THE EU AI ACT AND CRIMINAL JUSTICE: REGULATORY CHALLENGES FOR BIOMETRIC AND IMAGE RECOGNITION TECHNOLOGIES

Alžběta Solarczyk Krausová*

Abstract: *The EU's applicable regulatory framework defines specific rules for cases in which AI-driven biometric and image recognition tools are used in criminal investigations. At the same time, the regulatory framework comprises multiple applicable legal instruments. This paper analyzes how the EU AI Act and the Law Enforcement Directive jointly govern police use of image-based AI, focusing on prohibited practices, high-risk classifications, and transparency duties, and clarifying their interaction with GDPR during system training. It then examines operational implications for law enforcement agencies developing or deploying image-recognition systems, including evidentiary reliability, human oversight, and organizational safeguards against automation bias and "silent omission". Finally, it evaluates the proposed Digital Omnibus and Digital Omnibus on AI and their potential to recalibrate data-access and compliance timelines for law-enforcement AI. The paper offers a normative and practical roadmap for aligning powerful image-recognition tools with fundamental-rights protection and sustainable criminal-justice legitimacy.*

Keywords: *EU AI Act, Law Enforcement Directive, GDPR, artificial intelligence, image recognition, law enforcement, prohibited AI practices, biometric identification, biometric categorization*

INTRODUCTION

We have arrived at a moment in legal history, where we start to reevaluate the role of modern technologies in a very sensitive area of criminal justice. Criminal investigation and criminal proceedings traditionally represent one of the most important parts of a legal system as they have the most significant impact on lives of individuals as on the society as well. The purpose of criminal law is to prevent, investigate, and detect crimes, to bring offenders to justice, and to reform them during their potential sentence period. On the general level, its purpose is to protect the society from harmful behavior. Police, as the body responsible for law enforcement, has had limited resources when fulfilling their role in fulfilling the abovementioned purposes. However, rapid advancements and developments of technologies such as artificial intelligence (AI), and especially machine learning (ML) started to provide police with unprecedented possibilities in both crime investigation and law enforcement areas.

Despite the fact that AI systems *"may offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies* […] *at the same time they may entail significant risks for the fundamental rights of people.*"[1] Some of

* Mgr. Alžběta Solarczyk Krausová, Ph.D., LL.M., Institute of State and Law of the Czech Academy of Sciences, Prague, Czech Republic. E-mail: alzbeta.krausova@ilaw.cas.cz. ORCID: https://orcid.org/0000-0002-1640-9594.
This paper was supported by the Ministry of Interior of the Czech Republic under grant No. VJ02010029 "AISEE - Artificial Intelligence based Search Environment for video/photo."
AI assistance disclosure. The author used ChatGPT (OpenAI) and Gemini (Google) to refine the presentation of arguments, and to improve phrasing and readability. Google Translate was used to assist with translation of parts of the text. Grammarly was used for minor grammatical improvements. All substantive intellectual decisions, interpretations, and conclusions are those of the author, who also reviewed and edited all AI-assisted text.

the most controversial use cases involve AI-based image recognition technologies. The most feared technology is definitely biometric identification in real time that gave rise to a number of analyses examining its impact on fundamental human rights. Greatest concerns were related to potential abuse of facial recognition technologies in form of discrimination or mass surveillance[2] and a number of experts mentioned problems related to use of privately held facial recognition technologies such as Clearview.[3] Some of these concerns were projected into European proposals on AI regulation[4] and an overlapping regime of AI regulations and other laws in the context of criminal investigation was examined early on as well.[5] The potential of AI technologies use in the area of criminal justice has been researched by international organizations such as the Council of Europe,[6] OECD,[7] Interpol,[8] or Europol.[9]

In the realm of criminal justice, image recognition technologies serve a wide range of investigative and operational functions oriented on identifying individuals as well as analyzing physical environments. Police can use AI systems for forensic facial comparison and database searching (e.g. comparing suspects against official watchlists or personal records) as well as for "softer" biometric analysis like gait or silhouette recognition. Beyond identifying people, AI systems can automate monitoring of vehicles through license plate recognition or track specific car models or colors across multiple camera feeds to reconstruct the route of their movement. Image recognition systems can also provide real-time alerts for the presence of weapons, abandoned bags, or tools associated with burglaries, and can even flag specific behavioral events such as fights or unauthorized intrusions. In the field of digital forensics, these technologies are indispensable for so called evidence management.

