

Facial Recognition Technology and the Right to Privacy: Legal and Constitutional Challenges in the Digital Era

Dr. Amelia Johnson¹

¹ School of Law and Technology, University of Manchester, United Kingdom.

Received: 18 Oct 2025 **Revised:** 28 Nov 2026 **Accepted:** 28 Jan 2025 **Published:** 28 Feb 2026

ABSTRACT

Facial recognition technology has emerged as a powerful artificial intelligence-based tool for identification, authentication, surveillance, border management, policing, and commercial services. Its increasing deployment has generated significant legal and constitutional concerns concerning privacy, data protection, individual autonomy, discrimination, surveillance, and procedural safeguards. Unlike conventional identification mechanisms, facial recognition can potentially identify individuals without their active participation or awareness, creating new possibilities for large-scale monitoring. This article examines the legal and constitutional implications of facial recognition technology with particular emphasis on the right to privacy, informational self-determination, consent, proportionality, and state surveillance. It argues that the deployment of facial recognition technology should be subject to clear legal authorization, necessity and proportionality requirements, transparency, independent oversight, and effective remedies. The article further considers the risks associated with algorithmic bias and inaccurate identification, particularly in law-enforcement contexts. It proposes a rights-based regulatory framework designed to balance legitimate technological and security objectives with constitutional protections. The study concludes that technological efficiency cannot by itself justify unrestricted biometric surveillance and that meaningful legal safeguards are essential for preserving privacy and individual liberty.

Keywords: Facial recognition; Right to privacy; Artificial intelligence; Biometric data; Constitutional law; Data protection; Surveillance.

© 2026. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Artificial intelligence has increasingly become integrated into everyday social, commercial, and governmental activities. Among the technologies attracting significant legal attention is facial recognition technology (FRT), which uses computational systems to analyze facial characteristics and compare them against stored or available information. Facial recognition can be used for identity verification, access control, financial authentication, airport security, policing, border management, attendance systems, and commercial personalization.

The technology offers several potential benefits. It can assist law-enforcement agencies in identifying suspects, help organizations prevent identity fraud, facilitate secure authentication, and improve access-control systems. However, these advantages must be considered alongside the possibility of intrusive surveillance and misuse of biometric information.

The legal significance of facial recognition arises primarily from the nature of facial information itself. Unlike a password, facial characteristics cannot ordinarily be replaced once compromised. Biometric information can therefore create long-term privacy implications. Furthermore, facial recognition systems may operate without the knowledge or active participation of the person being identified.

The possibility of identifying individuals in public spaces creates an important constitutional question: to what extent should the state or private organizations be permitted to monitor individuals through automated biometric technologies?

This question becomes particularly significant in democratic societies where privacy, dignity, liberty, and equality are protected through constitutional or human-rights frameworks. The challenge is to develop a legal framework that permits legitimate technological applications while preventing disproportionate surveillance.

This article examines facial recognition through the lens of privacy and constitutional law. It focuses on biometric data protection, consent, surveillance, proportionality, algorithmic bias, accountability, and remedies.

2. Understanding Facial Recognition Technology

Facial recognition technology generally involves capturing an image or video of an individual's face, extracting distinguishing facial characteristics, converting those characteristics into a mathematical representation, and comparing the resulting representation with one or more stored templates.

Two broad applications can be distinguished: **facial verification** and **facial identification**.

Facial verification generally asks whether an individual is the person they claim to be. For example, a system may compare a person's face with an image previously associated with that person's account.

Facial identification involves determining who an individual is among a larger database of potential identities. This application creates greater privacy concerns because individuals may be identified without voluntarily presenting credentials.

Facial recognition systems may also be deployed in real-time surveillance environments. Cameras can continuously capture individuals in public spaces and automatically compare their facial characteristics against watchlists or databases.

The legal implications depend significantly on the purpose, scale, accuracy, retention period, and institutional context of deployment.

3. The Right to Privacy

Privacy is a fundamental legal interest that protects individuals from unjustified interference with their personal lives and autonomy. Modern privacy law increasingly recognizes that privacy is not limited to physical spaces. It also encompasses control over personal information and protection against unauthorized collection and processing.

Facial recognition raises unique privacy concerns because biometric information is inherently connected to an individual's identity. Continuous or large-scale facial surveillance can potentially create detailed records of where individuals travel, whom they meet, and which public spaces they visit.

