RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES

DOI:10.5281/zenodo.22802269

# The Right to Privacy in the Age of AI-Based Facial Recognition

**Andreea Corsei**

*"Petre Andrei" University, Iași, Romania*
*Dean, "College of Legal Advisers Suceava" Association*
*General Secretary, "Order of Legal Advisers from Romania" Federation*
*office.corsei@yahoo.co.uk*

**Abstract:** The rapid development of artificial intelligence has led to the expansion of the use of facial recognition technologies in both the public and private sectors. Although these systems can contribute to increasing security, identifying individuals and making certain services more efficient, their use raises important legal issues regarding the protection of privacy and the processing of biometric data. This article analyzes the impact of facial recognition systems based on artificial intelligence on the right to privacy, paying particular attention to the collection and processing of biometric data, the consent of individuals, surveillance in public spaces and the risk of disproportionate use of these technologies. The analysis also follows the difficulties generated by identification errors, the lack of algorithmic transparency and the possibility of the emergence of some forms of discrimination. The study highlights the need to achieve a balance between the advantages offered by facial recognition technologies and the protection of the fundamental rights of the individual. It argues that technological development must be accompanied by adequate legal safeguards, based on the principles of legality, necessity, proportionality, transparency and accountability. In conclusion, the article highlights the need for effective regulatory and oversight mechanisms to prevent facial recognition from becoming a tool for excessive surveillance and to ensure effective protection of privacy in the age of artificial intelligence.

**Keywords:** Artificial Intelligence, Facial Recognition, Right To Privacy, Biometric Data

## Introduction

The accelerated development of artificial intelligence has transformed the way personal data is collected, analyzed and used. Among the technologies that have seen significant expansion are facial recognition systems based on artificial intelligence, capable of identifying or verifying a person's identity by analyzing their facial features. These systems are used in increasingly diverse contexts, from identity verification and access control to security, surveillance of public spaces and law enforcement activities.

The use of facial recognition offers important advantages in terms of speed of identification, process automation and security. However, the expansion of this technology generates a series of complex legal issues. Unlike many other categories of personal data, biometric characteristics are closely related to a person's identity. Their collection, storage and analysis can also take place without the active participation or, in certain situations, without the knowledge of the person concerned. From this perspective, the use of facial recognition can affect not only the protection of personal data, but also individual autonomy and the effective exercise of the right to privacy. The issue becomes particularly important when facial recognition systems are used in public spaces. The ability to automatically identify and track individuals can transform traditional forms of surveillance into a continuous and automated process. In the absence of clear legal boundaries, the advantages associated with security may conflict with the fundamental rights of individuals. In this context, the principles of legality, necessity and proportionality become essential for assessing the situations in which the use of technology can be justified.

Another legal issue is the accuracy of the systems and the consequences of mistaken identifications. Poor performance or differences in accuracy can have significant effects when the results of the systems are used to make decisions that affect people. At the same time, the lack of transparency regarding the operation of algorithms, data sources and the retention period

of biometric information can limit the possibility of the individual to understand and challenge the way his data is used. In this context, this article aims to analyze the relationship between the development of facial recognition systems based on artificial intelligence and the legal protection of privacy. The research examines the main risks associated with the collection and processing of biometric data, surveillance, lack of consent, mistaken identification and algorithmic discrimination. At the same time, the analysis aims to determine to what extent the existing legal principles and mechanisms can respond to the challenges generated by the increasingly extensive use of these technologies.

The hypothesis from which the research starts is that technological development and the protection of privacy should not be considered incompatible goals. However, the legitimate use of facial recognition requires the existence of effective legal guarantees, transparency and adequate accountability and oversight mechanisms. Therefore, the fundamental legal challenge lies not only in determining the situations in which the technology can be used, but also in defining the necessary limits so that its advantages do not lead to the disproportionate restriction of the right to privacy.

## Facial Recognition and Biometrics: conceptual and legal framework

Facial recognition technology is a form of automated processing of digital images of a person's face, used for the purpose of identifying or verifying their identity (Council of Europe, 2021). Unlike simply capturing an image, facial recognition systems analyze facial features and create biometric representations that can be compared with data in a database. From this perspective, facial recognition should be analyzed not only as a technological tool, but also as a mechanism for processing information directly associated with individual identity.