---

[1] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). In: *EUR-Lex* [online]. 2021 [2025-12-02]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_132_R_0003>. See point H.

[2] MOBILIO, Giuseppe. Your face is not new to me – Regulating the surveillance power of facial recognition technologies. *Internet Policy Review*, 2023. Vol. 12, No. 1. DOI: 10.14763/2023.1.1699.

[3] See for instance REZENDE, Isadora Neroni. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*. SAGE Publications Ltd STM, 2020, Vol. 11, No. 3, p. 375–389. ISSN 2032-2844. DOI: 10.1177/2032284420948161 or SCIPIONE, Jacopo. Has the Horse Bolted? Dealing with Legal and Practical Challenges of Facial Recognition. *SSRN Electronic Journal*. 2022. ISSN 1556-5068. DOI: 10.2139/ssrn.4019105.

[4] PAPAKONSTANTINOU, Vagelis. ZARKADOULAS, Evangelos. Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement. *EUCRIM*, 2023. No. 2, p. 237-240. Available at: <https://eucrim.eu/articles/remote-biometric-identification-and-emotion-recognition-in-the-context-of-law-enforcement/>.

[5] RAPOSO, Vera Lúcia. "Look at the camera and say cheese": the existing European legal framework for facial recognition technology in criminal investigations. *Information & Communications Technology Law*. Taylor & Francis Ltd, 2024, Vol. 33, No. 1, p. 1–20. DOI: 10.1080/13600834.2023.2239621.

[6] The international convention prepared by the Council of Europe is significant for criminal justice as well. See The Framework Convention on Artificial Intelligence. In: *Council of Europe* [online]. [2025-12-02]. Available at: <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>. The Council of Europe started to prepare a specific instrument on AI and criminal law as well. See Artificial Intelligence and Criminal Law - European Committee on Crime Problems. In: *Council of Europe* [online]. [2025-12-02]. Available at: <https://www.coe.int/en/web/cdpc/artificial-intelligence-and-criminal-law>.

[7] AI in law enforcement and disaster risk management: Governing with Artificial Intelligence. In: *OECD* [online]. 18. 9. 2025 [2025-12-02]. Available at: <https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/ai-in-law-enforcement-and-disaster-risk-management_99fc1804.html>.

[8] See for instance Future of policing. In: *Interpol* [online]. [2025-12-02]. Available at: <https://www.interpol.int/en/How-we-work/Innovation/Future-of-policing>.

[9] AI and policing – The benefits and challenges of artificial intelligence for law enforcement. In: *Europol* [online]. [2025-12-02]. Available at: <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>.

They allow investigators to search through massive volumes of seized data for specific visual cues like pieces of clothing, tattoos, or geolocation landmarks. Moreover, specific AI systems can assist in the detection of deepfakes or illegal content. Finally, these systems can help in the protection of privacy, as AI can automatically blur the faces of witnesses or third parties in video evidence before it is shared within the judicial system.

It is obvious that the use of AI systems in criminal justice has a huge potential. At the same time, given its potential riskiness, the area of development and use of AI systems becomes to be heavily regulated. Therefore, the aim of this paper is to explore implications of the latest European regulatory developments on the specific area of use of AI image recognition and biometrics in the area of police work. The paper will namely explore two main regulatory instruments that cover development and use of these technologies – the EU AI Act (hereinafter also AIA)[10] and the Law Enforcement Directive (hereinafter also LED)[11] that specifically covers processing personal data in the context of prevention, investigation, detection or prosecution of criminal offences. Firstly, the paper will describe the relevant rules that apply to AI image recognition. Secondly, the paper will identify what are the implications of these rules for training and deploying specialized AI systems for image recognition (including biometric data processing). Different use cases will be explored and recommendations will be provided on how to proceed with using the technology in order to protect fundamental rights while keeping a high evidentiary value of AI systems' outputs. Thirdly, the paper will explore the latest regulatory trends in simplification of rules for data processing and potential changes to the AI Act.