Such monitoring may have consequences even when no criminal activity occurs. Individuals may modify their behavior if they believe that their movements are continuously observed. This phenomenon can affect not only privacy but also freedom of expression, freedom of association, and individual autonomy. People may become reluctant to participate in lawful demonstrations, political meetings, or social activities if they believe that their identities can be automatically recorded.

Therefore, facial recognition regulation should consider the broader constitutional consequences of biometric surveillance rather than treating the technology merely as another form of data processing.

4. Biometric Data and Data Protection

Facial information presents particular risks because biometric identifiers are closely associated with individual identity. If biometric databases are compromised, individuals may not be able to simply change their facial characteristics in the way they can replace a password.

A comprehensive data protection framework should therefore address the collection, storage, processing, sharing, retention, and deletion of biometric information.

Organizations using facial recognition should have a clearly defined purpose for collecting facial data. Data should not be collected merely because future use may become technologically possible.

Data minimization is another important principle. Organizations should collect only the information necessary for the specified purpose. Retention periods should also be limited, and biometric information should be securely protected against unauthorized access.

Where facial recognition is deployed by private organizations, individuals should receive appropriate information regarding its use and, where legally required, meaningful consent mechanisms should be provided.

However, consent may not always be sufficient. In environments such as workplaces or public services, individuals may have limited practical ability to refuse biometric processing. Legal safeguards should therefore operate even where formal consent exists.

5. State Surveillance and Constitutional Limits

The use of facial recognition by government authorities raises particularly significant constitutional concerns. Governments possess extensive investigative and enforcement powers, and the deployment of biometric surveillance may significantly increase those capabilities.

State use of facial recognition should therefore be based on clear legal authority. The mere existence of a technological capability should not automatically establish legal authority to use it.

A proportionality-based approach provides a useful framework. A facial recognition measure should pursue a legitimate objective, be suitable for achieving that objective, be necessary in the circumstances, and maintain an appropriate balance between the public interest and individual rights.

For example, using facial recognition in a narrowly defined investigation involving a serious offence may raise different legal considerations from continuously scanning the faces of everyone entering a public area.

The scale and intrusiveness of surveillance should therefore be relevant to the level of legal scrutiny.

6. Consent and Public Spaces

One of the most difficult questions concerns facial recognition in public places. Individuals generally understand that they may be visible to other people when they enter a public area. However, visibility is not necessarily equivalent to consent to automated biometric identification.

A person walking through a shopping center may expect to be seen by other individuals but may not reasonably expect their face to be automatically compared against a biometric database.

The legal distinction between observation and automated identification is therefore important. Facial recognition transforms ordinary visual observation into systematic and searchable personal data processing.

Regulatory frameworks should consequently establish specific safeguards for biometric surveillance in public spaces, particularly where identification occurs without individual participation.

7. Algorithmic Bias and Discrimination

Another major concern involves accuracy and algorithmic bias. Facial recognition systems may produce different error rates across demographic groups depending on the quality and representativeness of the data used to develop and test the system.

An inaccurate identification can have serious consequences when facial recognition is used in law enforcement. A false match may cause an innocent person to become the subject of investigation or detention.

From a legal perspective, the problem is not merely technological. Repeatedly inaccurate outcomes affecting particular groups may raise equality and discrimination concerns.

Organizations deploying facial recognition should therefore conduct rigorous accuracy testing and monitor performance across relevant populations. High-impact applications should require stronger safeguards than low-risk authentication systems.

8. Facial Recognition and Law Enforcement

Law-enforcement applications represent one of the most controversial uses of facial recognition. The technology can potentially assist investigators by comparing images from surveillance footage with databases containing known identities.

However, investigative usefulness should not eliminate traditional legal safeguards. Facial recognition results should generally be treated as investigative information rather than unquestionable proof of identity.

Human verification is particularly important. A facial recognition match should be independently assessed, and investigators should consider alternative explanations and potential system errors.

Legal frameworks should also define when facial recognition may be used, who may authorize its use, what databases may be searched, how long resulting data may be retained, and what oversight mechanisms apply.

Independent review can help prevent the technology from becoming an unchecked surveillance mechanism.