From a functional point of view, it is important to differentiate between biometric verification and identification. Verification generally aims to confirm whether a person is who they claim to be, by comparing their characteristics with a determined biometric reference. Identification involves a more extensive operation, since a person's image can be compared with several biometric profiles or models in a database. This distinction is legally relevant because the extent of data processing and the risks to privacy can vary considerably depending on the purpose and manner in which the system is used.

The sensitivity of biometric data is one of the main justifications for granting enhanced legal protection. Data obtained from a person's physical characteristics are closely linked to their identity and their use for identification purposes can have significant consequences for privacy. Under the European data protection framework, biometric data used for the purpose of uniquely identifying a person benefit from a special legal regime (European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, art. 4(14) and art. 9). The importance of this protection is amplified by the fact that, unlike a password or other authentication elements, a person's biometric characteristics cannot be replaced with the same ease if they are compromised.

A particular feature of facial recognition is the possibility of processing data without the active participation of the data subject. Cameras installed in public spaces or surveillance systems can capture images of a large number of people, and biometric analysis can take place without them directly interacting with the technology. The Council of Europe has drawn attention to the fact that the integration of facial recognition into surveillance systems can create serious risks to the right to privacy and the protection of personal data, including because the use of the technology does not always require the knowledge or cooperation of the person whose data is being processed (Council of Europe, Consultative Committee of Convention 108, 2021).

From a legal perspective, the mere existence of a legitimate aim, such as preventing crime or protecting security, is not sufficient to justify any form of biometric surveillance. The use of facial recognition must be assessed in relation to the aim pursued, the necessity of the

intervention and its proportionality. This approach becomes particularly important in the case of real-time facial recognition, as the technology allows for the automated analysis of a very large number of people, including those who are not suspected of having committed an illegal act.

In this sense, the responsible implementation of facial recognition systems requires the integration of privacy protection from the design stage. Recent technical and institutional documents highlight the need for "privacy by design" measures, as well as the importance of proportionality, human rights and the protection of the anonymity of individuals who are not of interest for the legitimate purpose pursued (National Institute of Standards and Technology, OSAC Facial & Iris Identification Subcommittee, Framework for Implementing Passive Live Facial Recognition, 2024). Such guarantees demonstrate that the protection of privacy should not be treated as an obstacle subsequent to the implementation of the technology, but as a fundamental condition for its design and legitimate use.

The legal issue of facial recognition therefore goes beyond the simple protection of a personal image. It concerns the possibility of automatic identification, tracking and correlation of a person with other information, as well as the control that the individual can exercise over the use of his or her biometric identity. For this reason, the establishment of rules on the purpose of processing, access to data, retention period, information security, transparency and responsibility of operators are essential elements for the effective protection of the right to privacy.

## The Right to Privacy and the Legal Challenges of Biometric Surveillance

The right to privacy is one of the fundamental rights that the development of modern surveillance technologies has had significant effects on. In the case of facial recognition, the legal issue does not arise exclusively from the collection of a person's image, but especially from the possibility of transforming it into a tool for identification, monitoring and analysis. Through artificial intelligence-based systems, a facial image can be converted into biometric data and automatically compared with information in databases, which substantially changes the nature and scope of surveillance.

The legal literature has highlighted the fact that facial recognition technology can transform traditional forms of surveillance through its ability to identify and track individuals on a scale that is difficult to achieve through conventional means. The possibility of connecting facial recognition systems to surveillance cameras and extensive image databases allows for the rapid identification of individuals and can facilitate the monitoring of their movements in different spaces (Ferguson, 2021). This technological capability raises important questions about the limits to which surveillance can be compatible with the legal protection of privacy.

One of the major difficulties lies in the difference between simply observing a person in a public space and systematically collecting information about their activity. Traditionally, being in a public space implies a lower level of expectation regarding the privacy of certain actions. However, modern technologies allow for the collection, storage and correlation of a very large volume of information. When analyzed together, this data can reveal relevant aspects about a person's movements, activities and relationships. For this reason, the application of legal doctrines developed before the advent of digital surveillance may become insufficient to protect privacy in the context of new technologies.

