

UDK: 342.721 : 004

57

62

Original scientific paper

Pawel Urzenitzok, PhD student

Kozminski University, Poland

E-mail: purzenitzok@kozminski.edu.pl

ORCID ID: 0009-0003-2245-7407

ALGORITHMIC ACCOUNTABILITY IN FACIAL RECOGNITION TECHNOLOGY: ADDRESSING BIAS AND TRANSPARENCY IN EUROPEAN LAW ENFORCEMENT APPLICATIONS

ABSTRACT

Facial Recognition Technology (FRT) is now a key instrument for European police forces, increasing crime prevention and public security. FRT deployment presents several legal, ethical, and social concerns, especially about algorithmic bias and transparency, along with conformity to the standards of European legislation. Literature indicates that FRT technology is more likely to misidentify individuals belonging to minority groups disproportionately, thereby reinforcing structural discrimination and weakening confidence among the public. Despite efforts through regulation, such as the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act), there are loopholes in ensuring algorithmic accountability, control, and bias mitigation. The article critically analyzes the European regulatory framework governing FRT, focusing on data protection, algorithmic fairness, and human rights. The research employs doctrinal legal analysis, case studies, and empirical findings. It identifies gaps in current oversight and highlights the challenges of algorithms and fragmented national rules. The article calls for a European legal framework that would compel algorithmic transparency, independent audits, and bias monitoring in real-time in law enforcement scenarios. The study provides policy suggestions, including required impact analyses, accountability mechanisms, and encouragement of international collaboration, for creating ethical guidelines and technical norms for reconciling technological advancement with essential human rights.

Keywords: *Facial Recognition Technology, FTR, Law Enforcement Technology, Algorithmic Bias, Algorithmic Transparency*

1. INTRODUCTION

Facial Recognition Technology (FRT) has recently become increasingly important in virtually all law enforcement practices. The technology is viewed as a ticket to

absolute safety, excellent investigative processes, and quick suspect identification. Its applications have gone from airport terminals and anti-terrorist watchlist surveillance to crowd control monitoring in real-time. Notwithstanding, the rapid progress of FRT has been met with skepticism in many European countries, particularly regarding its potential biases in algorithmic decision-making, transparency, and compliance with the law. The breakthroughs in machine learning have improved face verification accuracy; however, the trend of erratic error rates to date has been observed that impacts more users among minorities and women.¹ Such variances lead to moral and legal concerns because mistakes in the identification of a person by the police can lead to the loss of individual rights and increase societal inequalities.²

Educational institutions and global technological companies working on rectifying technological bias have targeted the foundational sources of the biases by investigating the technical components, such as selecting training data, facial alignment techniques, and determining the threshold settings.³ Achieving full mitigation is, however, complex, particularly when public bodies are utilizing proprietary or “black-box” algorithms, i.e., those that restrict the possibilities of the people not directly affected or the independent auditors to recognize or contest the biased outcomes. On the other hand, the European Union has followed a strong regulatory strategy to protect personal data and AI governance. The General Data Protection Regulation (GDPR) sets out the basic rules of the game regarding the processing of personal data, and it includes the relevant provisions for automated profiling. Still, some critics point out that the transparency requirement for “meaningful information” can be challenging when the facial recognition systems are not transparent. Also, the Artificial Intelligence Act (AI Act) introduced specific biometric surveillance devices as “high-risk” thus subjecting them to regulatory scrutiny. At the same time, the effectiveness of the regulations and synchronization among the Member States remains a question.⁴

¹ Liang, H.; Perona, P.; Balakrishnan, G., *Benchmarking Algorithmic Bias in Face Recognition: An Experimental Approach Using Synthetic Faces and Human Evaluation*, IEEE/CVF International Conference on Computer Vision (ICCV), 2023, p. 1, 8.

² Buolamwini, J.; Gebru, T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, vol. 81, Conference on Fairness, Accountability, and Transparency, 2018, p. 77.

³ Leslie, D., *Understanding bias in facial recognition technologies*, The Alan Turing Institute, 2020, p. 8–12.

⁴ Raposo, V. L., *The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal*, *European Journal on Criminal Policy and Research*, vol. 28, 2022, p. 1.

This paper investigates the inconsistency between the expansion of law enforcement functions using the FRTs and the need to respect the fundamental rights to privacy, the principle of equality, and the proper course of the law. It primarily pivots around three central research questions:

1. In what specific ways do the GDPR and the AI Act provide explicit and enforceable mechanisms for detecting and correcting algorithmic bias in facial recognition technology, including the one utilized by law enforcement authorities in Europe?
2. What specific legal, technical, and policy measures should form a unified framework across Europe to ensure transparency and accountability in law enforcement's deployment of FRT?
3. How can European regulatory frameworks balance law enforcement's operational requirements with the individuals' rights threatened by FRT's algorithmic biases?

The study employs doctrinal analysis and case studies and highlights serious remaining gaps. It illuminates the vital interdependence between the technical design options, data protection obligations, and the overall legal framework in which law enforcement agencies operate.

2. METHODOLOGY

The research employs a hybrid methodology that combines doctrinal legal analysis with a concentrated examination of the relevant academic and policy documents on facial recognition technology. This study's primary goal is to evaluate the adequacy of the GDPR and the AI Act to mitigate documented biases and enforce the respective transparency and accountability obligations. In this process, the paper looks at the text of each legal instrument, explanatory materials, and interpretive guidance provided by European institutions where necessary.⁵ The study originates in the line of Reasoning that involves a technical evaluation of FRT followed by an empirically grounded application that highlights theoretical issues and addresses the practical difficulties law enforcement agencies face when employing facial recognition in various operational contexts.

The analysis is primarily based on legal texts such as the GDPR, the AI Act, regulations at the EU level regarding FRT by police authorities, the European Data

⁵ European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final, Brussels 2021.

Protection Board (EDPB), and White Papers from the European Commission clarifying the key obligations and risk-classification methodologies.⁶⁷

The literature review heavily relies on indexed and peer-reviewed articles. After thematic analysis, these sources were organized around specific issues related to algorithmic bias detection, fairness metrics, data governance, and accountability. Key considerations were given to empirical studies that examined different demographic groups in the performance of FRT and work advocating for formal instruments like algorithmic impact assessments (AIAs).⁸ Other documents from advocacy bodies such as Fair Trials, Access Now, and AlgorithmWatch provide practical case studies showing companies' difficulties in auditing proprietary algorithms and guaranteeing the proper oversights of the deployments.⁹

This paper investigates the question of incorporating transparency and non-discrimination principles for FRT within the script and AI Act and GDPR through the doctrinal lens. The analysis reaches the endpoint with substantial empirical findings indicating that certain underrepresented demographic groups are more likely to experience higher false match rates, raising the possibility of systematic discrimination.