9. Transparency and Accountability

Individuals may find it difficult to challenge facial recognition systems because the processing frequently occurs invisibly. A person may not know that their face has been captured or analyzed.

Transparency is therefore essential. Organizations should provide appropriate information regarding the existence and purpose of facial recognition systems, subject to legitimate security considerations.

Accountability also requires clear identification of the institution responsible for the technology. Organizations should maintain records concerning system deployment, accuracy testing, data retention, access controls, and security incidents.

Where significant harm occurs, affected individuals should have access to appropriate complaint and redress mechanisms.

10. Judicial Oversight and Legal Remedies

Judicial oversight can provide an important safeguard against disproportionate biometric surveillance. Courts may be required to assess whether facial recognition was used pursuant to lawful authority and whether the interference with privacy was justified.

Legal remedies should be available where biometric information is collected or processed unlawfully. Depending on the applicable legal system, remedies may include deletion of improperly collected data, compensation, exclusion of unlawfully obtained evidence, administrative sanctions, or judicial orders restricting future processing.

Effective remedies are particularly important because privacy violations involving biometric data may be difficult to reverse once information has been disseminated.

11. Proposed Rights-Based Regulatory Framework

A rights-based legal framework for facial recognition should incorporate the following principles.

Legality: Facial recognition should operate pursuant to a clear legal basis.

Purpose limitation: Biometric information should be collected only for specified and legitimate purposes.

Necessity and proportionality: Intrusive facial recognition should be justified by a legitimate and sufficiently important objective.

Transparency: Individuals should receive meaningful information about biometric processing where appropriate.

Accuracy: Organizations should conduct regular testing and address unreasonable error rates.

Human oversight: Significant decisions should not depend exclusively on automated facial recognition outputs.

Security: Biometric databases should be protected against unauthorized access and misuse.

Retention limitation: Facial data should not be stored longer than necessary for the lawful purpose.

Independent oversight: High-risk systems should be subject to appropriate regulatory or judicial supervision.

Effective remedies: Individuals should have practical mechanisms to challenge unlawful or inaccurate biometric processing.

Together, these principles can provide a balanced regulatory structure that protects fundamental rights without unnecessarily preventing beneficial technological applications.

12. Commercial Use of Facial Recognition

Private-sector deployment of facial recognition also deserves careful legal consideration. Retailers, financial institutions, transportation companies, technology platforms, and other organizations may use facial recognition for authentication, security, personalization, or customer management.

Commercial incentives may encourage organizations to expand biometric processing beyond the original purpose for which information was collected. For this reason, purpose limitation and transparency are particularly important.

Businesses should clearly define why facial recognition is being used and should avoid treating biometric identification as the default option where less intrusive alternatives are reasonably available.

Where consumers have genuine alternatives, consent may provide an additional safeguard. However, legal protection should not depend entirely on consent because consumers may not fully understand the long-term implications of biometric processing.

13. Challenges in Regulation

Regulating facial recognition presents several challenges. First, technological development is rapid, while legislative processes are comparatively slow. Rules designed around a particular technical architecture may become outdated.

Second, different jurisdictions may adopt different approaches to biometric surveillance. This can create difficulties for companies operating internationally and for cross-border investigations.

Third, excessive regulation could prevent beneficial applications, including secure authentication and certain public-safety uses.

Fourth, technological accuracy may improve over time, making legal standards based exclusively on current error rates difficult to maintain.

For these reasons, legislation should focus on fundamental principles and risk-based regulation rather than attempting to regulate every technical detail.

14. Future Directions

Future research should examine the relationship between facial recognition and emerging technologies such as generative artificial intelligence, deepfakes, biometric authentication, and large-scale surveillance platforms.

Particular attention should be given to the development of independent algorithmic audits and standardized impact assessments.

Courts and regulatory authorities may also require greater technical expertise to evaluate evidence involving biometric systems.

International cooperation will become increasingly important as biometric databases and digital platforms operate across national boundaries. Common principles concerning biometric privacy, lawful surveillance, transparency, and remedies could improve consistency while protecting fundamental rights.

15. Conclusion

Facial recognition technology represents both an important technological development and a significant legal challenge. Its ability to identify individuals rapidly can provide legitimate benefits in authentication, security, and law enforcement. At the same time, unrestricted deployment can create serious risks to privacy, autonomy, equality, and freedom.

