



Freedom, Security & Justice:
European Legal Studies

Rivista giuridica di classe A

2026, n. 2

EDITORIALE
SCIENTIFICA



DIRETTRICE

Angela Di Stasi

Ordinario di Diritto Internazionale e di Diritto dell'Unione europea, Università di Salerno
Titolare della Cattedra Jean Monnet 2017-2020 (Commissione europea)
"Judicial Protection of Fundamental Rights in the European Area of Freedom, Security and Justice"

CONSIGLIO SCIENTIFICO

Giandonato Caggiano, Ordinario f.r. di Diritto dell'Unione europea, Università Roma Tre
Sergio Maria Carbone, Professore Emerito, Università di Genova
Roberta Clerici, Ordinario f.r. di Diritto Internazionale privato, Università di Milano †
Nigel Lowe, Professor Emeritus, University of Cardiff
Paolo Mengozzi, Professore Emerito, Università "Alma Mater Studiorum" di Bologna - già Avvocato generale presso la Corte di giustizia dell'UE
Massimo Panebianco, Professore Emerito, Università di Salerno
Nicoletta Parisi, Ordinario f.r. di Diritto Internazionale, Università di Catania - già Componente ANAC
Guido Raimondi, già Presidente della Corte EDU - già Presidente di Sezione della Corte di Cassazione
Silvana Sciarra, Professore Emerito, Università di Firenze - Presidente Emerito della Corte Costituzionale
Giuseppe Tesaro, Professore f.r. di Diritto dell'UE, Università di Napoli "Federico II" - Presidente Emerito della Corte Costituzionale †
Antonio Tizzano, Professore Emerito, Università di Roma "La Sapienza" - Vice Presidente Emerito della Corte di giustizia dell'UE
Ennio Triggiani, Professore Emerito, Università di Bari †
Ugo Villani, Professore Emerito, Università di Bari

COMITATO EDITORIALE

Maria Caterina Baruffi, Ordinario di Diritto Internazionale, Università di Bergamo
Alfonso-Luis Calvo Caravaca, Catedrático Jubilado de Derecho Internacional Privado, Universidad Carlos III de Madrid
Ida Caracciolo, Ordinario di Diritto Internazionale, Università della Campania - Giudice dell'ITLOS
Pablo Antonio Fernández-Sánchez, Profesor Emérito de Derecho Internacional, Universidad de Sevilla
Inge Govaere, Director of the European Legal Studies Department, College of Europe, Bruges
Paola Mori, Ordinario f.r. di Diritto dell'Unione europea, Università "Magna Graecia" di Catanzaro
Lina Panella, Ordinario f.r. di Diritto Internazionale, Università di Messina
Lucia Serena Rossi, Ordinario di Diritto dell'UE, Università "Alma Mater Studiorum" di Bologna - già Giudice della Corte di giustizia dell'UE