I. REGULATION OF AUTOMATED IMAGE RECOGNITION IN CRIMINAL JUSTICE

I.1 Artificial Intelligence Act

The AIA is the main regulatory instrument that sets out comprehensive rules covering a number of use cases of automated image recognition technologies in the context of criminal justice. By adopting a risk-based approach, the AIA distinguishes between applications that are strictly prohibited due to their unacceptable threat to fundamental rights, high-risk AI applications, whose development and use is permitted under rigorous oversight, AI systems with transparency requirements and general-purpose AI models. The following text will examine whether and how these categories apply and what these rules mean for criminal justice.

[10] 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) (Text with EEA relevance). In: *EUR-Lex* [online]. 2024 [2025-12-02]. Available at: <http://data.europa.eu/eli/reg/2024/1689/oj>.

[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. In: *EUR-Lex* [online]. 2016 [2025-12-02]. Available at: <http://data.europa.eu/eli/dir/2016/680/oj>.

Prohibited AI Practices

The AIA sets out a number of prohibited practices that are relevant for the use of AI image recognition systems in criminal investigation. Three of the practices are rather general use cases. The fourth use case is a highly sensitive one – a real-time remote biometric identification. This use case is in principle prohibited. However, there are specific exemptions for police work. Firstly, we will analyze application of the three use cases on criminal justice scenarios and then the real-time remote biometric identification will be analyzed.

From the perspective of AI image recognition, the AIA prohibits the use of visual analysis tools for predictive policing when they rely on profiling personality traits (Art. 5, par. 1, letter (d)). This means police cannot use AI systems that analyze photos or video footage of a person – such as their facial micro-expressions, gait, or clothing style – to predict the likelihood of committing a future crime based on a psychological profile. For example, a camera system cannot be deployed to scan people in a train station and flag an individual as "high risk" simply because an AI system interprets their nervous facial ticks or body language as indicating a "criminal personality." However, this prohibition allows for an important exception regarding objective visual evidence. Image recognition systems can still be used to detect specific, verifiable criminal acts or objects. While AI systems must not predict that a person looks like they might steal, it is permitted to use AI systems to analyze video streams to detect the objective presence of a weapon in someone's hand or to flag a person currently climbing over a security fence, as these are factual indicators of a crime in progress rather than abstract character assessments.

The AIA strictly forbids not only creation but also the use of AI-based facial recognition systems that function by matching input images against databases built through untargeted scraping (Art. 5, par. 1, letter (e)). In the context of image recognition, this prevents police from using software that compares a suspect's photo from a crime scene against a massive repository of facial images harvested indiscriminately from the internet or public CCTV feeds. Practically, this means an investigator cannot take a still frame of an unknown suspect from a surveillance video and upload it to a commercial platform that searches against billions of photos scraped from social media sites like Facebook or Instagram. The image recognition process must instead rely on official, controlled databases, such as a national registry where the images were collected lawfully, ensuring that the technology is not powered by the non-consensual harvesting of citizens' public photos. This is also important from the perspective of picture quality as unofficial pictures van produce an increased number of false positives and, thus, negatively impact fundamental human rights. It is, however, important to note that this prohibition does not apply in situations when no AI systems are involved in scraping. [12] This might be a tricky requirement though because of a potential lack of information about how does a particular system work.

[12] See point (234) of EUROPEAN COMMISSION. Communication from the Commission. Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). C(2025) 5052 final. In: *European Commission* [online]. 4. 2. 2025 [2025-12-02]. Available at: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.

AIA also limits how image recognition systems can categorize individuals based on their physical appearance (Art. 5, par. 1, letter (g)). It prohibits the use of AI to analyze biometric data in photos or videos to infer sensitive private attributes like race, political opinions, or religious beliefs. A practical example of this prohibition would be the ban on using video analytics at a public demonstration to automatically scan the crowd and classify participants into groups based on their ethnicity or religious clothing. The AI cannot be used to deduce a person's internal beliefs or private status from their visual biometric markers. However, a key exception exists for the management of visual evidence. Police is permitted to use image recognition to filter or label lawfully acquired video files. For instance, if police have seized hours of digital videos or CCTV footage, they can use an AI tool to "filter for individuals wearing glasses" or "find all images of a person with a beard" to organize the information, as this uses visual biometrics for sorting rather than for inferring sensitive personal traits (see Recital 30 of AIA).