The central legal issue is therefore not whether facial recognition should exist, but under what conditions it should be permitted. A rights-based framework should require legality, necessity, proportionality, transparency, accuracy, human oversight, data security, limited retention, independent supervision, and effective remedies.

Facial recognition should not be treated as inherently unlawful merely because it involves biometric information. Equally, technological efficiency should not be accepted as sufficient justification for unrestricted biometric surveillance.

The future regulation of facial recognition must maintain a careful balance between legitimate technological objectives and constitutional values. If appropriate safeguards are established, facial recognition may be used responsibly while preserving individual rights. Without such safeguards, however, the technology may transform ordinary public visibility into persistent and largely invisible biometric surveillance. The rule of law must therefore remain the guiding principle governing the deployment of facial recognition in the digital era.

1. Introduction

Artificial intelligence has increasingly become integrated into everyday social, commercial, and governmental activities. Among the technologies attracting significant legal attention is facial recognition technology (FRT), which uses computational systems to analyze facial characteristics and compare them against stored or available information. Facial recognition can be used for identity verification, access control, financial authentication, airport security, policing, border management, attendance systems, and commercial personalization.

The technology offers several potential benefits. It can assist law-enforcement agencies in identifying suspects, help organizations prevent identity fraud, facilitate secure authentication, and improve access-control systems. However, these advantages must be considered alongside the possibility of intrusive surveillance and misuse of biometric information.

The legal significance of facial recognition arises primarily from the nature of facial information itself. Unlike a password, facial characteristics cannot ordinarily be replaced once compromised. Biometric information can therefore create long-term privacy implications. Furthermore, facial recognition systems may operate without the knowledge or active participation of the person being identified.

The possibility of identifying individuals in public spaces creates an important constitutional question: to what extent should the state or private organizations be permitted to monitor individuals through automated biometric technologies?

This question becomes particularly significant in democratic societies where privacy, dignity, liberty, and equality are protected through constitutional or human-rights frameworks. The challenge is to develop a legal framework that permits legitimate technological applications while preventing disproportionate surveillance.

This article examines facial recognition through the lens of privacy and constitutional law. It focuses on biometric data protection, consent, surveillance, proportionality, algorithmic bias, accountability, and remedies.

2. Understanding Facial Recognition Technology

Facial recognition technology generally involves capturing an image or video of an individual's face, extracting distinguishing facial characteristics, converting those characteristics into a mathematical representation, and comparing the resulting representation with one or more stored templates.

Two broad applications can be distinguished: **facial verification** and **facial identification**.

Facial verification generally asks whether an individual is the person they claim to be. For example, a system may compare a person's face with an image previously associated with that person's account.

Facial identification involves determining who an individual is among a larger database of potential identities. This application creates greater privacy concerns because individuals may be identified without voluntarily presenting credentials.

Facial recognition systems may also be deployed in real-time surveillance environments. Cameras can continuously capture individuals in public spaces and automatically compare their facial characteristics against watchlists or databases.

The legal implications depend significantly on the purpose, scale, accuracy, retention period, and institutional context of deployment.

3. The Right to Privacy

Privacy is a fundamental legal interest that protects individuals from unjustified interference with their personal lives and autonomy. Modern privacy law increasingly recognizes that privacy is not limited to physical spaces. It also encompasses control over personal information and protection against unauthorized collection and processing.

Facial recognition raises unique privacy concerns because biometric information is inherently connected to an individual's identity. Continuous or large-scale facial surveillance can potentially create detailed records of where individuals travel, whom they meet, and which public spaces they visit.

Such monitoring may have consequences even when no criminal activity occurs. Individuals may modify their behavior if they believe that their movements are continuously observed.

This phenomenon can affect not only privacy but also freedom of expression, freedom of association, and individual autonomy. People may become reluctant to participate in lawful demonstrations, political meetings, or social activities if they believe that their identities can be automatically recorded.

Therefore, facial recognition regulation should consider the broader constitutional consequences of biometric surveillance rather than treating the technology merely as another form of data processing.

4. Biometric Data and Data Protection

Facial information presents particular risks because biometric identifiers are closely associated with individual identity. If biometric databases are compromised, individuals may not be able to simply change their facial characteristics in the way they can replace a password.