COMITATO DEI REFEREES

Bruno Barel, Associato f.r. di Diritto dell'Unione europea, Università di Padova **Marco Benvenuti**, Ordinario di Istituzioni di Diritto pubblico, Università di Roma "La Sapienza"
Fiammetta Borgia, Ordinario di Diritto Internazionale, Università di Roma "Tor Vergata" **Francesco Buonomenna**, Associato di Diritto dell'Unione europea, Università di Salerno
Raffaele Cadin, Ordinario di Diritto Internazionale, Università di Roma "La Sapienza" **Ruggiero Cafari Panico**, Ordinario f.r. di Diritto dell'Unione europea, Università di Milano
Federico Casolari, Ordinario di Diritto dell'Unione europea, Università "Alma Mater Studiorum" di Bologna **Luisa Cassetti**, Ordinario di Istituzioni di Diritto Pubblico, Università di Perugia
Anna Cavaliere, Associato di Filosofia del diritto, Università di Salerno **Giovanni Cellamare**, Ordinario f.r. di Diritto Internazionale, Università di Bari
Giuseppe D'Angelo, Ordinario di Diritto e religione, Università di Salerno **Sara De Vido**, Ordinario di Diritto Internazionale, Università Ca' Foscari Venezia **Valeria Di Comite**, Ordinario di Diritto dell'Unione europea, Università di Bari "Aldo Moro" **Marcello Di Filippo**, Ordinario di Diritto Internazionale, Università di Pisa
Carmela Elefante, Associato di Diritto e religione, Università di Salerno **Rosario Espinosa Calabuig**, Catedrático de Derecho Internacional Privado, Universitat de València **Valentina Faggiani**, Professoressa Titular de Derecho Constitucional, Universidad de Granada
Caterina Fratea, Associato di Diritto dell'Unione europea, Università di Verona **Ana C. Gallego Hernández**, Profesora Ayudante de Derecho Internacional Público y Relaciones Internacionales, Universidad de Sevilla
Pietro Gargiulo, Ordinario f.r. di Diritto Internazionale, Università di Teramo
Francesca Graziani, Associato di Diritto Internazionale, Università della Campania "Luigi Vanvitelli" **Giancarlo Guarino**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Elsbeth Guild**, Associate Senior Research Fellow, CEPS **Victor Luis Gutiérrez Castillo**, Profesor de Derecho Internacional Público, Universidad de Jaén
Ivan Ingravalle, Ordinario di Diritto Internazionale, Università di Bari **Paola Ivaldi**, Ordinario di Diritto Internazionale, Università di Genova **Luigi Kalb**, Ordinario f.r. di Procedura Penale, Università di Salerno
Gianfranco Liace, Associato di Diritto dell'economia, Università di Salerno **Luisa Marin**, Ricercatore di Diritto dell'UE, Università dell'Insubria **Simone Marini**, Associato di Diritto dell'Unione europea, Università di Pisa **Fabrizio Marongiu Buonaiuti**, Ordinario di Diritto Internazionale, Università di Macerata **Rostane Medhi**, Professeur de Droit Public, Université d'Aix-Marseille
Michele Messina, Ordinario di Diritto dell'Unione europea, Università di Messina-Esperto Giuridico presso la Rappresentanza Permanente d'Italia a Bruxelles **Stefano Montaldo**, Associato di Diritto dell'Unione europea, Università di Torino **Violeta Moreno-Lax**, Senior Lecturer in Law, Queen Mary University of London
Claudia Morviducci, Professore Senior di Diritto dell'Unione europea, Università Roma Tre **Michele Nino**, Ordinario di Diritto Internazionale, Università di Salerno
Criseide Novi, Ordinario di Diritto dell'Unione europea, Università di Foggia **Anna Oriolo**, Associato di Diritto Internazionale, Università di Salerno **Leonardo Pasquali**, Ordinario di Diritto internazionale, Università di Pisa **Piero Pennetta**, Ordinario f.r. di Diritto Internazionale, Università di Salerno **Francesca Perrini**, Associato di Diritto Internazionale, Università di Messina
Gisella Pignataro, Associato di Diritto privato comparato, Università di Salerno **Emanuela Pistoia**, Ordinario di Diritto dell'Unione europea, Università di Teramo
Anna Pitrone, Associato di Diritto dell'Unione europea, Università di Messina **Concetta Maria Pontecorvo**, Ordinario di Diritto Internazionale, Università di Napoli "Federico II" **Pietro Pustorino**, Ordinario di Diritto Internazionale, Università LUISS di Roma **Santiago Ripol Carulla**, Catedrático de Derecho internacional público, Universitat Pompeu Fabra Barcelona
Angela Maria Romito, Associato di Diritto dell'Unione europea, Università di Bari **Gianpaolo Maria Ruotolo**, Ordinario di Diritto Internazionale, Università di Foggia
Teresa Russo, Associato di Diritto dell'Unione europea, Università di Salerno **Alessandra A. Souza Silveira**, Diretora do Centro de Estudos em Direito da UE, Universidade do Minho
Ángel Tinoco Pastrana, Profesor de Derecho Procesal, Universidad de Sevilla **Sara Tonolo**, Ordinario di Diritto Internazionale, Università degli Studi di Padova
Chiara Enrica Tuo, Ordinario di Diritto dell'Unione europea, Università di Genova **Talitha Vassalli di Dachenhausen**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Alessandra Viviani**, Ordinario di Diritto Internazionale, Università di Siena **Valentina Zambrano**, Associato di Diritto Internazionale, Università di Roma "La Sapienza" **Alessandra Zanobetti**, Ordinario f.r. di Diritto Internazionale, Università "Alma Mater Studiorum" di Bologna