This research evaluates the currently available channels, including laws, technical research, and advocacy materials. It presents precise steps to tackle algorithmic bias in facial recognition technology. The comprehensive aim is to stimulate a spirit of a coherent EU-wide approach that would be capable of demonstrating both requirements of law enforcement as well as essential protections for equality, due process, and human dignity.

⁶ European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, Brussels 2020.

⁷ European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, adopted on 26 April, 2023.

⁸ Kaminski, M. E.; Malgieri, G., *Multi-layered explanations from algorithmic impact assessments in the GDPR*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery, New York 2020, p. 68.

⁹ https://www.accessnow.org/wp-content/uploads/2022/07/Access-Now-submission-to-the-consultation-on-the-European-Data-Protection-Boards-FRT-for-LEAs-guidelines-05_2022.pdf, 13 February, 2025.

3. LITERATURE REVIEW

3.1. Evidence of Bias in FRT

Empirical studies show that Facial Recognition Technology exhibits higher error rates for certain demographic groups. In evaluation prepared by the U.S. National Institute of Standards and Technology that covers 189 algorithms it was found out that algorithms had far higher positive rates for Asian and African American faces in comparison to Caucasian faces with difference ranging 10 to 100 times depending on the algorithm. Additionally, African American females experienced disproportionately high false positive rates in one-to-many searches that in used by law enforcement to identify suspects in the crowds.¹⁰ Commercial gender-classification systems mis-gendered 34% of darker-skinned women compared with less than 1% of lighter-skinned men.¹¹ European pilots reveal similar patterns. During trials of live FRT led by South Wales Police 95% of the alerts were false positive with Asians disproportionately flagged.¹²

With intersectional accuracy, it is said that commercial gender classification systems were misclassifying darker-skinned females at a rate that was dramatically higher than lighter-skinned men.¹³ Despite promoting the ideas of mitigating racial bias by generative data augmentation and more balanced datasets,¹⁴ it is also mentioned that the underlying network design decisions can exacerbate or lessen these diverse outcomes - such as specific normalization layers or loss functions. All of the above is further complicated by factors such as masks. Masked face recognition could create a more significant imbalance if the number of females is lower in the training set.¹⁵

Evidence shows that new advances can enhance algorithmic performance, which augmentation techniques, but the option of eliminating the risk of disproportional

¹⁰ <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>, 14 February, 2025.

¹¹ <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>, 11 February, 2025.

¹² <https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurling-towards-surveillance-state>, 11 February, 2025.

¹³ Buolamwini, J.; Geburu, T., *op. cit. note 2*, p. 87–88.

¹⁴ Sumsion, A.; Torrie, S.; Lee, D.-J.; Sun, Z., Surveying Racial Bias in Facial Recognition: Balancing Datasets and Algorithmic Enhancements. *Electronics* 2024, 13, 2317, p. 1-2

¹⁵ Atay, M.; Poudyel, M.; Evora, S., *Evaluation of Gender Bias in Masked Face Recognition with Deep Learning Models*, IEEE Symposium Series on Computational Intelligence (SSCI), Mexico City, 2023, p. 829–835.

and wrong classifications remains challenging.¹⁶ The researchers highlight the significance of robust auditing practices like systematic performance benchmarks on demographically balanced samples to identify if models tend to disadvantage a specific subpopulation. Literature warns that the consequences of these biases become increasingly severe in law enforcement contexts, where one misidentification can have legal implications for the person involved.

3.2. Ethical, Human Rights, and European Legal Frameworks

Besides the empirical data, there is a comprehensive discussion about the human rights implications of using facial recognition technology (FRT) - especially about privacy, autonomy, and equality. Critics claim that facial recognition used in public places on a large scale or in real time may deter people from participating freely in assembly and movement, affecting core democratic freedoms.¹⁷ Presently, the debate is ongoing about the predisposition of “machine bias” to replicate social inequalities and, hence, to expose particular racial or ethnic groups to increased surveillance.¹⁸ The same challenge was pointed out by stating that the weak safeguards around the design of FRT can be a risk to fundamental civil liberties.¹⁹ From these angles, it is evident that the technical errors of the algorithms are the problem, as well as the societal prejudices that come into play when used in conjunction with law enforcement. It is also illustrated that historical racial injustices are likely to form both the development of these technologies and their application.²⁰

The context of law in Europe is primarily revolving around two primary tools. The General Data Protection Regulation (GDPR) classifies biometric data as a sensitive category, restricting its processing unless there is a legitimate basis or explicit exception.²¹ Scholars advocate that GDPR is a great foundational framework for data protection. Still, because of the lawfulness of derogations

¹⁶ Amigo, G.; Perea, P. R.; Marks, R. J., *Mitigating Algorithmic Bias on Facial Expression Recognition*, arXiv preprint, arXiv:2312.15307, 2023, p. 4.

¹⁷ Qandeel, M., *Facial recognition technology: regulations, rights and the rule of law*, *Frontiers in Big Data*, vol. 7, 2024, p. 10–11.

¹⁸ Perkowitz, S., *The Bias in the Machine: Facial Recognition Technology and Racial Disparities*, MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2021, p. 3.

¹⁹ Leslie, D., *op. cit. note 3*, p. 4.

²⁰ Bacchini, F.; Lorusso, L., *Race, again. How face recognition technology reinforces racial discrimination*, *Journal of Information, Communication and Ethics in Society*, vol. 17, no. 3, 2019, p. 2.

²¹ General Data Protection Regulation (GDPR), Art. 9(1), Regulation (EU) 2016/679.

extended to national security or law enforcement, there is a question about consistent implementation.²² Right to transparency, the first and foremost right to “meaningful information” concerning the logic behind automated systems, is one of the most binding problems, often in opposition to the models that own the information and the secrecy surrounding police operations. Some scholars propose that Data Protection Impact Assessments (DPIAs) could help the situation. Yet, the police departments often remain under minimal scrutiny, and thus, the GDPR's regulatory power has been significantly reduced.²³

In addition, the AI Act takes a risk-based approach, including specific biometric monitoring surveillance systems within the “high-risk” category where they have to meet additional requirements.²⁴ In literature, large generative AI and facial recognition are situated under this new regulatory structure, which aims to ensure trustworthy AI while fostering innovation.²⁵ However, opponents counter that they worry about the Act's dependency on internal conformity checks and its narrowed focus on “product safety,” which may give rise to the problems of broader human rights.²⁶ Justification for a specialized law enforcement-oriented regulation would be more helpful and have stricter and enforceable rules than a broad patchwork.²⁷

3.3. Accountability, Enforcement, and Real-World Gaps

The GDPR and the AI Act are both laws that include clauses designed to address algorithmic bias and safeguard fundamental rights; however, practical challenges are often grounds to undermine their effectiveness. Authors claim that real-world implementation of FRT technologies is tricky for them as law programs do not always abide by comprehensive oversight. Law enforcement agencies often claim

²² Brkan, M., *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, International Journal of Law and Information Technology, vol. 27, no. 2, 2019, p. 91, 95–97.