Real-time remote biometric identification (often called live facial recognition) is considered by the AIA as an exceptionally intrusive technology and is generally prohibited in publicly accessible spaces. This prohibition prevents police to use this technology as a standard surveillance tool. It is an exceptional measure, strictly limited to three specific operational objectives (Art. 5, par. 1, letter (h)). If a situation does not fall into one of these three categories, police does not have the legal authority to activate a real-time remote biometric identification system.

The first exception allows police to use real-time identification to conduct targeted searches for specific victims. This permission is granted for finding missing persons or victims of abduction, human trafficking, or sexual exploitation. For example, if a child goes missing or intelligence indicates a trafficking victim is being moved through a city, law enforcement is authorized to deploy live recognition tools to locate them. They cannot, however, use this justification to search for individuals who are merely witnesses or persons of interest in non-critical investigations; the focus must remain on the safety of the victim.

The second exception allows police to deploy these systems to prevent a specific, substantial, and imminent threat to life or physical safety, or to avert a terrorist attack. This allows police to react to immediate dangers, such as a bomb threat at a public venue or intelligence regarding an impending attack. In these scenarios, police can turn on the system to detect the specific individuals posing the threat. They cannot use this exception for general crime prevention or to monitor peaceful protests, as the threat must be "genuine and present" or "foreseeable" and involve serious physical harm.

The third exception allows police to use real-time biometrics to locate or identify suspects involved in serious criminal offenses. However, they cannot use this power for just any crime. The offense must be listed in a specific legal annex (Annex II) and must be punishable by a prison sentence of at least four years in their Member State. This means police can use the technology to track a murder suspect or an armed robber, but they are prohibited from using it to identify someone suspected of petty theft, vandalism, or other lower-level crimes that do not meet this severity threshold.

Even when a situation fits one of these three categories, police cannot simply activate the system on their own authority. In standard cases, they must obtain prior authorization from a judicial authority or an independent administrative authority (Art. 5, par. 3). They

are required to submit a reasoned request proving that the use is necessary, proportionate, and limited in time and geographic scope. If the judge does not grant permission, the police cannot proceed. There is an exception for urgent situations where waiting for a judge would be impossible, such as an active terrorist attack. In these "duly justified cases of urgency," police can use the system without prior approval. However, they cannot operate indefinitely without oversight. Authorization must be requested within 24 hours of activation. If the judicial authority rejects the request, the police must immediately stop the system and delete all data, results, and outputs generated during that time. They cannot keep or use any evidence gathered during an unauthorized period if the judge subsequently rules against the urgency.

High-Risk AI Systems

High-risk AI systems are systems that are considered to pose a significant threat to health, safety, or the fundamental rights of individuals. The right determination of whether an AI systems falls under the category of high-risk AI systems has a significant impact on how police can operate. In the context of police work (and namely use of AI image recognition systems), the Annex III. of AIA is especially relevant. According to this Annex, the following two categories of use cases are the most relevant:

- Biometrics (point 1): This category includes AI systems used to identify individuals or infer their internal states (emotions). It specifically covers post-remote biometric identification, where police use software to search through recorded videos to identify a suspect after an event has occurred. It also includes emotion recognition systems, which are used to detect lies or assess the emotional state of a person during questioning. These tools are high-risk because errors can lead to wrongful identification or the misinterpretation of a suspect's nervousness as evidence of guilt.
- Law enforcement (point 6): This category includes AI systems used for risk assessment, both for assessing the risk of a person becoming a victim and for predicting the likelihood of an individual re-offending. It also includes systems designed to detect lies, such as AI-driven polygraphs used during interrogations, as well as tools used for profiling individuals. Finally, this high-risk classification includes AI systems used to evaluate the reliability of evidence.

The regulation of high-risk AI systems in the AIA creates a specific operational framework for how police can use automated image recognition technologies that are permitted but at the same time sensitive. Specifically, while real-time biometric identification is largely banned, the use of AI to identify individuals in recorded footage (post-remote biometric identification) is classified as high-risk. This means that when police uses AI software to analyze hours of CCTV footage to identify a suspect based on their biometrics, they cannot treat it as a standard software tool. They are subject to a vast number of obligations designed to ensure the technology is safe, accurate, and non-discriminatory.