A comprehensive data protection framework should therefore address the collection, storage, processing, sharing, retention, and deletion of biometric information.

Organizations using facial recognition should have a clearly defined purpose for collecting facial data. Data should not be collected merely because future use may become technologically possible.

Data minimization is another important principle. Organizations should collect only the information necessary for the specified purpose. Retention periods should also be limited, and biometric information should be securely protected against unauthorized access.

Where facial recognition is deployed by private organizations, individuals should receive appropriate information regarding its use and, where legally required, meaningful consent mechanisms should be provided.

However, consent may not always be sufficient. In environments such as workplaces or public services, individuals may have limited practical ability to refuse biometric processing. Legal safeguards should therefore operate even where formal consent exists.

5. State Surveillance and Constitutional Limits

The use of facial recognition by government authorities raises particularly significant constitutional concerns. Governments possess extensive investigative and enforcement powers, and the deployment of biometric surveillance may significantly increase those capabilities.

State use of facial recognition should therefore be based on clear legal authority. The mere existence of a technological capability should not automatically establish legal authority to use it.

A proportionality-based approach provides a useful framework. A facial recognition measure should pursue a legitimate objective, be suitable for achieving that objective, be necessary in the circumstances, and maintain an appropriate balance between the public interest and individual rights.

For example, using facial recognition in a narrowly defined investigation involving a serious offence may raise different legal considerations from continuously scanning the faces of everyone entering a public area.

The scale and intrusiveness of surveillance should therefore be relevant to the level of legal scrutiny.

6. Consent and Public Spaces

One of the most difficult questions concerns facial recognition in public places. Individuals generally understand that they may be visible to other people when they enter a public area. However, visibility is not necessarily equivalent to consent to automated biometric identification.

A person walking through a shopping center may expect to be seen by other individuals but may not reasonably expect their face to be automatically compared against a biometric database.

The legal distinction between observation and automated identification is therefore important. Facial recognition transforms ordinary visual observation into systematic and searchable personal data processing.

Regulatory frameworks should consequently establish specific safeguards for biometric surveillance in public spaces, particularly where identification occurs without individual participation.

7. Algorithmic Bias and Discrimination

Another major concern involves accuracy and algorithmic bias. Facial recognition systems may produce different error rates across demographic groups depending on the quality and representativeness of the data used to develop and test the system.

An inaccurate identification can have serious consequences when facial recognition is used in law enforcement. A false match may cause an innocent person to become the subject of investigation or detention.

From a legal perspective, the problem is not merely technological. Repeatedly inaccurate outcomes affecting particular groups may raise equality and discrimination concerns.

Organizations deploying facial recognition should therefore conduct rigorous accuracy testing and monitor performance across relevant populations. High-impact applications should require stronger safeguards than low-risk authentication systems.

8. Facial Recognition and Law Enforcement

Law-enforcement applications represent one of the most controversial uses of facial recognition. The technology can potentially assist investigators by comparing images from surveillance footage with databases containing known identities.

However, investigative usefulness should not eliminate traditional legal safeguards. Facial recognition results should generally be treated as investigative information rather than unquestionable proof of identity.

Human verification is particularly important. A facial recognition match should be independently assessed, and investigators should consider alternative explanations and potential system errors.

Legal frameworks should also define when facial recognition may be used, who may authorize its use, what databases may be searched, how long resulting data may be retained, and what oversight mechanisms apply.

Independent review can help prevent the technology from becoming an unchecked surveillance mechanism.

9. Transparency and Accountability

Individuals may find it difficult to challenge facial recognition systems because the processing frequently occurs invisibly. A person may not know that their face has been captured or analyzed.

Transparency is therefore essential. Organizations should provide appropriate information regarding the existence and purpose of facial recognition systems, subject to legitimate security considerations.

Accountability also requires clear identification of the institution responsible for the technology. Organizations should maintain records concerning system deployment, accuracy testing, data retention, access controls, and security incidents.

Where significant harm occurs, affected individuals should have access to appropriate complaint and redress mechanisms.

10. Judicial Oversight and Legal Remedies

Judicial oversight can provide an important safeguard against disproportionate biometric surveillance. Courts may be required to assess whether facial recognition was used pursuant to lawful authority and whether the interference with privacy was justified.