Another essential issue is the consent of the person whose biometric data is being processed. Facial recognition systems can analyze images without the person actively participating in the process and, in some situations, without the person's knowledge of the processing. The collection and use of facial images without genuine consent raises important legal and ethical issues, especially when individuals do not have the effective possibility to refuse the processing of their biometric data (Bu, 2021).

From this perspective, a distinction must be made between the possibility of observing or photographing a person and the right to use their facial features for biometric identification. The

fact that a person's image is publicly accessible should not automatically lead to the conclusion that they have expressed their consent to the transformation of the image into a biometric identifier, its storage in a database or its use for other purposes. The legal literature has also proposed the use of the doctrine of the right to one's own image and identity, the "right of publicity", as a possible tool to regulate certain uses of facial recognition technology and to strengthen the role of informed consent (Yew & Xiang, 2022).

Privacy risks are not exclusively associated with the use of technology by public authorities. Private actors use or may use facial recognition for user authentication, access control, fraud prevention, security and the provision of commercial services. In such situations, legal issues extend to the purpose for which the data is collected, the period for which it is retained, the security of databases, access by third parties and the possibility of reusing the information for a purpose other than the one initially declared.

Legislation on biometric information represents, in this context, an important tool for strengthening individual protection. However, legal regulation faces the difficulty of adapting normative concepts to the concrete way in which facial processing technologies work. Analysis of the application of the legislation on the protection of biometric information in Illinois highlights the existence of tensions between legal definitions and obligations and the technical characteristics of facial processing systems. This aspect demonstrates that the effectiveness of a regulation also depends on the legislator's ability to understand and anticipate technological evolution. A distinct issue concerns the accuracy of facial recognition systems. An incorrect identification can have much more serious consequences than a simple technical error when the result is used to adopt a decision that affects a person's legal status. Research on biometric systems has identified the issue of demographic differences in performance and the need to assess the bias that may arise in the operation of such technologies (Drozdowski et al., 2020, pp. 89–103). In areas such as law enforcement or security, the consequences of misidentification can include unjustified suspicions, investigations and other interference with individual rights.

The use of facial recognition can also have effects on the exercise of other fundamental rights. The possibility of automatically identifying people participating in demonstrations, political meetings, religious events or other legitimate activities can lead to changes in their behaviour. People who know or assume that they can be identified and tracked may become less willing to participate in certain activities, even if these are perfectly legal. Thus, the issue of biometric surveillance goes beyond the strict sphere of privacy and can have implications for freedom of expression, freedom of association and freedom of assembly. Consequently, the legitimate use of facial recognition requires more than the existence of a justified purpose. The necessity of the measure, its proportionality and the existence of effective safeguards against abuse must be analysed. The regulation should clearly establish the conditions under which biometric data may be collected, the purposes for which they may be used, the retention period, the persons who may have access to them and the mechanisms through which the individual can challenge any improper use.

The fundamental legal challenge therefore lies in finding a balance between the social and security benefits of facial recognition and the need to protect privacy. The principles of legality, necessity, proportionality, transparency and accountability must be central to such a balance. Protecting the right to privacy does not mean rejecting technology, but establishing legal limits capable of preventing the transformation of an identification tool into a mechanism for generalised surveillance.

## Consent, transparency and legal control over biometric data

The development of facial recognition systems based on artificial intelligence has considerably changed the relationship between the individual, technology and the protection of privacy. While traditional forms of identification usually required the conscious participation of the person by presenting a document, entering a password or voluntarily providing information, facial

recognition can work without such active participation. A person's image can be captured, analysed and compared with information existing in a database in a very short time and, in certain situations, without the person concerned being aware of this process. This particularity determines the transformation of consent, transparency and control over biometric data into essential legal issues for the effective protection of privacy.

Consent is one of the traditional mechanisms through which individuals can exercise control over the processing of information concerning them. In the field of facial recognition, however, the efficiency of this mechanism is questioned. Facial features are permanently visible and can be captured by cameras or extracted from digital photographs without specific action on the part of the individual. As a result, the collection of data necessary for biometric identification can take place in a much less obvious way than in the case of other categories of personal information. This situation is of particular legal importance because the facial image should not be confused with the biometric data generated by its technological processing. A photograph may exist for a specific purpose, but its subsequent use for the extraction of biometric features, the creation of a facial model and its comparison with other images represents an additional form of processing. The literature highlights the existence of significant issues regarding the rights of the individual when images are collected, analysed or stored without adequate information and without the possibility of effective control over the biometric data (Krishan et al., 2022).