COMITATO DI REDAZIONE

Angela Festa, Docente incaricato di Diritto dell'Unione europea, Università della Campania "Luigi Vanvitelli"
Anna Iermano, Associato di Diritto Internazionale, Università di Salerno
Daniela Marrani, Associato di Diritto Internazionale, Università di Salerno
Rossana Palladino (Coordinatore), Associato di Diritto dell'Unione europea, Università di Salerno

Revisione linguistica degli abstracts a cura di

Francesco Campofreda, Dottore di ricerca in Diritto Internazionale, Università di Salerno





Indice-Sommario 2026, n. 2

Editoriale

La riforma della legislazione sulla cittadinanza tra Corte costituzionale e Corte di giustizia dell'Unione europea p. 1
Bruno Barel

Saggi, Articoli e Commenti

Free movement of persons in the agreement between the EU and the United Kingdom in respect of Gibraltar. Special status of military personnel p. 21
Pablo Antonio Fernández Sánchez

Storia diplomatica: Italia-Europa-Occidente p. 44
Massimo Panebianco

¿Hacia un modelo de Estado híbrido? Entre *court-packing* e intentos de revertir la *backsliding* p. 53
Valentina Faggiani

Vulnerabilità digitale del minore e forme di tutela nel contesto europeo p. 93
Gisella Pignataro

The case law of the European Court of Human Rights regarding contested territories: “Differentiated” jurisdiction as a panacea or as an Achilles’s heel? p. 120
Elisa Ruozzi

The EU legal framework on social security for migrants: A comparative assessment of national practices p. 139
Paolo Iafrate

Il danno ambientale sistemico e la soglia di gravità: tra qualificazione giuridica e tutela giurisdizionale p. 163
Adelaide Francesca Daniela Luminari



FOCUS

The EU as a Global Security Provider: Countering Transnational Crime and New Cooperation Architectures

Collected Papers of the Jean Monnet Module (2023-2026) Transnational Crime & EU Law: Towards Global Action against Cross-border Threats to Common Security, Rule of Law and Human Rights (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo)

Presentazione del Focus/Focus Overview
Anna Oriolo

p. 185

Parte I

Contrasto alla criminalità transnazionale e minacce globali/Countering Transnational Crime and Global Threats

Traffico illecito di armi via mare, criminalità transnazionale e sicurezza globale: verso un nuovo paradigma di legalità universale
Anna Oriolo

p. 191

The tragedy of the global commons in the age of artificial intelligence: Illegal mining, transnational crime, and the future of EU global enforcement
David Schultz

p. 216

The European legal framework on the return of cultural objects: An effective tool to foster civil and administrative cooperation between EU Member States?
Fulvia Staiano

p. 241

Il ruolo degli Stati nella prevenzione e nella repressione degli illeciti contro il patrimonio culturale subacqueo: obiettivi e strumenti comuni tra la Convenzione UNESCO del 2001 e le politiche dell'Unione europea
Patrizia Vigni

p. 257

Parte II

Nuove architetture di cooperazione e strumenti di contrasto dell'Unione europea/New Cooperation Architectures and Enforcement Tools of the European Union

Il principio di fiducia reciproca nella cooperazione giudiziaria penale a dieci anni dal caso *Aranyosi*. Alcune considerazioni sull'attualità del “doppio test” alla luce della sentenza *Commissione c. Ungheria (Valeurs de l'Union)*
Angela Festa

p. 281

Intelligence, diritti umani e sicurezza: criticità e prospettive in ambito internazionale ed europeo
Francesco Focillo

p. 312



War-crimes investigations: New technologies, new complexities, new vulnerabilities. A strategic shortfall or evolutionary opportunity for NATO p. 334
Luigi Bramati