Legal remedies should be available where biometric information is collected or processed unlawfully. Depending on the applicable legal system, remedies may include deletion of improperly collected data, compensation, exclusion of unlawfully obtained evidence, administrative sanctions, or judicial orders restricting future processing.

Effective remedies are particularly important because privacy violations involving biometric data may be difficult to reverse once information has been disseminated.

11. Proposed Rights-Based Regulatory Framework

A rights-based legal framework for facial recognition should incorporate the following principles.

Legality: Facial recognition should operate pursuant to a clear legal basis.

Purpose limitation: Biometric information should be collected only for specified and legitimate purposes.

Necessity and proportionality: Intrusive facial recognition should be justified by a legitimate and sufficiently important objective.

Transparency: Individuals should receive meaningful information about biometric processing where appropriate.

Accuracy: Organizations should conduct regular testing and address unreasonable error rates.

Human oversight: Significant decisions should not depend exclusively on automated facial recognition outputs.

Security: Biometric databases should be protected against unauthorized access and misuse.

Retention limitation: Facial data should not be stored longer than necessary for the lawful purpose.

Independent oversight: High-risk systems should be subject to appropriate regulatory or judicial supervision.

Effective remedies: Individuals should have practical mechanisms to challenge unlawful or inaccurate biometric processing.

Together, these principles can provide a balanced regulatory structure that protects fundamental rights without unnecessarily preventing beneficial technological applications.

12. Commercial Use of Facial Recognition

Private-sector deployment of facial recognition also deserves careful legal consideration. Retailers, financial institutions, transportation companies, technology platforms, and other organizations may use facial recognition for authentication, security, personalization, or customer management.

Commercial incentives may encourage organizations to expand biometric processing beyond the original purpose for which information was collected. For this reason, purpose limitation and transparency are particularly important.

Businesses should clearly define why facial recognition is being used and should avoid treating biometric identification as the default option where less intrusive alternatives are reasonably available.

Where consumers have genuine alternatives, consent may provide an additional safeguard. However, legal protection should not depend entirely on consent because consumers may not fully understand the long-term implications of biometric processing.

13. Challenges in Regulation

Regulating facial recognition presents several challenges. First, technological development is rapid, while legislative processes are comparatively slow. Rules designed around a particular technical architecture may become outdated.

Second, different jurisdictions may adopt different approaches to biometric surveillance. This can create difficulties for companies operating internationally and for cross-border investigations.

Third, excessive regulation could prevent beneficial applications, including secure authentication and certain public-safety uses.

Fourth, technological accuracy may improve over time, making legal standards based exclusively on current error rates difficult to maintain.

For these reasons, legislation should focus on fundamental principles and risk-based regulation rather than attempting to regulate every technical detail.

14. Future Directions

Future research should examine the relationship between facial recognition and emerging technologies such as generative artificial intelligence, deepfakes, biometric authentication, and large-scale surveillance platforms.

Particular attention should be given to the development of independent algorithmic audits and standardized impact assessments.

Courts and regulatory authorities may also require greater technical expertise to evaluate evidence involving biometric systems.

International cooperation will become increasingly important as biometric databases and digital platforms operate across national boundaries. Common principles concerning biometric privacy, lawful surveillance, transparency, and remedies could improve consistency while protecting fundamental rights.

15. Conclusion

Facial recognition technology represents both an important technological development and a significant legal challenge. Its ability to identify individuals rapidly can provide legitimate

benefits in authentication, security, and law enforcement. At the same time, unrestricted deployment can create serious risks to privacy, autonomy, equality, and freedom.

The central legal issue is therefore not whether facial recognition should exist, but under what conditions it should be permitted. A rights-based framework should require legality, necessity, proportionality, transparency, accuracy, human oversight, data security, limited retention, independent supervision, and effective remedies.

Facial recognition should not be treated as inherently unlawful merely because it involves biometric information. Equally, technological efficiency should not be accepted as sufficient justification for unrestricted biometric surveillance.

The future regulation of facial recognition must maintain a careful balance between legitimate technological objectives and constitutional values. If appropriate safeguards are established, facial recognition may be used responsibly while preserving individual rights. Without such safeguards, however, the technology may transform ordinary public visibility into persistent and largely invisible biometric surveillance. The rule of law must therefore remain the guiding principle governing the deployment of facial recognition in the digital era.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.