From this perspective, the mere existence of an image in a publicly accessible space should not automatically be equated with the individual's consent to any further form of biometric processing. A person may agree to be photographed in a certain context without agreeing to have the image entered into a biometric database, automatically compared with a very large number of other images, or subsequently used for surveillance and identification purposes. The difference is important because the use of artificial intelligence allows the extraction of information from the image that goes beyond the initial function of the photograph and transforms facial features into a persistent identification tool.

Consent must also be analyzed from the perspective of its informed nature. In order for the person to be able to make a real decision regarding the use of their data, they must know the identity of the controller, the nature of the information collected, the purpose of the processing, the period for which the data will be kept, the possibility of transmitting them to third parties, and the rights they can exercise. A general formulation by which the user accepts the processing of personal data may become insufficient when it does not clearly explain that the facial image will be used to generate, store, or compare biometric identifiers. In addition, the possibility that the data may be used later in a different context than the one in which it was initially collected must be taken into account.

The difficulties are even more evident when facial recognition is implemented in public spaces. In airports, train stations, streets, shopping malls, stadiums or other areas frequented by large numbers of people, obtaining prior individual consent can be difficult. Systems can simultaneously analyze many faces, and among the people subject to processing may be individuals who have no connection to the specific purpose for which the technology was installed. In these circumstances, there is a risk that surveillance will no longer be exclusively directed at certain people or specific situations, but will become a generalized form of biometric information collection and analysis.

In the case of the use of facial recognition by authorities, the issue acquires an additional legal dimension. Biometric surveillance can be justified by objectives such as preventing crime, identifying wanted persons or protecting public security. However, the existence of a legitimate purpose does not mean that any method of surveillance automatically becomes acceptable. The use of facial recognition technology by law enforcement agencies may result in significant interferences with the right to privacy and data protection, which is why the necessity, appropriateness and proportionality of the measure must be carefully assessed (Akhtar, 2020).

The more the technology allows for the surveillance of a larger number of people and the collection of a larger volume of information, the stronger the legal justification and safeguards against abuse must be.

In such situations, consent cannot be the sole basis for legal protection. A person who has to cross a public area does not always have a real possibility of avoiding surveillance cameras. Similarly, the mere display of a notice about the existence of facial recognition does not necessarily mean that the person has freely given their consent to the biometric processing. When there is no realistic alternative, the idea of fully voluntary consent becomes difficult to sustain. For this reason, the protection of privacy must also be based on legal obligations imposed on the entities that develop and use these systems.

Transparency acquires, in this context, an essential function. Individuals should be able to find out whether they are subject to a facial recognition system, which institution or company is responsible for it, what is the purpose of using the system and what happens to the resulting information. Transparency should not be reduced to simply placing a notice on the existence of cameras. In the case of facial recognition, the relevant information must allow understanding of the difference between ordinary video surveillance and biometric analysis. A person can be aware that a space is being video monitored for security reasons without assuming that their image is being analyzed biometrically and automatically compared with the information in a database. Transparency must also concern the actors involved in the entire technological process. The system can be developed by a company, provided by another entity and used by a public institution or a private operator. The data can be stored on the infrastructure of another provider or can come from previously established databases. This fragmentation of the process can make it difficult to establish responsibility when an individual's rights are violated. Comparative analyses of facial recognition regulation demonstrate that issues of oversight and accountability need to be considered alongside privacy and the ethical implications of artificial intelligence (Almeida et al., 2022). Transparency must therefore not only allow for knowledge that the technology is being used, but also for the identification of the actors who control the data and make decisions about its use.

Another key issue concerns the purpose for which biometric information is collected. Data obtained for a specific purpose should not be automatically used for any other purpose. In the field of facial recognition, this issue is particularly important because an image provided for identity verification can acquire value for numerous other uses. The technology allows information to be copied, stored, transferred and compared without the need to re-capture the person's face. Therefore, the legal risk does not only concern the initial collection, but also what happens to the data after the purpose for which it was obtained has been achieved. For example, the use of an image to gain access to a building should not automatically lead to the inclusion of the person in a database intended for behavioral monitoring. Similarly, a database created for user authentication should not be reused for the development of a surveillance system without the existence of an appropriate legal basis. This possibility of gradually expanding the use of data is relevant to the right to privacy because the individual may gradually lose control over their biometric identity. An initially limited and apparently justified processing can become, through reuse and interconnection, part of a much larger monitoring mechanism.