AI tools for combating transnational crime within the EU p. 345
Roxana Matefi

Parte III

Responsabilità e giustizia penale/Accountability and Criminal Justice

Luci e ombre (soprattutto) occidentali sul consolidamento della giustizia penale internazionale p. 355
Paolo Bargiacchi

The EU's cross-border cybercrime enforcement and the limits of extraterritorial jurisdiction p. 388
Heybatollah Najandimanesh

La vittima di tratta al centro della sicurezza in Europa tra standard CEDU e nuove sfide nell'era digitale p. 410
Anna Iermano

La regolamentazione delle catene di approvvigionamento in Europa come strumento per combattere la criminalità: dall'opposizione alla convergenza dei modelli francese e italiano p. 442
Virginie Mercier

La responsabilità penale degli enti creditizi nella gestione delle misure restrittive UE: tra obblighi di garanzia e nuove fattispecie sovranazionali di incriminazione p. 453
Carmine Renzulli

Parte IV

Diritti umani e minacce transfrontaliere/Human Rights and Cross-Border Threats

La *transnational repression* quale minaccia “rinnovata” a diritti umani e sicurezza: la necessità di una risposta mirata da parte dell'Unione europea p. 465
Stefano Busillo

Children pornography, online sextorsion, revenge porn: the provisions of Greek penal code and the EU regulatory developments p. 507
Georgios Nouskalis

Intelligenza artificiale e “fenomeno religioso” nel prisma dei diritti umani p. 518
Daniela Marrani

Postfazione/Afterword p. 539
Angela Di Stasi

Appendice p. 541
EU-GLOBACT Policy Recommendations and Guidelines
Francesco Focillo, Emanuele Sorgente

AI TOOLS FOR COMBATING TRANSNATIONAL CRIME WITHIN THE EU

Roxana Matefi *

SUMMARY: 1. Introduction. – 2. General Considerations Regarding the EU Legal Framework Laying Down Harmonised Rules on AI. – 3. AI Systems Used in the Fight Against Transnational Crimes. – 3.1. Biometric Identification AI Systems. – 3.2. Migration, Asylum or Border Control Management AI Systems. – 3.3. Risk Assessment AI Systems. – 3.4. The SyRI case. – 4. Conclusions.

1. Introduction

In the age of digitalization, new technologies, and artificial intelligence crime, in general, and transnational crime, in particular, is taking on new dimensions in terms of how it operates - with its methods constantly evolving and becoming more sophisticated. “The intricacy and extent of international crime are exacerbated by technological, communicative, and transportation improvements, enabling criminal networks to function more clandestinely and effectively than before. These networks use regulatory gaps, variations in legal systems, and jurisdictional constraints to elude apprehension, rendering it exceptionally challenging for law enforcement organizations to maintain effectiveness”.¹

As new methods of criminal activity emerge, the means of combating them must also be adapted and refined in line with the new and innovative technological advances.

Human and drug trafficking, money laundering, cybercrime, arms trafficking or terrorism financing are just a few examples of crimes that have become increasingly prevalent in recent years due to technological advances and whose methods have become increasingly sophisticated, posing serious challenges in terms of detection, investigation, and prosecution.

Due to the capacity of the AI systems to improve prediction, optimize operations, allocate resources, personalize digital solutions, process great amount of data, detect hidden patterns, the use of artificial intelligence can provide huge advantages in various areas, including security and justice.

* Associate Professor, Faculty of Law, Transilvania University of Braşov. E-mail: roxana.matefi@unitbv.ro.

¹ F.O. JEJELOLA, *The Role of Artificial Intelligence in the Eradication of Transnational Crime*. *International Journal of Research and Innovation in Social Science*, in *International Journal of Research and Innovation in Social Science (Ijriiss)*, 2024, no. 11.

Artificial intelligence is thus increasingly becoming an effective, powerful and transformative² tool that can be used efficiently to combat transnational crime at the EU level and worldwide.