²³ European Data Protection Board, *Guidelines 05/2022*, *op. cit.*, note 7, p. 5–6.

²⁴ Almada, M.; Petit, N., *The EU AI Act: Between Product Safety and Fundamental Rights*, SSRN Electronic Journal, 2022, p. 5–7.

²⁵ Hacker, P.; Engel, A.; Mauer, M., *Regulating ChatGPT and Other Large Generative AI Models*, Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, 2023, p. 1.

²⁶ *Ibid.*, p. 5–7.

²⁷ Raposo, V. L., *op. cit.* note 4, p. 1, 3.

exceptions for public security or trust private-sector partnerships.²⁸ Algorithmic Impact Assessments (AIAs) present a solution to the issue of implementing essential accountability, described as a process involving system developers, end users, and impacted communities who make evaluative standards together.²⁹ There are also advocates of creating "multi-layered explanations," which would meet the data protection regulations already in place and promote a culture of transparency through iteration.³⁰ Still, applying these accountability methods is challenging sometimes. Large organizations struggle with resource constraints and internal structures that are often isolated from each other, which prevents them from carrying out meaningful auditing or risk mitigation before an FRT system launches.³¹ Proponents argue that the vendors are also to be blamed for the problem as they often require intellectual property protection, which is analogous to implementing black-box algorithms that are even less clear to independent evaluators.³² Even though the guidelines exist, several Member States take liberal stands while others do not, resulting in a split-up regulatory network that makes cross-border task forces more complicated. Data governance risks should be considered, requiring broader legal harmonization and uniform enforcement.³³

Policy refinements are necessary to bridge the gap between theory and practice. It is not just a call for higher accuracy but a need for explicitly enforceable standards of FRT adoption. This would demand the standardization of the scope of DPIAs or AIAs to evaluate bias, the obligatory periodic transparent auditing of the autonomous systems deployed, and appropriate redresses for misidentified or discriminated against citizens. These proposals show that this is a multi-level struggle: on the one hand, the police might see FRT as a quick solution to public safety. On the other hand, civil society and legal researchers fear that the contracts

²⁸ https://www.accessnow.org/wp-content/uploads/2022/07/Access-Now-submission-to-the-consultation-on-the-European-Data-Protection-Boards-FRT-for-LEAs-guidelines-05_2022.pdf, 14 February, 2025.

²⁹ Metcalf, J.; Moss, E.; Watkins, E. A.; Singh, R.; Elish, M. C., *Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts*, Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery, New York 2021, p. 735.

³⁰ Kaminski, M. E.; Malgieri, G., *op. cit. note 8*, p. 68, 72–73.

³¹ Ashar, A.; Ginena, K.; Cipollone, M.; Barreto, R.; Cramer, H., *Algorithmic Impact Assessments at Scale: Practitioners' Challenges and Needs*, Journal of Online Trust and Safety, vol. 2, no. 4, 2024, p. 16.

³² Urquhart, L.; Miranda, D., *Policing Faces: The Present and Future of Intelligent Facial Surveillance*, Information & Communications Technology Law, vol. 31, no. 2, 2022, p. 211.

³³ Gültekin-Várkonyi, G., *Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation*, Internet Policy Review, vol. 13, no. 3, 2024, p. 9, 16.

of the present times insufficiently protect individuals' rights in a changing environment of technology.

4. FRT IN EUROPEAN LAW ENFORCEMENT

Facial recognition technology has gained considerable traction among the different police forces across Europe, as some of them are conducting pilot testing, and others are already implementing it in major cities. Despite the law enforcement agencies arguing for its advantages, such as the benefits of suspect identification, time cost, and the provision of more personnel to other areas of safety, the deployments are also a challenge. This section looks into the practical environment of FRT in European policing, analyzes the infrastructure of law governing it, and highlights significant rights implications. In the end, it calls for a uniform that protects rights, assures technological efficiency, and, at the same time, upholds democratic values.

4.1. Technical and Operational Context

European law enforcement agencies have employed FRT to automate finding and matching faces in digital images or real-time video materials. The process converts a face into a distinctive numeric faceprint pattern that can be compared to known reference databases. Since the FRT works on the following lines, a face is first encoded into a faceprint, and afterward, it is compared against known reference databases. At present, the technology witnesses its usage in at least three main scenarios:

1. Real-Time Scanning in Public Spaces

Cameras are widely used in transport hubs, sporting venues, and city centers. They continuously match faces against watch lists of suspects, missing persons, or others. Real-time FRT is generally the most intrusive application because it scans all persons who pass through the facility's entrance, whether they know this fact or not, and tries to match them in just a few seconds. FRT professionals usually call this model "1:N" or "one-to-many" matching, because it checks one unknown face against an entire database of known faces.³⁴

2. Retrospective (Post-Incident) Analysis

Investigators have used CCTV cameras to extract still frames of unknown individuals after they commit a crime and then submit them for comparison against

³⁴ European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, FRA Focus Paper, 2019, p. 10–14.

national or EU-wide criminal databases. This method was used in the case *R. (Bridges) v. South Wales Police*, in which retrospective scanning was subject to legal scrutiny for compliance with data protection and human rights standards.³⁵

3. Mobile On-the-Spot Checks

Some agencies are testing a system in which police officers use smartphones or tablets to capture a suspect's face in the field and cross-reference it with police records to verify the suspect's identity. It might seem narrow in scope, but if used without the provision strictly for its purposes, it can again become an abuse.³⁶ While FRT can speed up the process of suspect identification, technical audits reveal that it is often more difficult with women, ethnic minorities, children, and older adults. Although the FRT systems usually offset errors as false positives (wrong matches) or false negatives (missed matches) in these groups, FRT machines have been observed to struggle with these issues at higher levels. Even one use of a single person of 'false positive' can, in the eyes of society, lead to the establishment of unreasonable acts or arrests and discrimination based on that intervention.³⁷

4.2. Fragmented Regulatory Framework

European law enforcement agencies use facial recognition technology based on fragmented regulations. No single, consistent one provides specific solutions for processing large-scale biometric data, which is a unique problem. Three main pillars are the GDPR, the Law Enforcement Directive (LED), and the AI Act. Although each has different provisions, the sum is partial and contradictory, which leaves considerable room for divergent practices among Member States.