The duration of data retention is another fundamental component of privacy protection. Even if the initial processing is justified, the indefinite retention of biometric information may create additional risks. The longer the data is stored and in more systems, the greater the possibilities of unauthorized access, transfer, reuse or compromise. The problem is accentuated by the particular nature of biometric information. If a password is compromised, it can be changed. However, a person's physical characteristics cannot be replaced in the same way, which means that a security breach of biometric information can have consequences that are much more difficult to fix.

Recent research on the protection of privacy in facial recognition systems shows that risks do not arise at a single moment of processing, but can manifest themselves at different stages of the technological cycle, from data generation and processing to inference and storage (Sun & Liu, 2025). This perspective is of legal importance because it demonstrates that the duty to protect cannot end after the information is obtained. Safeguards must accompany biometric data throughout its existence and use. In this sense, data minimization is an important measure. Operators should collect and store only the information necessary to achieve the stated purpose and avoid storing data that is no longer needed.

The relationship between law and technology should not be conceived exclusively in the form of legal intervention subsequent to the occurrence of damage. A preventive approach involves integrating privacy protection from the system design stage. In the case of facial recognition, this may involve limiting the information collected, reducing retention periods, strictly controlling access to databases and using technical mechanisms designed to protect biometric patterns. Research on privacy-protecting techniques in facial recognition demonstrates the existence of solutions that aim to reduce the exposure of facial features at various stages of the identification process (Hasan et al., 2023). The existence of these solutions is also relevant legally, as it demonstrates that privacy protection can be integrated into the system architecture itself and should not be treated exclusively as an external obligation imposed after the technology is implemented.

At the same time, technical protection cannot replace legal responsibility. The person whose data is being processed must be able to identify the responsible entity and have the means to request information, challenge improper use and, when the legal conditions are met, obtain redress. This requirement is particularly important in the case of artificial intelligence-based systems, where the process may involve many participants. The algorithm developer, the system provider, the database administrator and the institution using the results may be distinct entities. In the absence of a clear delineation of obligations, there is a risk of dispersion of responsibility and difficulty in identifying the actor responsible for a breach.

The recent literature on facial recognition highlights the need for an integrated approach that combines privacy protection, ethical principles and legal regulatory mechanisms, especially in the context of the expansion of surveillance systems based on artificial intelligence (Wang et al., 2024). Accountability must include not only the reaction to breaches already produced, but also preventive risk assessment, justification of the purpose of use, verification of system performance, documentation of operations and continuous supervision of the effects of the technology on individuals.

Consent therefore remains an important element of privacy protection, but it cannot be the only legal guarantee in the field of facial recognition. The automatic and sometimes difficult to observe nature of biometric processing, the possibility of using systems in public spaces and the imbalance between the individual and the entity controlling the technology limit the capacity of consent to provide effective control on its own. Protection must be built by combining consent with transparency, purpose limitation, data minimisation, information security, the establishment of fixed retention periods, the integration of privacy protection into the design of systems and the existence of clear accountability mechanisms.

Such a model does not imply the rejection of facial recognition technology, but rather the establishment of the conditions under which it can be used without transforming biometric identity into a permanently available resource for surveillance. Technological development cannot, in itself, constitute a justification for reducing legal standards for the protection of the individual. On the contrary, the greater the ability of technology to identify, track and correlate information about individuals, the clearer, more effective and proportionate the legal guarantees must be to the risks created.

**Algorithmic errors, discrimination and the legal consequences of facial recognition**

The use of facial recognition systems based on artificial intelligence raises legal issues that go beyond data protection and individual consent. A particularly important dimension concerns the accuracy of these systems and the possibility that algorithmic errors may have different effects on certain categories of people. When the technology is used exclusively to facilitate access to a device or service, an incorrect identification may represent, first and foremost, an inconvenience. The situation changes fundamentally, however, when the same type of technology is used by law enforcement authorities, in security systems or in other contexts where the result of the identification may influence the exercise of fundamental rights. In such circumstances, the issue of accuracy is no longer exclusively technical, but acquires a clear legal dimension.