AI practices like biometric identification (facial recognition, voice recognition, integrating AI into fingerprints, iris scan, gait analysis, etc.) or risk assessments of natural persons used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity are increasingly being integrated into judicial proceedings, which plays a significant role in enhancing the ability to address security challenges that EU countries face.

Besides the undeniable advantages of using AI in the field of justice and security, we cannot overlook the risks associated with its use towards public fundamental rights, being aware of its potential to cause material or immaterial harm. As the Executive Director of Europol (European Union Agency for Law Enforcement Cooperation) mentioned in the foreword of the Europol Innovation Lab observatory 2023 report, “it is imperative that we navigate these advancements with a strategic approach, balancing innovation with the ethical implications and societal impact”.³

Taking into account both the benefits and the risks associated with the use of artificial intelligence, we aim to analyze the new technological opportunities offered by AI while dealing with transnational crimes and the ways of combating it, without losing sight of the risks associated with the use of these systems and their potential to infringe upon fundamental rights.

2. General Considerations Regarding the EU Legal Framework Laying Down Harmonised Rules on AI

Since Artificial Intelligence “has emerged as a fascinating and influential force in today’s technological (...) world”⁴ with implications in almost all the domains, including criminal justice where AI “has become a pivotal instrument (...) in recent years”,⁵ the adoption of a comprehensive, uniform AI regulation at the EU level was crucial.

In this context, in 2024 was adopted the Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU)

² *Ibid.*

³ Europol (European Union Agency for Law Enforcement Cooperation), *Innovation Lab The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement - An Observatory Report from the Europol*, Luxembourg, 2023, https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Observatory_Report%20-%20The%20Second%20Quantum%20Revolution.pdf.

⁴ G. PAVLIDIS, *Unlocking the Black Box: Analysing the EU Artificial Intelligence Act’s Framework for Explainability in AI*, in *Law Innovation and Technology*, 2024, no. 1.

⁵ M. KARAYIGIT, D. CELIKKAYA, *The Use of AI in Criminal Justice: Unpacking the EU’s Human-Centric AI Strategy*, in *Nordic Journal of European Law*, 2025, no. 1.

2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, also known as Artificial Intelligence Act.

As emphasized at the very beginning of the AI ACT, in its preamble, the main purpose of the Regulation is to develop “a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the ‘Charter’), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation”.⁶

We need to admit from the very beginning the difficulty of proving a comprehensive definition for artificial intelligence, despite all the efforts made over the years, some of the definitions compounding “a broader understanding of AI, (while) others consider only certain technologies to be AI”.⁷ Acknowledging this difficulty in defining AI, the EU Regulation refers to AI system as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.⁸

In this context it is worth noting that in 2025 the European Commission published guidelines on AI systems definition to facilitate the first AI Act’s rules application, provided that the guidelines are not binding, being designed to evolve over time and to be updated when needed.⁹

The recently adopted European Regulation is meant to provide the framework for the use of AI systems in accordance with fundamental human rights and with the values of the European Union. The approach taken by the European Union was that of “placing humans at the heart of AI and prioritizing human needs and wellbeing accordingly sets the EU AI strategy apart from those of other countries with the capacity to offer valuable global lessons in terms of the use of AI in the criminal justice system”.¹⁰

⁶ Regulation (EU) 2024/1689 of the European Parliament and of the Council, *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*, of 13 June 2024, Recital 1, in OJ L, 2024/1689, 12 July 2024.

⁷ FRA (European Union Agency for Fundamental Rights), *Assessing High-Risk Artificial Intelligence Fundamental Rights Risks*, Vienna, 2025, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf.

⁸ Regulation (EU) 2024/1689, cit., art. 3(1).

⁹ European Commission, *The Commission Publishes Guidelines on AI System Definition to Facilitate the First AI Act’s Rules Application*, 6 February 2025, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>.

¹⁰ *Ibid.*

“By prioritising human oversight, the EU stands as a guardian against the de-humanisation, de-subjection, de-individualisation of justice or legal reasoning absent justice and underscores the importance of keeping human judgment at the core of AI systems, especially those designated as high-risk”.¹¹

While being described as “a fast-evolving family of technologies that contributes to a wide array of benefits”,¹² AI has also the potential of generating consistent risks and harm towards fundamental human rights and public interests, based on circumstances related to its application, use or technological development.