4.2.1. The GDPR's Approach to Biometric Data

Facial data constitutes a sensitive personal data category and it stands as a special category under the GDPR, which notes that biometric data reveals a person's unique identifiers and is especially sensitive and subject to elevated protection.³⁸ As a rule, the Regulation prohibits processing such data unless it is strictly

³⁵ *Bridges v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058, Court of Appeal (Civil Division), United Kingdom.

³⁶ House of Commons Science and Technology Committee, *The Work of the Biometrics Commissioner and the Forensic Science Regulator*, HC 1970, 6 February, 2019

³⁷ Grother, P.; Ngan, M.; Hanaoka, K., *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*, National Institute of Standards and Technology, NIST IR 8280, Gaithersburg 2019, p. 5.

³⁸ Brkan, M., *op. cit.* note 22, p. 2.

necessary and there is a proper legal basis. Article 9 introduces very stringent conditions for processing sensitive data, and Recital 51 in particular, talks about the considerable risks from biometric technology such as FRT. Generally, police or other public bodies cannot make systematic public space face scans simply because they perceive it is a public good. Apart from what the law requires, they must observe the GDPR's preconditions of necessity and proportionality; the measure should be the only way to fulfill the aim and not be more intrusive than necessary.³⁹ The reality is that, apart from being busy with travelers and consumers, cameras at these events can take snaps of all left aside people, which might trigger questions regarding whether such wide-scale capture corresponds with the GDPR mandate of data minimization. Strangers outside the target group cannot consent to the scanning or opt-out. Observers raise this argument by saying that even though the FRT system would discard the samples of bystanders immediately, temporally stored information or partial data storage might contravene the GDPR unless there is a definite time, a narrow scope, or a specific law enforcement aim. Concerns also emerge from GDPR's transparency rules: police typically do not notify thousands of tourists in real-time or provide them with an easily accessible way of challenging processing.

4.2.2. The LED and Criminal Justice Data

Directive (EU) 2016/680, commonly known as the Law Enforcement Directive (LED), was adopted concurrently with the GDPR and acts as a framework governing personal data handling by law enforcement bodies.⁴⁰ Like the GDPR, it restates the main principles, such as accuracy and accountability, but instead emphasizes crime prevention and prosecution goals. Integrating the Directive into different national legislations by Member States takes diverse forms. A few jurisdictions enforce strict oversight while communities are left in the dark about security measures taken, as others engage the police under broadly defined “public security” or “national security” laws.⁴¹ As a consequence of the abovementioned phenomenon, significant practical disparities exist. Police service in one Member State may be compelled to do a complete data protection impact assessment and need pragmatic consent from a supervisory authority before initiating real-time scanning. At the same time, a different one might see the LED as granting them

³⁹ Kaminski, M. E.; Malgieri, G., *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations*, International Data Privacy Law, vol. 11, no. 2, Oxford University Press, 2021, p. 130, suggesting strict necessity as a key threshold for large-scale biometric data gathering.

⁴⁰ Gültekin-Várkonyi, G., *op. cit.* note 33, p. 3.

⁴¹ *Ibid.*, p. 16.

broad rights to use the system almost indefinitely with no required outside accountability. Causing legal uncertainty also cleaves cross-border cases or big cities dreaming of attracting international mobility like airport hubs or major rail traffic lines. The initiation of new policing technologies without a consistent framework for managing face-derived biometric data further weeds the field in which FRT is field-tested and installed.

4.2.3. The AI Act

In 2021, the European Parliament appeared with a proposal for an Artificial Intelligence Act that aims to end the “high-risk” AI applications, such as those based on remote biometric identification.⁴² Earlier drafts proposed ruling out real-time FRT in public places as generally incompatible with fundamental rights. But from the beginning, the discussions have been over the possible exemptions such as those for serious or organized crime, anti-terror operations, and other “public security” concerns. If the exemptions are adopted broadly, they might neutralize the protective character of the law. The key feature of this Act is that it will focus on transparency, accountability, and accuracy testing. However, civil society coalitions protest that real-time scanning will not be complex to deal with theoretical questions without obligatory conditions and external checks.⁴³ Another pivotal aspect is the interplay between the Act's enforcement and existing data protection authorities. If the latter are confined to narrower data oversight, then it is likely that “high-risk” FRT systems avoid proper scrutiny.⁴⁴ It might seem as if law enforcement's needs are more important than the European Union's desire to ensure an ethical and human rights-compatible AI.

4.2.4. Centralized EU Oversight

A practical route out of this patchwork might be a centralized EU oversight model built around EDPB and ADPS. Under proposals advanced in Joint Opinion 5/2021 on AI Act, every law-enforcement FRT system would be entered in EU-wide registry managed by two bodies and deployment would require:

- 1) A Data-Protection Impact Assessment and Algorithmic Impact Assessment submitted for ex-ante clearance,

⁴² Almada, M.; Petit, N., *op. cit. note 24*, p. 4–7, 25, referencing parallels between broad national security arguments and AI-based procedures.

⁴³ Leslie, D., *op. cit. note 3*, p. 22.

⁴⁴ Almada, M.; Petit, N., *op. cit. note 24*, p. 22.

- 2) Conformity assessment and post-market monitoring supervised by the future EU AI Office (Art. 63 AI Act),
- 3) Ongoing publication of demographic performance metrics enabling cross-border comparison⁴⁵

EDPB's final Guidelines 05/2022 on FRT in Law Enforcement include procedural template with obligatory DPIAs, independent accuracy testing and periodic audits.

4.2.5. National Security

Often, law enforcement officials argue that extensive video surveillance is due to public security as a reason for such things. According to Article 2(2)(d) GDPR, "activities concerning national security" can be considered outside its perimeter, while LED Article 2 rather excludes certain operations for the sake of national security itself. The danger is that police may classify crowd scanning using FRT technology as one of the national security matters and hence evade to be examined. This modality ends up in a lack of accountability, where neither data protection authority nor ordinary administrative oversight can adequately supervise the processes regarding the deployment of the biometric register.

4.2.6. Consequences of the Patchwork

Notwithstanding the worldwide admiration that Europe has in regard to its data protection laws, the simultaneous operation of the GDPR, LED, and the unresolved AI Act make it a patchwork legal system. According to the norm, the GDPR's requirement for strict necessity and the LED's focus on purpose limitation should, in principle, negate broad, real-time face scanning. Practically speaking, the agencies usually claim that "public security" and "national security" entitlements permit them to analytically deploy the systems with ex-ante review. The responses of the authorities are diverse, as some local governments and courts take action by prohibiting partially or calling for robust assessments of the impacts on data protection. Others, however, concentrate on projects that they justify by a timely projected security fraction that defies concerns about privacy or bias. This lack of coherence makes it even more challenging to enforce the law across borders, as different states have different thresholds for what counts as a necessary and proportional response.