Facial recognition systems work by comparing the features extracted from an image with the biometric features associated with other images. The result of such a comparison should not be understood as an absolute certainty regarding the identity of the person. Performance can be influenced by many factors, such as image quality, lighting, face position, camera resolution, database characteristics, and the specifics of the algorithm used. For this reason, using an algorithmic result as if it were an infallible identification can have serious consequences.

The problem becomes even more complex when the error rate is not evenly distributed across different demographic categories. Evaluations of facial recognition algorithms by the National Institute of Standards and Technology have identified demographic differences in the performance of many algorithms analyzed, including variations associated with gender, age, and demographic groups (Grother et al., 2019). The legal importance of these findings is considerable. If the probability of an error occurring differs depending on the characteristics of the person analyzed, the use of technology can lead to an unequal distribution of risks and consequences.

From a legal perspective, equality involves more than just the formal application of the same rules to all individuals. An apparently neutral technology can produce disproportionate results for certain groups, and this becomes relevant when the results are used to make decisions with legal effects. A system can apply the same procedure to all images and at the same time generate different levels of error. The formal neutrality of the algorithm does not therefore guarantee the neutrality of its effects. The issue of performance differences has also become apparent in research on commercial facial recognition systems. A study by Buolamwini and Gebru demonstrated significant differences in accuracy between groups tested in commercial gender classification systems. The authors found that darker-skinned women had the highest error rates among the groups tested, highlighting the need for intersectional evaluation of automated systems (Buolamwini & Gebru, 2018). Although gender classification and facial recognition are distinct technical tasks, the research has made an important contribution to the broader debate on the bias of facial recognition systems and the need to test them on diverse populations.

The origin of such differences cannot be reduced to a single technical flaw. The performance of the systems can be influenced by the data used to develop and evaluate the algorithms, the representation of different categories in the databases, the quality of the images, and the specific conditions in which the technology is used. The literature on demographic bias in biometrics shows that the issue must be analyzed from both a technical and a social perspective, since differences in performance can arise at several stages of the development and use of a biometric system (Drozdowski et al., 2020). This observation is important for establishing legal liability. If a system is used in a field with a significant impact on the rights of the individual, the mere assertion that the result was produced by an algorithm cannot remove the responsibility of the actor who decided to use the technology. The institution implementing a facial recognition system must be aware of its limitations, assess the level of accuracy, and establish procedures for verifying the results before they are transformed into measures affecting an individual.

Particularly in the field of law enforcement, the distinction between a possible biometric match and establishing the identity of a person must be rigorously maintained. The result provided by a facial recognition system should be treated as an element requiring verification, and not as an autonomous conclusion about identity. When this distinction is ignored, a technological error can be transformed into an institutional error. A false match can focus an investigation on an innocent person and influence how other information is subsequently interpreted.

From this perspective, one of the most serious consequences of the inappropriate use of facial recognition is the possibility of a mistaken identification followed by coercive measures. Recent legal literature documents concerns about the use of the technology by law enforcement agencies and cases in which identifications generated by facial recognition have contributed to the arrest of innocent people. Cebreros (2025) examines the issue of mistaken arrests and the disproportionate impact that the use of the technology can have on already vulnerable communities, arguing for the need for legislative limits on the situations in which authorities rely on identifications produced by such systems. The consequences of a misidentification are not limited to the initial moment of intervention by the authorities. A misidentified person may be subject to investigation, summoned for explanations, detained or, in more serious cases, arrested. Even when the error is subsequently corrected, the effects on reputation, professional life, social relationships and personal status may persist. For this reason, the legal assessment of risk must take into account not only the statistical probability of an error, but also the severity of the consequences it may produce.

An apparently low error rate can become problematic when the technology is used on a very large scale. If millions of people are analyzed, even a small percentage of incorrect results can generate a significant number of false matches. Furthermore, in a one-to-many identification system, a person's image is compared to a very large number of records, which creates different problems than simply verifying the identity of a known person. Technical assessments highlight the importance of distinguishing between different ways of using facial recognition when assessing the performance of an algorithm.