One of the most important provisions introduced by the AI Act is the classification of AI systems based on the level of risk they pose to fundamental rights, the Regulation providing an ample leeway for systems posing an unacceptable level of risk as well as for those posing a high level of risk towards human rights. The EU Regulation makes an important step forward by prohibiting unacceptable AI practices, while also establishing strict requirements for high-risk AI practices as well as important transparency obligations.

The need to deal with the risks those systems pose on fundamental rights is also emphasized by the State of the Digital Decade Eurobarometer 2025 presenting the European citizens’ opinion on some essential aspects concerning the digital transformation in the 27 EU Member States which shows that 83% of Europeans consider important the shaping of the development of Artificial Intelligence and new digital technologies to ensure respect for individuals rights and values.¹³

According to the same survey, only 44% of the Europeans appreciate that EU protects their rights in the digital environment, *totally well*.¹⁴

3. AI Systems Used in the Fight Against Transnational Crimes

As far as AI systems used in the fight against transnational crime are concerned, most fall under the category of exceptions (subject to extremely strict conditions) to systems that pose an unacceptable risk to fundamental rights or are classified as posing a high risk to fundamental rights, as regulated by the AI Act.

Therefore, they must be used with great caution and only for the purpose for which they are intended.

3.1. Biometric Identification AI Systems

Some of the most widely used technologies of this kind are those that involve biometric identification. Though, biometrics as a concept and tool are not novel, with the

¹¹ *Ibid.*

¹² Regulation (EU) 2024/1689, cit.

¹³ European Union, *The Digital Decade 2025*, <https://europa.eu/eurobarometer/surveys/detail/3362>.

¹⁴ *Ibid.*

history of biometrics going back for centuries. “Early” biometrics, such as fingerprints or identification based on photographs, have been used by public authorities since the 19th century”.¹⁵ The novelty comes with the combination of biometrics and Artificial Intelligence, which has the potential of generating a considerable impact when dealing with preventing and combating transnational crimes.

As stated in a Europol report on the impact of quantum computing and quantum technologies on law enforcement released in 2023, “in this rapidly evolving landscape, computer vision and biometrics have emerged as game-changers for law enforcement, both from prevention and investigation standpoints. Effectively (...) coupled with biometric techniques that utilise the unique physiological traits of individuals, these technologies promise a new frontier in policing. The fusion of biometrics and AI can deliver a blend of efficiency and accuracy, offering in-depth insights to swiftly and effectively identify criminals while at the same time protecting the privacy of non-relevant individuals”.¹⁶

As defined by the Artificial Intelligence Act, the notion of ‘biometric identification’ refers to “the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual’s identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not”.¹⁷

The notion does not apply to “AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.”

According to Article 5 (1), par. H from the AI Act, one of the AI practices that shall be prohibited is “the use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement”.

As an exception to this prohibition, the use of the above mentioned systems is permitted if such use is strictly necessary for one of the following objectives: “ (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack; (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or

¹⁵ K. HUSZTI-ORBÁN, F. NÍ AOLÁIN, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*, Minneapolis, 2020, <https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf>.

¹⁶ Europol, *Innovation Lab The Second Quantum Revolution: The Impact of Quantum Computing and Quantum Technologies on Law Enforcement - An Observatory Report from the Europol*, cit.

¹⁷ Regulation (EU) 2024/1689, cit.

executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.”

According to Annex II, the criminal offences referred to above are the following: terrorism, trafficking in human beings, sexual exploitation of children, and child pornography, illicit trafficking in narcotic drugs or psychotropic substances, illicit trafficking in weapons, munitions or explosives, murder, grievous bodily injury, illicit trade in human organs or tissue, illicit trafficking in nuclear or radioactive materials, kidnapping, illegal restraint or hostage-taking, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft or ships, rape, environmental crime, organised or armed robbery, sabotage, participation in a criminal organisation involved in one or more of these offences.