⁴⁵ https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, 7 February, 2025.

The subjects of bias, transparency, and redress remain unresolved. If an FRT system wrongly tags someone as a suspect, the maze of legal instruments does not provide a clear guide for the individual to prove the role of facial matching in his police action or in any other way to rectify the in- pursued information. Critics maintain that these accountability gaps not only arise from mere general-purpose data protection guidelines but are rather a necessity for specific regulations of the FRT domain, which have to be built on a solid foundation of auditing, thorough demographic tests, and accessible complaints and redress mechanisms.

5. IMPLICATIONS FOR RIGHTS AND FREEDOMS

Despite the efficiency benefits, FRT's proliferation may also endanger some of the European Union's essential human rights, such as privacy, anti-discrimination, freedom of expression and assembly, and effective redress.

5.1.1. Privacy and Data Protection

FRT in public places permanently undercuts the sense of anonymity in daily life. The Court of Justice of the EU (CJEU) has repeatedly expressed that personal data being retained broadly and without discrimination is presumptively unfair.⁴⁶ Real-time identification in a central area could mean that people are being “mass identified” as a group, with vast amounts of facial data collected from unknown passersby. Although non-matching data is discarded after a short while, the practice, in its essence, changes the old paradigm of “being in public.” The main questions pertain to how police officers can prove strict necessity and proportionality criteria, as stipulated in ECHR Article 8 and EU Charter Article 7.⁴⁷

5.1.2. Accuracy, Bias, and Non-Discrimination

Empirical evaluations, including audits by the U.S. National Institute of Standards and Technology (NIST), show that error rates are systematically higher for specific demographic groups.⁴⁸ Within Europe, various pilot projects - such as the one in

⁴⁶ *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12), EU:C:2014:238.

⁴⁷ *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (C-311/18), EU:C:2020:559, 16 July, 2020.

⁴⁸ Buolamwini, J.; Gebru, T., *op. cit.* note 2, p. 3, 10.

the UK - demonstrated that Black and Asian individuals have been unfairly represented in the false positive statistics. This type of deviation does not align with the fundamental principle of equal treatment in Article 21 of the Charter. An algorithm that marks a large part of the minority citizens who are not culpable of any crime as potential suspects can convert the existing biases of the police into a high-tech feedback loop in the form of real-time FRT. On the other hand, several authorities are not obligated to calculate the demographic error rates and publish information concerning them.

5.1.3. Freedom of Assembly and Expression

Public demonstrations and the right to spontaneous protests sustain the inhibitory effect of the public on the citizens' democracy.⁴⁹ Individuals who realize that their faces might be scanned and logged decide not to participate in the marches or gatherings, which then affects the country's civic life. ECHR Article 11 protects peaceful assembly rights, but it will be very troublesome if law enforcement knows each demonstrator and they can even match with the list of the security files; this could lead to unimaginable harm. The opposers claim that real-time FRT is rarely the only option for keeping order, and they suggest other more proportionate ways, like using non-intrusive crowd management tactics.

5.1.4. Accountability and Redress

Part of democracy in policing is individuals making complaints regarding wrongful stops or arrests. If FRT was the technology used to justify the intervention, achieving fair means becomes impossible if the matching algorithm is regarded as proprietary or "highly technical."⁵⁰ Thus, this inconsistency is a deterrent to the fairness principle enshrined in EU data protection law. In 2020, the UK Court of Appeal, the aforementioned *R. (Bridges) v. South Wales Police* brought to notice the "lack of adequate guidance" on the technology's usage and, therefore, the demand for more explicit patrolling rules. Many European police forces, in contrast, still refrain from going public on crucial operational details (e.g., watch-list composition, match thresholds). False matches can still be hidden from the public without thorough auditing and the availability of a remedy process.

⁴⁹ Commissioner for Human Rights of the Council of Europe, *2nd Quarterly Activity Report 2022, 1 April to 30 June*, CommDH(2022)25, Strasbourg 2022.

⁵⁰ Selbst, A. D.; Boyd, D.; Friedler, S. A.; Venkatasubramanian, S.; Vertesi, J., *Fairness and Abstraction in Sociotechnical Systems*, Proceedings of the 2019 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery, New York 2019, p. 59–60, analyzing "black-box" issues in machine-learning algorithms.

5.2. The road to cohesive governance

Regions with solid data protection traditions face challenges that may be either not addressed or not responded to through standard regulatory channels. The fact that many law enforcement actions are taken under exceptions related to national security or significant crime creates a daunting oversight authority, which cannot impose practical limitations or gain the transparency to examine operational details. The existence of extended pilots without any time limit is a model of how public acceptance may be engendered or forced by using the vague term "crime reduction," leaving the individuals wrongly tagged without legal recourse.

Observers suggest some reforms. First, stronger accountability should control the special agencies so that they regularly conduct bias and performance tests, and the results are subject to an external audit. Second, rules on ex-ante approvals by an independent court or data protection regulator will ensure that the public never sees real-time scanning unless done under specific, proportionate, and strictly limited conditions.⁵¹

As long as the plan is still not firmly in place, local or national-level bans or partial freezes may be the best and only shield against the unfettered expansions of FRT. Problems worsen as time goes by with no clear EU-wide or national framework. Hence, the inequality grows with law enforcement agencies or private vendors taking the lead in the regulatory vacuum, which is only loosely covered by fundamental rights. Whether a stricter approach - for example, the overall ban on real-time scanning - will lead the scene depends on ongoing discussions and the value that the courts confer on privacy, equality, and transparency in a democratic society. The powerful capacity FRT has to turn policing inside out is a torment for lawmakers, data protection bodies, and judicial authorities. This means they have a parallel duty to make sure that the fundamental rights do not become collateral damage due to technological advancement.

It is worth it to notice emphasize that the use of Facial Recognition Technology may have demonstrable public-safety gains. The UK Home Office argues that FRT "quickly and accurately identify those wanted for serious crimes as well as missing

⁵¹ Oliveira, A. M. de; Rodrigues, H. X.; Nery, A. S.; Mendonça, F. L. L. de; Ribeiro Junior, L. A., *Influence of Racial Bias in the Use of Facial Recognition Applied to Access Control: A Critical Analysis*, Research, Society and Development, vol. 14, no. 2, 2025, p. 11.

or vulnerable people. It also frees up police time and resources".⁵² South Wales Police report that their deployments of FRT facilitated 61 arrests for a robbery, violence and outstanding warrants without a single unlawful arrest.⁵³

6. RECOMMENDATIONS

The increasing dependence on facial recognition technology by law enforcement throughout Europe is a clear indication of the immediate need for a rights-oriented and coherent regulatory system. Although the General Data Protection Regulation, the Law Enforcement Directive, and the AI Act contribute with partial controls, the result is a patchwork solution that does not address several key risks that the technology poses during its implementation. The chapter identifies the proposals that are meant to ensure the balance between legitimate policing purposes and the fundamental principles of fairness, transparency, and non-discrimination.

