17th Year of Publication, No.2
December 2025

USE OF ARTIFICIAL INTELLIGENCE FOR BIOMETRIC IDENTIFICATION UNDER EU REGULATION NO. 2024/1689

Rrezart Bushati*, Emanuela Furramani**

*Albanian University, Tiranë
**Universiteti "Luigj Gurakuqi", Shkodër

Abstract

The use of artificial intelligence (AI) brings both innovations and advantages, but it also poses risks, particularly when applied within the criminal justice system. To ensure that technology does not undermine fundamental rights and freedoms, criminal law must adapt to these new technological advancements. One area of concern is the application of biometric identification technology during the investigation phase or the criminal procedure.
In June 2024, the European Union adopted Regulation No. 2024/1689 on Artificial Intelligence, focusing on the protection of human rights. This regulation amends previous laws regarding artificial intelligence and establishes harmonized rules. It prohibits the marketing, deployment, or use of artificial intelligence systems for predictive policing and crime risk analysis, as well as the placing on the market, putting into service, or use of artificial intelligence systems that are manipulative or deceptive, and at the same time limits the use of artificial intelligence for biometric identification.

Keywords: *Artificial intelligence, biometric identification, fundamental rights, European Union, criminal justice.*

1. The use of artificial intelligence in criminal justice

The use of artificial intelligence is confronting human society with new challenges to fundamental human rights and freedoms. Based on the use of new technologies in various fields, numerous discussions have emerged in the field of criminal justice regarding their application for the purpose of protecting public safety.
Researchers raise the most problematic issue regarding artificial intelligence in the field of criminal justice: its use in developing investigations, such as real-time biometric identification of a person based on specific facial characteristics[1]. Artificial intelligence employs systems that record and process

1 M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in Sistema penale, 12 settembre 2022: https://www.sistemapenale.it/.; G. Mobilio,

biometric data of an infinite number of individuals, enabling the identification of an individual based on body characteristics, fingerprints, DNA, or iris shape[2], all of which are considered sensitive data[3]. The question posed in this paper pertains precisely to the issue of whether, in the name of public security, the fundamental rights of the individual, guaranteed at the constitutional level, can be limited, including the rights to privacy, assembly, manifestation, and the free expression of opinions. The balance between human rights protection and public security is very fragile, as there is the possibility of abuse by users of this technology, as well as the risk that the latter may make erroneous assessments.

2. The risk to fundamental human rights from the use of artificial intelligence

The challenge of guaranteeing fundamental rights and freedoms in the context of criminal justice is related to the evolution and adaptation of the criminal justice system to ensure that the use of technology does not undermine respect for these rights and freedoms. One of the applications of artificial intelligence that raises concerns is the use of biometric identification technology during the investigation or criminal procedure.

In fact, researchers consider the use of artificial intelligence in the field of criminal justice as a high-risk activity[4]. Although it is worth noting that the use of artificial intelligence cannot be completely excluded, it should be subject to limitations by domestic laws. To address the problems that arise from the use of artificial intelligence, EU Regulation No. 2024/1689 *on Artificial Intelligence* aims to regulate the use of artificial intelligence by striking a balance between the adoption of new technologies and respect for the fundamental rights and freedoms of individuals[5].

The numerous concerns raised as a result of the use of artificial intelligence in the criminal field are related to several fundamental rights and freedoms, including the right to privacy; the protection of personal data; the freedom of assembly and association; freedom of expression and opinion[6], which may be violated in cases of surveillance[7] without the consent of individuals; and the right to non-discrimination on the basis of race, ethnicity, etc., as in cases of profiling[8] on racial or

Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative, Editoriale Scientifica, Napoli, 2021.; E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, 16 ottobre 2020: www.lalegislazionepenale.it.

2 M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, cit., p. 2-3.

3 Law No. 124/2024 on the Protection of Personal Data, in Article 5, point 28, provides the definition of sensitive data: "*Sensitive data are special categories of personal data that reveal racial or ethnic origin, political opinions, religious beliefs or philosophical views, union membership, genetic data, biometric data, data about a person's health, life or sexual orientation.*"; See also *Riconoscimento biometrico delle persone: i falsi miti da conoscere e sfatare*, 13/07/2020: https://www.studiolegalestefanelli.it/.

4 M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali,* in *Processo penale e giustizia,* 31.3.2025.; S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, 16 gennaio 2025: https://dirittodidifesa.eu/.

5 S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, 16 gennaio 2025: https://dirittodidifesa.eu/.

6 M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali,* cit.; G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, cit., p. 57.