As stipulated by para. (32) from the AI ACT, “the use of AI systems for ‘real-time’ remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights.”

Consequently, the use of these systems will be permitted only “in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years and as they are defined in the law of that Member State”.¹⁸

As previously noticed, the use of such biometric systems is likely to prejudice, especially the right to private life and freedom of assembly but are not limited to these. The constant feeling of surveillance has the potential to generate fear and restrain the individual from expressing themselves freely.

That is why the European Regulation limits the use of these systems to specific, expressly regulated situations, that serve a substantial public interest, coupled with the fact that the benefits of using these systems must outweigh the risks.

3.2. Migration, Asylum or Border Control Management AI Systems

AI systems used in migration, asylum and border control management are another important tool in the fight against transnational crimes. However, they must be used with caution, given the high risk they pose to fundamental rights.

¹⁸ *Ibid.*

Annex III of the AI Regulation refers to the following systems in this category, classifying them as high-risk:

- AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies as polygraphs or similar tools;
- AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State;
- AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence;
- AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, except for the verification of travel documents.

As is also noted in the legal literature, “the use of these technologies raises a plethora of human rights questions”,¹⁹ especially because those affected by such systems are the immigrants and persons seeking for asylum that are “a particularly vulnerable group with few easily accessible avenues to contest unfair practices”.²⁰

Given the heightened risk these systems pose to individuals’ fundamental rights, especially those persons that find themselves in a position of vulnerability, being dependent on the outcome of the actions of the competent authorities, as emphasized by the European Regulation, it is essential that these systems comply with transparency requirements, ensuring at the same time accuracy and non-discrimination of the decision-making process. These requirements play a key role in ensuring viable safeguards for compliance with fundamental human rights, especially the right to non-discrimination, free movement, protection of private life, protection of personal data, international protection, etc.

In accordance with the EU AI Act, those artificial intelligence systems that are used in the area of migration, asylum and border control management need to respect the requirements indicated by the Regulation (EC) No 810/2009 of the European Parliament and of the Council, the Directive 2013/32/EU of the European Parliament and of the Council, as well as other relevant Union law.

The regulation also prohibits the use of these systems to circumvent the Member States or EU institutions, bodies, offices or agencies’ international obligations under the UN Convention relating to the Status of Refugees done at Geneva on 28 July 1951 as

¹⁹ L. NALBANDIAN, *An Eye for an ‘I’: A Critical Assessment of Artificial Intelligence Tools in Migration and Asylum Management*, in *Comparative Migration Studies*, 2022, no. 32, p. 10.

²⁰ *Ibid.*

amended by the Protocol of 31 January 1967, to infringe on the principle of non-refoulement, or to deny safe and effective legal avenues into the territory of the Union, including the right to international protection.

The need for solid legal safeguards is clear with migration becoming increasingly “a transaction requiring migrants to exchange biometric and biographic data for access to resources or a jurisdiction. This transaction can be viewed as one where the migrant trades parts of their physical identity to be viewed as a person: an eye for an ‘I’.”²¹ This metaphorical expression is highly evocative in the context of these systems, which can have a deeply intrusive effect on every aspect of the human personality, with all its many facets.

3.3. Risk Assessment AI Systems

Another category of AI systems that can be effective in detecting and combating transnational crime is that used to assess the likelihood of a person committing a crime.

While the AI ACT expressly prohibits the “use of use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics”, the prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity”.²²

When dealing with AI systems meant to predict the risk of a natural person of committing a crime, the EU Regulation on AI emphasizes that the presumption of innocence requires that the natural person should not be judged on AI-predicted behavior which is based only on their profiling, personality traits or characteristics, like nationality, place of birth, place of residence, etc., if there is not a reasonable suspicion that the person in question was involved in a criminal activity. Suspicion needs to be based on facts which are objectively verifiable and a human assessment is also required.