One of the pivotal measures is the improvement of algorithm transparency. Research have shown that FRT is frequently characterized by exhibiting elevated error rates for certain demographic groups, however, it is rare for it to be mentioned in public reports. Legislators and data protection supervisory authorities should make it mandatory for police agencies to publish demographic performance metrics for every FRT system they have deployed (or disclose the same to a supervisory body). This approach would correspond to the arguments raised by scholars who accentuate the importance of systematic evaluations of face recognition accuracy across different demographic variables, consequently making biases visible and subject to remedy.⁵⁴ If these demographic results reveal consistent false-match spikes for certain populations, agencies would have to adopt specific mitigations - such as enhanced training data diversity or adjustment of algorithmic thresholds. Furthermore, official guidelines could potentially require law enforcement to perform continuous "field condition" audits, which underlines the fact that real-life performance often varies from the controlled laboratory tests.

The second critical goal is that the legal grounds for FRT usage must be set in clearly defined and limited terms. Even if the GDPR and LED demand necessity

⁵² <https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/>, 9 February, 2025.

⁵³ <https://www.south-wales.police.uk/news/south-wales/news/2023/abr-apr/commitment-facial-recognition-technology-reaffirmed-report-tech-does-not-breach-equality-requirements>, 28 January, 2025.

⁵⁴ Liang, H.; Perona, P.; Balakrishnan, G., *op. cit. note 1*, p. 1, 8.

and proportionality conditions, it is pointed out that many current deployments are dependent on general allusions to public security or serious crime prevention, allowing, in some cases, real-time scanning of the public without any bounding limits and with no or less-than-usual pre-assessment. A more careful legal arrangement would compel agencies to give exact location-situated time-restricted justifications for not permitting specific live scanning. Real-time FRT is the least intrusive and most justifiable when used for a short period, so the operations are critical. Indefinite or "always-on" scanning in public spaces poses a risk of breaching proportionality and data minimization, as always-on scanning would be against respect toward people and their data. Courts or data protection authorities not being independent could also be used to oversee this authorization process, just as judges do when they issue warrants for other sensitive surveillance actions.

Besides its transparent technology, every facial recognition application should also ensure that people who are wrongly identified are entitled to adequate redress. Right now, the victims of FRT systems misidentification find out too late, if at all, that their match was automated and, therefore, triggered the police traffic stop. The "Black box" nature of proprietary algorithms makes it difficult to challenge the unequal outcomes of any such systems. Law enforcement should be compelled to state how their use of FRT in any police stop is pivotal; in addition to this, they are to offer formal access to the procedures that could be used to correct or wipe erroneous face-match logs, thus upholding the fairness and accuracy which the LED demands. If feasible, FRT vendors can be made to agree to allow at least some expert external tech audits.

To create uniformity in these measures across Europe, the suggested AI Act might outline uniform standards and regulations for law enforcement targeting FRT's "high-risk" usage. It would explicitly state that collective public real-time scanning is allowed only under exceptional and specific conditions. Algorithmic impact assessments should be permanently embedded into the project, ensuring that biases and adverse impacts are identified and acted on before the FRT systems are operational.⁵⁵

Lastly, the European Data Protection Board and Member State data authorities can set up a centralized registry listing all the approved FRT systems in the law enforcement sector, and each of them will have their watch list criteria, accuracy metrics, and operational limits specified. This registry, managed jointly by national and EU regulators, would be the perfect remedy to cases of agencies operating facial recognition tech unnoticed by data protection supervisors. A consistent framework established for data sharing and oversight will eliminate the situation

⁵⁵ Metcalf, J., et. al, *op. cit.*, note 29, p. 735–736.

where law enforcement might exploit lenient jurisdictions to test or operationalize experimental FRT solutions.⁵⁶

7. CONCLUSION

The summary of the previous chapters is the remarkable increase in the use of FRT in European law enforcement, its changing operations in policing, and the legal frameworks that aim to protect the rights of individuals and fundamental values. Researchers illustrate that machine learning is not just a copy of the existing societal biases but can also worsen them if some demographic categories are missing or are wrong in the training datasets.⁵⁷ A single technical shortfall in an FRT algorithm can be translated into police contexts, which can promote the wrong arrests or profiling. At the same time, these technical aspects connect to a divided regulatory framework, where the GDPR, the Law Enforcement Directive, and the AI Act overlap but do not present a genuinely uniform, comprehensive regime.

A core concern is that law enforcement usually utilizes broad security targets to validate scanning entire populations - frequently with little demonstration of strict necessity and proportionality and possibly initiate an EU data protection principles breach, which requires narrow and definite uses of sensitive biometric data specifically. When real-time scanning becomes a regular activity in public life, Europeans might lose the anonymity usually linked with their freedom of movement; whether people will retain their strong civil liberties in a culture with almost all electronic identities is now crucial.

One of the main purposes of the AI Act is to qualify remote biometric identification as a high-risk, and even unacceptable practice that has to be subjected to audits or even completely prohibited at times in public places. However, security exemptions may well become the reason these protective provisions do not work, leaving law enforcement almost without any limits. The reasonable solution might be a more practical position that real-time scanning operations should not be used except in extraordinary cases, which should be for a limited period and only upon the approval of a judge or an impartial third party. In absence of a thorough, coherent system of checking, the local pilot projects can easily turn into a long-term status of continuous scanning across the entire city.

⁵⁶ Gültekin-Várkonyi, G., *op. cit. note 33*, p. 21–22,

⁵⁷ Liang, H.; Perona, P.; Balakrishnan, G., *op. cit. note 1*, p. 2.

Meanwhile, the attempts at bias reduction in FRT are often tied to improving datasets or using more advanced auditing methods like algorithmic impact assessments (AIAs). They indeed have good prospects, not the least because the empirical evidence suggests that slight changes to the proposal, like increased demographic balance in training data, can yield better accuracy rates for groups that are usually disregarded. Yet, the underutilization of performance metrics on the agencies' info handout is the leading direct cause of the relationship stalks, as the agencies cite the fear of getting attacked by the public or of revealing the investigative methodology as the reason for withholding the real-time numbers.