Police must ensure that the image recognition systems they utilize have been developed with high-quality data governance to prevent bias. Because these systems are high-risk, the algorithms must be trained on datasets that are sufficiently representative to avoid errors that disproportionately affect specific racial or ethnic groups. In the context

of criminal justice, this is critical to preventing wrongful identifications. Police authorities cannot deploy a system that performs accurately on one demographic but frequently misidentifies others. They rely on the provider of the system to verify this accuracy, but the police as users must also monitor the system's performance in real-world conditions and report any serious incidents or malfunctioning that could lead to a breach of fundamental rights.

A central requirement for police use of these high-risk image recognition systems is a strict human oversight. The regulation mandates that an AI system cannot be a sole or final decision-maker in criminal investigation. When an image recognition tool flags a "match" between a suspect and a face in a video, a human must verify and confirm that result. The police operational procedures must be designed to counteract "automation bias" – the tendency for humans to trust computer suggestions. Police officers must understand system's limitations and be competent to disregard AI's outputs if they contradict other evidence or professional judgment.

Finally, police is required to maintain high levels of transparency and accountability regarding their use of these technologies. Before deploying a high-risk AI system for image recognition, law enforcement agencies are generally required to conduct a Fundamental Rights Impact Assessment (FRIA)[13] to evaluate how the tool might affect the rights of citizens in that specific context. Furthermore, the system must automatically generate logs of its operations. This creates a digital audit trail, ensuring that every time the police use the AI to run a facial recognition search, the action is recorded. This logging is essential for criminal defense and judicial review, allowing courts to verify exactly how evidence was processed and ensuring that the technology is not being used for unauthorized or undocumented surveillance.

Systems with Transparency Requirements

AIA recognizes another category of AI systems for which it sets out specific requirements on transparency (Art. 50). These rules have an impact on both the use cases of AI image recognition as well as use cases of AI image generation. The transparency rules essentially divide police operations into "covert/investigative" (where secrecy is allowed) and "public service" (where transparency is required).

The first impact of these rules regards undercover operations and synthetic media. Police is explicitly exempt from the requirement to label AI-generated content as "fake" when investigating crime. This is operationally critical for digital image recognition and generation. For example, investigators can use AI to generate realistic, non-existent faces for fake social media profiles to infiltrate online criminal networks. If they were forced to label these profile photos as AI-generated, their cover would be blown immediately. This exception allows police to weaponize generative AI image tools for stinging operations without tipping off targets.

[13] For details, see Art. 27 AIA. Fundamental Rights Impact Assessment (FRIA) should describe exactly how, how often, and for which specific groups of people a high-risk AI system will be used. It requires identification of potential harms to those groups of people, documentation of human oversight measures put in place to prevent errors, and establishing clear internal governance for handling complaints or system failures if those risks occur.

The second impact of these rules concerns covert surveillance and analysis. When police use image recognition systems for emotion recognition or biometric categorization (e.g., estimating age or gender from video), they are exempt from the standard obligation to inform the subject. This means investigators can run AI analysis on footage of a suspect to gauge stress levels or verify physical characteristics without ever notifying the individual that they are being processed by a machine. This ensures that the use of advanced visual analytics remains a silent investigative tool rather than a declared administrative process.

The third impact of these rules lies in the necessity to properly distinguish between forensic enhancement and digital manipulation. The provision allows police to use AI tools for standard editing or functions that do not substantially alter the input data without needing to mark the output as artificially manipulated. In practice, this allows forensic teams to use AI to sharpen blurry videos or adjust lighting to identify a license plate or face. As long as the AI is clarifying existing evidence rather than hallucinating new features, the output can be used in investigations without the heavy technical branding required for deep fakes. The purpose of such process is to preserve the visual utility of the evidence. However, one must note that it does not grant police a license to hide this process from the judiciary. During the criminal investigation, police needs to document and reveal how exactly the image was enhanced to ensure the judge understands it is no longer a "raw" original. To put it simply, according to this rule AIA allows an image file to remain clean (no watermark), but the police report must be transparent as to the use of AI tools.