The prohibition of carrying out risk assessments of natural persons based only on profiling them does not apply to those AI systems that use risk analytics in order to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes.²³

3.4. The SyRI case

In this context of analyzing risk assessment AI systems, it is worth taking a quick look into the Syri case, which involved a Dutch AI system known as *Systeem Risico*

²¹ *Ibid.*

²² Regulation (EU) 2024/1689, cit., art. 5(1)(d).

²³ Regulation (EU) 2024/1689, cit.

Indicatie, a predictive policing AI instrument designed to identify individuals with allegedly high fraud risk, based on the information gathered from various authorities, like tax authorities or those dealing with unemployment policies.

On February 5, 2020, the District Court of The Hague ruled on the SyRI case, concluding that SyRI violates human rights. The solution came as a result of a lawsuit that had been filed against the state by a coalition consisting of NGOs, the largest Dutch trade union and two citizens claiming the mass profiling practices carried out through the SYRI system involving citizens which were not suspected of violations or crime. They argued that the above-mentioned system profiled entire neighborhoods, while the algorithm behind it lacked transparency and could not be subject to verification. Another argument that was brought referred to the use of SyRI mostly in vulnerable groups areas of extreme poverty. The Dutch Court concluded that the legislation governing SyRI does not ensure a fair balance to justify the interference with private life, also emphasizing its potential of discriminating and stigmatizing certain categories of vulnerable people, as well as the challenges that those identified by the system as high fraud risk face in defending themselves.²⁴

SyRI case reached international interest mainly concerning its “substantive considerations regarding fundamental rights aspects”,²⁵ although it is argued that “the case does not conclusively set legal limits to data-based surveillance more generally”,²⁶ being considered more of a “Pyrrhic victory”²⁷ for the plaintiffs.

4. Conclusions

The unprecedented evolution of artificial intelligence and new technologies is fundamentally changing not only the ways in which transnational crimes are committed, but also the ways in which they are prevented, combated, and punished, using new tools made available to us by technological advances.

The ability of AI systems to process large amount of data; new biometric identification systems that incorporate artificial intelligence (like face or voice recognition); AI systems used for migration, asylum, and border control management, as well as AI systems used for risk assessment, are now being considered game-changers for law enforcement, having an increasingly significant impact in this regard.

However, despite all the new and numerous advantages brought about by the ongoing evolution of artificial intelligence, the risks associated with its use must not be overlooked when assessing the overall picture.

²⁴ A. SACHOULIDOU, *Going Beyond the “Common Suspects”: to be Presumed Innocent in the Era of Algorithms, Big Data and Artificial Intelligence*, in *Artificial Intelligence and Law*, 2023.

²⁵ A. MEUWESE, *Regulating Algorithmic Decision-making One case at the Time: a Note on the Dutch “SyRI” Judgement*, in *European Review of Digital Administration&Law*, 2020, no. 1-2, p. 209.

²⁶ *Ibid.*

²⁷ *Ibid.*

The need to protect individuals' fundamental rights in the context of the use of new technologies is a real one, and it must guide any use of such systems.

In this context, the adoption of the European Regulation on Artificial Intelligence - which imposes restrictive conditions on high-risk systems while prohibiting the use of systems that pose a risk deemed unacceptable to fundamental rights - is an extremely important step toward ensuring safeguards for individual rights.

Striking a balance between the (undeniable) benefits derived from its use and the risks that highlight its potential to infringe upon fundamental rights makes artificial intelligence an extremely useful tool, but at the same time a weapon that can have serious consequences.

This is precisely why robust regulation and responsible use, grounded in ethical principles, are essential when it comes to artificial intelligence and the new technologies.

ABSTRACT: This article aims to analyze how artificial intelligence systems can be used to combat transnational crime within the EU, the legal framework governing their use, as well as the potential risks to personal rights arising from their use and how to address or mitigate these risks. With AI tools being used both in the commission of crimes and in their prevention, combating, and punishment, an analysis of the legal and ethical implications of technological progress regarding transnational crime is essential in the current context. The analysis will be based primarily on the relevant provisions set forth in the recently adopted AI Act.

KEYWORDS: AI – Fundamental Rights – Risks Assessment – SyRI Case – Transnational Crime.