7 "*The collection and processing of personal data, whether identifiable or not, for the purpose of influencing or controlling those to whom they belong"*: in this regard, see D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002, p. 2 dhe G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

8 According to Article 4 of the EU Regulation No. 2016/679, *on the Protection of Personal Data*, "profiling" means "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or*

ethnic grounds.

Here we can mention one of the most worrying cases in the international arena, that of China and the use of artificial intelligence to identify individuals belonging to the ethnic-religious (Turkic-Muslim) Uyghur[9] minority, justified by the Chinese government with the pretext of the fight against terrorism and the protection of national security. In this case, the technology focuses on detecting even the slightest changes in emotions and facial expressions. It also involves profiling individuals to evaluate or forecast the probability of future criminal behaviour (predictive policing). Consequently, individuals can be identified as potential criminals before they commit any crimes, based on an assessment of their future risk to engage in criminal behaviour[10]. This raises significant concerns about the impact on fundamental rights associated with the use of this technology. Additionally, the absence of domestic regulations in numerous countries that govern the use of artificial intelligence and address potential issues arising from its implementation heightens these concerns.

In 2021, the Italian Data Protection Authority ruled that the use of real-time facial recognition systems by the police was illegal due to violations of the right to privacy. This ruling specifically addressed the SARI Real-Time system, which was intended for police use. The system operates by deploying multiple cameras within a defined geographical area to identify individuals in real-time. It compared these individuals against data held by the relevant authorities. When the system identified a person, it would trigger an alert for police officers[11].

The Personal Data Protection Authority emphasized that the facial recognition system used for crime prevention poses significant threats. The Authority stated that such technology, which enables mass surveillance, may infringe on individuals' rights to privacy, human dignity, and other fundamental rights[12]. When processing biometric data through facial recognition technology, it is essential to meet several key conditions: the use must be necessary, proportionate to its intended purpose, and compliant with the guarantees outlined in EU Regulation No. 2016/679 on the Protection of Personal Data (GDPR). In response to this decision, Italian lawmakers implemented a moratorium on the use of cameras for facial recognition, which remained in effect until December 31, 2025.

3. European Union Regulation No. 2024/1689 on Artificial Intelligence

On 13 June 2024, the European Union adopted Regulation No. 2024/1689 on *Artificial Intelligence*[13], also known as the *AI Act*, which was published in the Official Journal of the European

movements"; The same definition is given by the Albanian legislation, Law No. 124/2024 on the Protection of Personal Data, Article 5, point 19: *"Profiling" is any form of automated processing of data consisting of the use of data to evaluate certain aspects relating to a natural person, in particular to analyze or predict aspects concerning his/her performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements."*

9 M. Clarke, *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, Manchester University Press, 2022, p. 10.; B. Chekroun, S. Deleuze, Q. Stevenart, *Riconoscimento facciale e diritti umani: linee guida per gli investitori*, Candriam, Marzo 2021, p. 15: https://www.candriam.com/.; Regarding the serious violations of the rights of the Uyghur ethnic-religious minority, a matter that was brought to the attention of the International Criminal Court, see: G. Pane, *Il popolo abbandonato degli Uiguri: il Prosecutor della CPI chiude le indagini contro la Cina*, in www.iusinitinere.it, 28 settembre 2021.; The Office of the Prosecutor - International Criminal Court, *Report on Preliminary Examination Activities 2020*, 14 dicembre 2020, para. 70: www.icc-cpi.int/sites/default/files/itemsDocuments/2020-PE/2020-pe-report-eng.pdf.

10 G. Pozza, *Sorveglianza di massa, la Cina non è poi così lontana: perché potremmo diventare tutti uiguri*, 21 luglio 2022: https://www.agendadigitale.eu/.; M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in Sistema penale, 12 settembre 2022, p. 11: https://www.sistemapenale.it/.

11 Il Garante per la Protezione dei Dati Personali, *Parere sul sistema Sari Real Time,* 25 marzo 2021 [9575877]: https://www.garanteprivacy.it/.

12 Il Garante per la Protezione dei Dati Personali*, Parere sul sistema Sari Real Time, cit.*

13 European Union Regulation, No. 2024/1689, 13 June 2024, on *Artificial Intelligence*, in the Official

Union on 12 July 2024. The EU Regulation emphasizes the protection of fundamental human rights and freedoms. It was created to establish a comprehensive legal framework for the use of artificial intelligence within the European Union, which includes specific limitations on the use of AI in certain cases.