Finally, a specific boundary is drawn for public reporting interfaces. While police can hide the use of AI during investigations, they cannot do so when the public is reporting a crime. If a police force deploys an AI-based visual chatbot for citizens to report offenses, they must disclose that the system is AI-driven. This ensures that while criminals can be deceived by AI tools during an investigation, law-abiding citizens are not deceived when asking the police for help.

I.2 Law Enforcement Directive

The LED is the primary European law governing how police and criminal justice authorities process personal data. It is *lex specialis* to the General Data Protection Regulation (GDPR)[14] as it is related to a specific context of personal data processing. Its main purpose is to ensure that while law enforcement agencies can effectively exchange information to fight crime, the fundamental privacy rights of individuals are protected. It is safe to say that when it comes to the rules for personal data processing, the LED is stricter than the GDPR. In the context of police investigations, it ensures that data processing is a regulated process where the intrusion into a person's privacy is balanced against the necessity of the investigation.

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). In: *EUR-Lex* [online]. 2016 [2025-12-02]. Available at: <http://data.europa.eu/eli/reg/2016/679/oj>.

Similarly to the GDPR, the LED sets out strict rules for processing of special categories of personal data (Art. 10). The LED mandates that police can only process this sensitive data when strictly necessary, subject to appropriate safeguards, and authorized by law. This is especially relevant for processing biometric data.

The LED also places significant restrictions on automated decision-making and profiling (Art. 11). This is directly relevant to AI systems that might automatically flag an individual as a "suspect" or a "risk" based on video analysis. The LED generally prohibits decisions based solely on automated processing if they produce an adverse legal effect on the person. In practice, this means an AI system recognizing a weapon or a person in a video feed should not automatically trigger a penalty or an arrest. It should merely alert a human operator to check the situation and intervene in the decision-making process.

For the use of new technologies that are likely to result in a high risk to the rights and freedoms of natural persons, the LED requires performance of the data protection impact assessment (Art. 27). Before adopting a new specialized AI system for image/video analysis, police forces must conduct a rigorous assessment to evaluate potential risks to individual rights. They must document how the technology works, what errors might occur (such as bias against certain demographics), and what security measures are in place to prevent misuse. This measure aims to prevent a hasty adoption of potentially dangerous or invasive surveillance technologies.

II. REGULATORY IMPLICATIONS FOR POLICE WORK

II.1 Implications for training AI systems for image recognition

When police decide to move beyond being a mere "deployer" and start to develop an own AI image recognition system, the regulatory burden shifts significantly. This development process requires a two-step legal assessment before any code is written or data is processed. First, the police examine whether the intended system would not fall under the category of prohibited AI practices. For example, a project aimed at training a model to predict a "criminal personality" through facial micro-expressions would be a non-starter, as it is strictly banned under Article 5 of the AIA. If the system passes this initial legality test, the police must then determine if it falls under the high-risk category. Most specialized image recognition tools for law enforcement (such as post-remote biometric identification or evidence reliability evaluation) will be classified as high-risk, triggering extensive technical and documentation obligations, including the requirement for high-quality, representative datasets to prevent algorithmic bias.

From a data protection perspective, the training of an AI system creates a distinct legal environment for police. While processing personal data with help of AI to investigate a specific crime is governed by the LED, the training and development of AI systems typically falls under the regime of the GDPR. This is because at the training stage, the processing of personal data is often not for the prevention, investigation, detection or prosecution of criminal offenses in a specific, active case, but rather for the technical purpose of system development or even scientific research. Consequently, the police must identify a valid legal basis under the GDPR (such as public task or legitimate interest) and adhere to principles like data minimization and purpose limitation. This means that a data-

set collected for one investigative purpose cannot be automatically repurposed to train a general AI model without a separate compatibility assessment and strict adherence to GDPR's higher transparency standards for data subjects. However, there are potential regulatory changes that might allow for certain limited use of personal data originally processed under the LED for the purposes of training AI systems (see Chapter III).