As the focal point, it is of paramount importance to develop a multifaceted plan. To begin with, the agencies must disclose demographic performance metrics, which will be subjected to third-party verification. They thus must restrict the general population scanning to genuinely urgent situational contexts. Watch-list criteria and retention of policies that allow for their independent audit would also make it possible for data protection bodies to establish whether FRT systems are operated in a reasonably proportional way with the threat. Leaps towards this goal will also involve the realization that accountability should be end-to-end, thus providing easy and straight solutions for wrongfully identified or profiled individuals. Courts and data protection authorities will have a decisive role by imposing the law enforcement agencies to include stringent transparency provisions within their procurement contracts and system rollouts.

Creating a coherent regulatory framework, Europe would stand on the one hand with FRT's development and on the other upholding their values of human dignity, privacy, and non-discrimination by including elements such as tighter rules on real-time scanning, thorough auditing of algorithmic performance, mandatory DPIAs or AIAs, and transparent watch-list management. Failing this would risk normalizing a greatly intrusive policing environment, decaying public trust, and eroding the fundamental rights that form the basis of European law. The advancements regarding the AI Act and the GDPR, and LED, which will continue to shape law enforcers' data processing, should form a coherent governance model, which is desired and needed. A society in which FRT genuinely serves security needs without perpetuating injustices is only feasible by having such robust guarantees, accompanied by a renewed pledge to transparency and algorithmic accountability.

REFERENCES

BOOKS AND ARTICLES

1. Access Now, *Submission to Consultation on EDPB's Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 2023.
2. Almada, M.; Petit, N., *The EU AI Act: Between Product Safety and Fundamental Rights*, Social Science Research Network, 2022.
3. Aloisi, A.; De Stefano, V., *Between risk mitigation and labour rights enforcement: Assessing the transatlantic race to govern AI-driven decision-making through a comparative lens*, Social Science Research Network, 2023.
4. Almeida, D.; Shmarko, K.; Lomas, E., *The Ethics of Facial Recognition Technologies, Surveillance and Accountability in an Age of Artificial Intelligence: A Comparative Analysis of USA, EU and UK Regulatory Frameworks*, Social Science Research Network, 2021.
5. Ashar, A.; Ginena, K.; Cipollone, M.; Barreto, R.; Cramer, H., *Algorithmic Impact Assessments at Scale: Practitioners' Challenges and Needs*, Journal of Online Trust and Safety, 2024.
6. Atay, M.; Poudyel, M.; Evora, S., *Evaluation of Gender Bias in Masked Face Recognition with Deep Learning Models*, IEEE Symposium Series on Computational Intelligence, 2023.
7. Bacchini, F.; Lorusso, L., *Race, Again: How Face Recognition Technology Reinforces Racial Discrimination*, Journal of Information, Communication and Ethics in Society, 2019.
8. Binns, R.; Adams-Prassl, J.; Kelly-Lyth, A., *Legal Taxonomies of Machine Bias: Revisiting Direct Discrimination*, Conference on Fairness, Accountability and Transparency, 2023.
9. Blacklaws, C., *Algorithms: transparency and accountability*, Philosophical Transactions of the Royal Society A, 2018.
10. Brkan, M., *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, International Journal of Law and Information Technology, 2019.
11. Brown, S.; Davidović, J.; Hasan, A., *The algorithm audit: Scoring the algorithms that score us*, Big Data & Society, 2021.
12. Buolamwini, J.; Gebru, T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, FAT, 2018.
13. Casaburo, D.; Marsh, I., *Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: the ALIGNER Fundamental Rights Impact Assessment*, AI and Ethics, 2024.

14. Castets-Renard, C., *Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making*, Fordham Intellectual Property, Media & Entertainment Law Journal, 2019.
15. Fortes, P. R. B.; Baquero, P. M.; Amariles, D. R., *Artificial Intelligence Risks and Algorithmic Regulation*, European Journal of Risk Regulation.
16. Gilman, M. E., *Five Privacy Principles (from the GDPR) the United States Should Adopt to Advance Economic Justice*, 2020.
17. Goodman, B.; Flaxman, S. R., *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, AI Magazine, 2017.
18. Grother, P.; Ngan, M.; Hanaoka, K., *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Standards and Technology, 2019.
19. Gültekin-Várkonyi, G., *Navigating data governance risks: Facial recognition in law enforcement under EU legislation*, Internet Policy Review, 2024.
20. Gültekin-Várkonyi, G., *Predictive Policing and Bias in a Nutshell: Technical and Practical Aspects of Personal Data Processing for Law Enforcement Purposes*, Social Science Research Network, 2022.
21. Gürsoy, F.; Kennedy, R.; Kakadiaris, I. A., *A Critical Assessment of the Algorithmic Accountability Act of 2022*, Social Science Research Network, 2022.
22. Hacker, P.; Engel, A.; Mauer, M., *Regulating ChatGPT and other Large Generative AI Models*, Conference on Fairness, Accountability & Transparency, 2023.
23. Hildebrandt, M., *Algorithmic regulation and the rule of law*, Philosophical Transactions of the Royal Society A, 2018.
24. Kaminski, M. E.; Malgieri, G., *Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR*, FAT, 2020.
25. Kaminski, M. E.; Malgieri, G., *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations*, International Data Privacy Law, vol. 11, no. 2, Oxford University Press, 2021, p. 130.
26. Kang, S. S., *Algorithmic accountability in public administration: the GDPR paradox*, FAT, 2020.
27. Kelly-Lyth, A., *Challenging Biased Hiring Algorithms*, Oxford Journal of Legal Studies, 2021.
28. Kouroupis, K., *The AI Act in light of the EU Digital Agenda: A critical approach*, Journal of Data Protection & Privacy, 2023.
29. Kun, E., *Exploring the Role of Data Protection Impact Assessments in the Use of Facial Recognition Technologies: From Accountability to Meta-Regulation*, Social Science Research Network, 2022.
30. Kuśmierczyk, M., *Algorithmic Bias in the Light of the GDPR and the Proposed AI Act*, Social Science Research Network, 2022.