The EU regulation amends previous regulations on the use of artificial intelligence and establishes harmonized rules, prohibiting practices such as:

- the placing on the market, putting into service, or use of artificial intelligence systems for ***predictive policing and crime risk analysis***[14];
- the placing on the market, putting into service, or use of artificial intelligence systems that are ***manipulative or deceptive or that exploit vulnerabilities, influencing the behaviour of users***[15];
- Social rating systems or real-time public area surveillance systems based on biometric recognition patterns. This prohibition is provided for by Article 5, paragraph 1, letter (g) of the Regulation, which prohibits the use of biometric categorization systems to conclude race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation[16], and letter (h) imposes strict restrictions on the use of real-time remote biometric identification for public security purposes, unless and to the extent that such use is strictly necessary for searching for specific victims of kidnapping, trafficking in human beings, or sexual exploitation of human beings; searching for missing persons; and preventing a terrorist attack[17].

The regulation will be fully implemented after 24 months. However, the prohibitions and prohibited practices will take effect 6 months after the regulation comes into force.

5. Conclusions

The use of artificial intelligence in the criminal justice system offers advantages in preventing and combating crime. Nevertheless, it also poses significant risks to fundamental human rights and freedoms. Consequently, states face the challenging task of regulating this emerging field to ensure a balance between the use of artificial intelligence and the protection of human rights.

Considering that artificial intelligence systems can be misused, legislators need to address these concerns by implementing necessary restrictions on their use. For this reason, the European Union has limited mass surveillance in public spaces aimed at the biometric identification of individuals.

Journal of the European Union, series L, 12.7.2024.

14 EU Regulation, No. 2024/1689, *cit.*, Article 5, point 1, letter d).

15 EU Regulation, No. 2024/1689, *cit.*, Article 5, point 1, letter a) and b).

16 EU Regulation, No. 2024/1689, *cit.*, Article 5, *Prohibited AI practices,* point 1, letter g): "*The following AI practices shall be prohibited (...): the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement".*

17 EU Regulation, No. 2024/1689, *cit.*, Article 5, Prohibited AI practices, point 1, letter h): *"the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as 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 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.;* See C. Morelli, *Categorizzazione e identificazione biometrica: guida UE ai divieti. Cosa prevedono le linee guida della Commissione Europea sui sistemi di intelligenza artificiale vietati dall'AI ACT*, 12/02/2025: https://www.altalex.com/.

5. Bibliography

1. European Union Regulation, No. 2024/1689, 13 June 2024, on *Artificial Intelligence*, in the Official Journal of the European Union, series L, 12.7.2024.
2. M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali,* in *Processo penale e giustizia,* 31.3.2025.
3. M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in Sistema penale, 12 shtator 2022: https://www.sistemapenale.it/.

4. G. Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021.

5. E. Sacchetto, *Face to face: il complesso rapporto tra automated facial recognition technology e processo penale*, 16 ottobre 2020: www.lalegislazionepenale.it.

6. D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano, 2002.

7. G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

8. M. Clarke, *Framing the Xinjiang emergency: colonialism and settler colonialism as pathways to cultural genocide?*, in ID. (a cura di), *The Xinjiang emergency Exploring the causes and consequences of China's mass detention of Uyghurs*, Manchester University Press, 2022, fq. 10.

9. G. Pozza, *Sorveglianza di massa, la Cina non è poi così lontana: perché potremmo diventare tutti uiguri*, 21 luglio 2022: https://www.agendadigitale.eu/.

10. Il Garante per la Protezione dei Dati Personali, *Parere sul sistema Sari Real Time,* 25 marzo 2021 [9575877]: https://www.garanteprivacy.it/.
11. EU Regulation No. 2016/679, *on the Protection of Personal Data (GDPR).*
12. G. Pane, *Il popolo abbandonato degli Uiguri: il Prosecutor della CPI chiude le indagini contro la Cina*, 28 settembre 2021: www.iusinitinere.it.
13. The Office of the Prosecutor - International Criminal Court, *Report on Preliminary Examination Activities 2020*, 14 dicembre 2020, para. 70: www.icc-cpi.int/sites/default/files/itemsDocuments/2020-PE/2020-pe-report-eng.pdf.
14. B. Chekroun, S. Deleuze, Q. Stevenart, *Riconoscimento facciale e diritti umani: linee guida per gli investitori*, Candriam, marzo 2021: https://www.candriam.com/.
15. *Riconoscimento biometrico delle persone: i falsi miti da conoscere e sfatare*, 13/07/2020: https://www.studiolegalestefanelli.it/.
16. Law No. 124/2024 on the *Protection of Personal Data.*
17. C. Morelli, *Categorizzazione e identificazione biometrica: guida UE ai divieti. Cosa prevedono le linee guida della Commissione Europea sui sistemi di intelligenza artificiale vietati dall'AI ACT*, 12/02/2025: https://www.altalex.com/.
18. S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, 16 gennaio 2025: https://dirittodidifesa.eu/.