rights-analysis-of-automated-decision-making-in-canadas-immigration-and-refugee-system/

NIST (National Institute of Standards and Technology). (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NISTIR 8280. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

PICUM (Platform for International Cooperation on Undocumented Migrants). (2023). *PICUM's recommendations on the EU AI Act*. https://picum.org/resource/picums-recommendations-on-the-eu-ai-act/

Ryan, M., & Leufer, K. (2023). *The EU AI Act's high-risk classification: Is it fit for purpose?* Computer Law & Security Review, 50, 105853. https://doi.org/10.1016/j.clsr.2023.105853

Smuha, N. A., Ahmed-Ghosh, H., Aleksandrova, A., Cobbe, J., Demetis, D. S., Fanni, R., ... & Veale, M. (2021). *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3899991

Statewatch. (2023). *EU: Artificial Intelligence Act risks embedding discrimination and surveillance*. https://www.statewatch.org/news/2023/december/eu-artificial-intelligence-act-risks-embedding-discrimination-and-surveillance/

Stumpf, J. (2006). The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power. *American University Law Review*, *56*(2), 367-419. https://digitalcommons.wcl.american.edu/aulr/vol56/iss2/3/

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97-112. https://doi.org/10.9785/cri-2021-220402

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.

Revista Científica de la Facultad de Derecho y Ciencias Sociales y Políticas - UNNE, Vol. 4. Núm.1, 2025. E-ISSN 2953-4232
DOI: https://doi.org/10.30972/rcd.418114 - CC BY-NC