31. Laux, J.; Wachter, S.; Mittelstadt, B., *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, Regulation & Governance, 2023.
32. Leslie, D., *Understanding Bias in Facial Recognition Technologies*, Social Science Research Network, 2020.
33. Liang, H.; Perona, P.; Balakrishnan, G., *Benchmarking Algorithmic Bias in Face Recognition: An Experimental Approach Using Synthetic Faces and Human Evaluation*, IEEE International Conference on Computer Vision, 2023.
34. Limantè, A., *Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*, Nordic Journal of Human Rights, 2023.
35. Malgieri, G., *Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations*, International Data Protection Law, 2019.
36. Metcalf, J.; Moss, E.; Watkins, E. A.; Singh, R.; Elish, M. C., *Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts*, Proceedings of FAccT, 2021.
37. Mobilio, G., *Your face is not new to me – Regulating the surveillance power of facial recognition technologies*, Internet Policy Review, 2023.
38. Mökander, J.; Axente, M.; Casolari, F.; Floridi, L., *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, Minds and Machines, 2021.
39. Mökander, J.; Floridi, L., *From algorithmic accountability to digital governance*, Nature Machine Intelligence, 2022.
40. Mökander, J.; Juneja, P.; Watson, D. S.; Floridi, L., *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?*, Minds and Machines, 2022.
41. Mundim De Oliveira, A.; Rodrigues, H. X.; Nery, A. S.; Mendonça, F. L. L.; Ribeiro Júnior, L. A., *Influence of racial bias in the use of facial recognition applied to access control: A critical analysis*, Research, Society and Development, 2025.
42. Neroni Rezende, I., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, The New Journal of European Criminal Law, 2020.
43. Njoto, S.; Cheong, M.; Frermann, L.; Ruppner, L., *Bias and Discrimination Against Women and Parents in Semi-Automated Hiring Systems*, New Technology, Work and Employment, 2024.
44. Nesterova, I., *Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance*, Information Polity, 2022.
45. Perkowitz, S., *The Bias in the Machine: Facial Recognition Technology and Racial Disparities*, 2021.

46. Qandeel, M., *Facial recognition technology: regulations, rights and the rule of law*, Frontiers Big Data, 2024.
47. Raposo, V. L., *The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal*, European Journal on Criminal Policy and Research, 2022.
48. Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, International Convention on Information and Communication Technology, Electronics and Microelectronics, 2022.
49. Sanz Urquijo, B.; Fosch-Villaronga, E.; López Belloso, M., *The disconnect between the goals of trustworthy AI for law enforcement and the EU research agenda*, AI and Ethics, 2022.
50. Selbst, A. D. et al., *Fairness and Abstraction in Sociotechnical Systems*, Proceedings of the Conference on Fairness, Accountability, and Transparency, 2019, pp. 59–68.
51. Shenkman, C.; Thakur, D.; Llans'o, E., *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis*, arXiv.org, 2021.
52. Shumilo, O.; Kerikmäe, T., *The European Approach to Building AI Policy and Governance: A Haven for Bureaucrats or Innovators?*, IDP Revista de Internet Derecho y Política.
53. Siapka, A., *The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI*, 2018.
54. Sumsion, A. W.; Torrie, S. A.; Lee, D.; Sun, Z., *Surveying Racial Bias in Facial Recognition: Balancing Datasets and Algorithmic Enhancements*, Electronics, 2024.
55. Szostek, D., *Is the Traditional Method of Regulation (the Legislative Act) Sufficient to Regulate Artificial Intelligence, or Should It Also Be Regulated by an Algorithmic Code?*, Białostockie Studia Prawnicze, 2021.
56. Treleaven, P.; Barnett, J.; Koshiyama, A. S., *Algorithms: Law and Regulation*, IEEE Computer, 2019.
57. Tsamados, A.; Aggarwal, N.; Cows, J.; Morley, J.; Roberts, H.; Taddeo, M.; Floridi, L., *The Ethics of Algorithms: Key Problems and Solutions*, AI & Society, 2020.
58. Urquhart, L. D.; Miranda, D., *Policing faces: the present and future of intelligent facial surveillance*, Information & Communications Technology Law, 2021.
59. Veale, M.; Brass, I., *Administration by Algorithm? Public Management Meets Public Sector Machine Learning*, 2019.
60. Wachter, S.; Mittelstadt, B.; Russell, C., *Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI*, Computer Law & Security Review, 2021.

61. Whittlestone, J.; Nyrupe, R.; Alexandrova, A.; Cave, S., *The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions*, AAAI/ACM Conference on AI, Ethics, and Society, 2019.
62. Williams, R., *Rethinking Administrative Law for Algorithmic Decision Making*, Oxford Journal of Legal Studies, 2021.
63. Yeung, K., *Algorithmic regulation: A critical interrogation*, Regulation & Governance, 2018.
64. Yeung, K.; Lodge, M., *Algorithmic regulation: an introduction*, Social Science Research Network, 2019.
65. Zouave, E. T.; Marquenie, T., *An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling*, European Intelligence and Security Informatics Conference, 2017.

LEGAL ACTS

1. General Data Protection Regulation (GDPR), 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, OJ L 119, 4/5/2016.
2. Artificial Intelligence Act (AI Act), Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.
3. Directive (EU) 2016/680 (Law Enforcement Directive - LED), 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, OJ L 119, 4/5/2016.
4. Council Directive (EU) 2016/1164, of 12 July 2016 laying down rules against tax avoidance practices directly affecting the functioning of the internal market, OJ L 193, 19/07/2016.

LEGISLATIVE MATERIALS

1. Council of Europe's Commissioner for Human Rights, *Safeguarding Freedom in the Digital Age*, CommDH(2022)2.
2. Commissioner for Human Rights of the Council of Europe, *2nd Quarterly Activity Report 2022, 1 April to 30 June*, CommDH(2022)25, Strasbourg 2022.

3. EDPB, *Guidelines on Facial Recognition Technology in Law Enforcement*, 2022.
4. European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, Brussels 2020.
5. European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, adopted on 26 April, 2023.
6. European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, FRA Focus Paper, 2019, p. 10–14.

COURT DECISIONS

1. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12), EU:C:2014:238.
2. *Bridges v. Chief Constable of South Wales Police* [2020] EWCA Civ 1058, Court of Appeal (Civil Division), United Kingdom.
3. *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems* (C-311/18), EU:C:2020:559.

NETWORK RESOURCES

1. Amigo, G. A.; Rivas-Perea, P.; Marks, R. J., "Mitigating Algorithmic Bias on Facial Expression Recognition," arXiv.org (2023), <https://arxiv.org/abs/2303.11780>.
2. https://www.accessnow.org/wp-content/uploads/2022/07/Access-Now-submission-to-the-consultation-on-the-European-Data-Protection-Boards-FRT-for-LEAs-guidelines-05_2022.pdf.
3. https://www.edpb.europa.eu/our-work-tools/our-documents/edpbbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en, 7 February, 2025.
4. <https://homeofficemedia.blog.gov.uk/2023/10/29/police-use-of-facial-recognition-factsheet/>, 9 February, 2025.
5. House of Commons Science and Technology Committee, The Work of the Biometrics Commissioner and the Forensic Science Regulator, 6 February 2019, HC 1970, <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/1970.pdf>.

6. <https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>, 11 February, 2025.
7. <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>, 14 February, 2025.
8. <https://www.south-wales.police.uk/news/south-wales/news/2023/abr-apr/commitment-facial-recognition-technology-reaffirmed-report-tech-does-not-breach-equality-requirements>, 28 January, 2025.
9. <https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurting-towards-surveillance-state>, 11 February, 2025.