II.2 Implications for deploying AI systems for image recognition

The deployment phase requires police to accurately categorize every AI tool before it touches operational data. Under the AIA, the deployment of high-risk systems requires fulfillment of strict obligations defined throughout the Chapter III. of AIA. For these systems, police must not only ensure human oversight to prevent automation bias but also maintain detailed logs and conduct a Fundamental Rights Impact Assessment (FRIA). In fact, the AIA aims to prevent the situation when the technology is only "set and forgotten." The AIA requires a permanent infrastructure of accountability and a clear chain of human responsibility for every operation.

However, one must not forget that not every AI tool used for image analysis is classified as high-risk.[15] A critical distinction exists for systems used as advanced search and filtering engines for lawfully acquired video and picture files. For example, if an investigator uses an AI tool to "find all sequences in 48 hours of footage where a person is wearing a red jacket" or to "filter for vehicles with a specific roof rack," this deployment typically does not fall under the high-risk regime. Such search would not qualify as an act of evaluating reliability of evidence according to Annex III., point 6, letter (c) AIA. As such AI-based search engines do not materially influence the final legal outcome but rather help a police officer to find relevant pieces of information their own assessment, such tools are viewed as lower-risk. While they still require transparency (the police report should note that AI was used to filter the footage), they are exempt from the scope of high-risk AI systems. This distinction is vital for operational efficiency: it allows police to use AI to navigate "data haystacks" without the administrative paralysis of high-risk regulations, provided the tool's purpose remains limited to data organization and retrieval rather than making autonomous judgments. In this regard it is important to realize that deployment of AI systems can also have significant influence on preparing evidence for judicial proceedings where the lack of proper operation as well as proper use of an AI system might be objected.

When it comes to AI-based search engines using image recognition, the most profound problem is occurrence of so called "silent omission". This happens when a system fails to flag relevant footage. Awareness of technical features like this is crucial for both setting up proper organizational protocols for searching as well as for preserving the evidentiary value of files and consequent human conclusions about a particular case.

---

[15] In this regard one needs to oppose statements of some researchers who do not distinguish among different use cases of AI-based image recognition technologies in criminal investigation and classify all use cases as high risk. For instance LORCH, Benedikt, Nicole SCHELER and Christian RIESS. Compliance Challenges in Forensic Image Analysis Under the Artificial Intelligence Act. *2022 30th European Signal Processing Conference (EUSIPCO)*, Belgrade, Serbia, 2022. p. 613-617. DOI: 10.23919/EUSIPCO55093.2022.9909723.

From an organizational perspective, police should set up procedural safeguards such as multiple-layered searching strategy (use of alternative formulations when searching for something), random sampling from files where a searched object was not identified and manual check of such files, combination of more searching models, etc.

In general, evidentiary value must always be taken into account when AI systems are used. Different use cases imply different evidentiary value. The less autonomous an AI system is, the higher the evidentiary value of its output is. For instance, in case of license plate or text recognition, the output of an AI system carries significant weight because it is based on objective data that is easily verifiable by a human observer viewing the original source. However, as the use case moves toward object classification (distinguishing a phone from a weapon) or behavioral interpretation (labeling a person as "aggressive"), the evidentiary value can be more easily challenged. Especially in these cases, the human judgment and rigorous argumentation are indispensable.

III. FUTURE REGULATORY ISSUES

Despite the AIA has been adopted only recently and is not yet fully applicable,[16] the European Commission has introduced two new regulatory proposals that – if accepted – would update some rules in AIA. The Commission has acknowledged that the rapid accumulation of digital laws has created a "regulatory thicket" that complicates both compliance as well as enforcement. Therefore, on 19 November 2025 the Commission introduced two critical simplification proposals: the Digital Omnibus and the Digital Omnibus on AI.

The Digital Omnibus[17] focuses on harmonizing existing data and cybersecurity rules. For criminal justice, its most significant contribution is the clarification of the GDPR, specifically regarding the processing of personal data for AI training. The proposal seeks to codify "legitimate interest" as a valid legal basis for training AI models, potentially making it easier for law enforcement agencies and their technology vendors to develop algorithms using real-world data without facing the legal gray areas that currently exist. The Digital Omnibus specifically proposes to add Article 88c "Processing in the context of the development and operation of AI" to the GDPR.[18] This does not imply that law enforcement agencies could use data processed under LED. However, such training is enabled by the Digital Omnibus on AI. [19]

---

[16] The rules of AIA become applicable in stages, as defined in Art. 113 AIA. Different parts of AIA are applicable from 2 February 2025 and from 2 August 2025. Other parts shall apply from 2 August 2026 and Art. 6(1) AIA shall apply from 2 August 2027, if not changed by upcoming new regulations.

[17] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). In: *EUR-Lex* [online]. 2025 [2025-12-02]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52025PC0837>.

[18] Ibid, Art. 3, point 15 of the Digital Omnibus.

[19] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). In: *EUR-Lex* [online]. 2025 [2025-12-02]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=comnat%3ACOM_2025_0836_FIN>.

For the area of law enforcement and police work, the Digital Omnibus on AI is far more consequential. This specific proposal aims to amend the AIA to prevent implementation bottlenecks, i.e. the situation when regulation is in place but the guidelines and standards necessary for legal compliance have not yet been created. Therefore, the Digital Omnibus on AI most notably proposes postponing the application of obligations for high-risk AI systems (originally set for August 2026) to ensure that technical standards are fully ready before the enforcement begins. For law enforcement agencies, this effectively pushes back the deadline for mandatory compliance – such as fundamental rights impact assessments and strict data governance – likely into late 2027 or 2028. While this delay offers police forces more time to prepare, it also prolongs the period of legal uncertainty.

As it was already mentioned, the Digital Omnibus on AI has also potential consequences for using data processed under the regime of LED during training AI systems. Namely, it proposes adding Art. 4a "Processing of special categories of personal data for bias detection and mitigation" to the AIA.[20] According to this provision, if a number of conditions is fulfilled, data originally collected for the purposes of the prevention, investigation, detection or prosecution of criminal offences under LED can be used for the purposes of bias detection and correction. This opens door for police forces to develop AI systems that are more in line with protection of fundamental rights and freedoms.

The Digital Omnibus on AI also removes the mandatory obligation of AI literacy (Art. 4 AIA). On one hand, this reduces training burdens for police officers, on the other hand this may result in increased risk of potentially risky use of AI systems. In the context of criminal justice, this could have serious impact not only on fundamental human rights, but also on the trust of society in police work and justice system as a whole.

CONCLUSION

This paper highlights how AI image recognition systems have already been transforming criminal investigations. At the same time it shows that the existing regulations require that such AI systems must remain only tools for assisting humans rather than replacing their judgment. This is especially critical when an individual's rights, liberty, and reputation are on the line.

The established EU regulatory framework uses multiple instruments to safeguard safety and respect for fundamental human rights. In this complex system of rules the AIA and the LED work in tandem. The AIA serves as the primary instrument for regulating AI systems while distinguishing among different use cases and AI systems with regard to the potential risks they pose. The AIA establishes clear boundaries for real-time remote biometric identification in public spaces by setting out its general prohibition, while allowing for narrow exceptions in cases of missing persons or imminent threats. By classifying post-event video analysis and evidence evaluation as high-risk, the AIA ensures that other biometric recognition technologies are subject to rigorous oversight, technical documentation, and human-in-the-loop requirements to mitigate risks like automation bias. Moreover, the AIA provides other safeguards by defining other types of high-risk AI

[20] Ibid. Art. 1, par. (5).

systems and at the same time by not burdening low-risk AI applications with additional obligations. The LED complements the AIAs regulatory framework with specific rules for processing personal data used by AI systems. It mandates that the use of sensitive biometric data must be strictly necessary and authorized by law, ensuring that any intrusion into a person's privacy is balanced against the specific needs of a criminal investigation. The LED also reinforces the AIA's goals by prohibiting significant legal decisions to be based solely on automated processing, requiring that a human remains the ultimate decision-maker as mentioned above.

However, the rules are still changing. Recent proposals seek to update or simplify the AI framework, and the success of these changes will depend on whether they maintain existing human safeguards or accidentally create new loopholes.

Ultimately, the most effective way to use AI image recognition systems in criminal justice is to keep them transparent and open to challenge. When police ensures that AI outputs can be explained and audited, the technology stops being a legal obstacle and becomes a roadmap for responsible innovation. By prioritizing responsible training and clear procedures, police can use AI to strengthen both their investigations and public trust simultaneously.