The composition of databases can in turn influence the results of identification systems. Research on demographic equity in facial identification has shown that demographic imbalances in the lists or databases used for comparison can contribute to performance differences (Drozdowski et al., 2021). This finding is important from a legal perspective because it demonstrates that the risk of discrimination cannot be assessed by analysing the algorithm code alone. The entire system in which it operates must be examined, including the data source, the structure of the reference database, the inclusion criteria and the context in which the result is interpreted. This raises the issue of auditing facial recognition systems before and after implementation. The assessment should not be limited to the overall accuracy rate. An aggregate percentage can hide important differences between demographic categories. For this reason, systems used in contexts with significant legal impact should be assessed using indicators that allow the identification of performance differences and the risk of producing inequitable effects. Research on measuring the fairness of facial recognition algorithms shows, however, that defining and measuring "fairness" is not straightforward, including difficulties in choosing appropriate indicators to compare demographic differences (Howard et al., 2022).

These technical difficulties do not diminish the legal obligation to control risks. On the contrary, uncertainty about the performance of a system can be an argument for introducing additional safeguards. The more serious the consequences of an error, the higher the level of human verification, documentation and possibility of challenge should be. In law enforcement, for example, a facial recognition result should not be the only element on the basis of which a coercive measure is adopted against an individual. Human oversight is necessary, but even this is not an automatic solution. The person interpreting the result may grant the technology more authority than its actual performance justifies. The existence of a result generated by a

sophisticated system can create the impression of objectivity and accuracy, even if the result is only a probabilistic estimate. In this respect, the training of the people using the technology is as important as the quality of the algorithm. Operators must understand the limits of the system and be trained to treat the results as information that requires independent confirmation.

The right of the individual to challenge the result is another fundamental guarantee. When a decision with significant effects is based, even in part, on facial recognition, the individual should be able to find out that the technology has been used and have the possibility to challenge the accuracy of the identification. Without transparency, the right to challenge becomes difficult to exercise, as the individual may not know the origin of the information that led to the intervention against him. The issue thus lies at the intersection of privacy (Rotaru, 2016), equality, non-discrimination, transparency and the right to a fair trial. The use of a technology with different performance for different categories of people can turn a technical deficiency into a fundamental rights issue when the results are integrated into the work of public institutions. For this reason, the regulation of facial recognition should not be limited to establishing the conditions under which the data can be collected. It is also necessary to regulate the way in which the results of the algorithms can be used for decision-making. A proper legal approach involves evaluating systems before implementation, periodically testing performance, documenting errors, analyzing demographic differences, human verification, and establishing independent oversight mechanisms. In situations where the technology is used by authorities, the standards must be all the more demanding if the result may contribute to restricting a person's freedom. Administrative efficiency or speed of identification cannot be sufficient arguments to ignore the risk of error.

Finally, the issue of algorithmic bias demonstrates that facial recognition technology cannot be evaluated solely on the basis of its average ability to correctly identify individuals. From a legal perspective, it is equally important to determine who bears the risk of errors, how serious their consequences are, and what mechanisms exist to prevent and correct them. A system that works very well for most people may continue to be problematic if its errors are concentrated in specific categories and if the affected individuals do not have effective means of challenging them. Protecting privacy and equality in the context of facial recognition therefore requires moving from simple trust in technological progress to a model based on verification, accountability and legal control. Artificial intelligence can significantly improve identification capacity, but efficiency should not be confused with infallibility. When algorithmic outputs may affect a person's freedom, reputation or the exercise of rights, the applicable legal standard must reflect the seriousness of these consequences and ensure that technological error does not turn into legal injustice.

## Conclusion

The use of facial recognition technologies based on artificial intelligence offers important advantages in areas such as security, authentication and identification of individuals, but at the same time generates significant risks for the right to privacy. The sensitive nature of biometric data, the possibility of their collection without the active participation of the individual and their use in surveillance systems require the existence of clear and effective legal guarantees. The analysis highlights that the protection of privacy cannot depend exclusively on consent, but must be supported by transparency, purpose limitation, data minimisation, security, oversight and clear accountability mechanisms. At the same time, the risk of misidentifications and differences in performance between different groups demonstrates the need for continuous verification of systems and the preservation of real human control over decisions with legal impact.

The main challenge is therefore not to stop the development of the technology, but to strike a balance between innovation and the protection of fundamental rights. Facial recognition can only be used legitimately to the extent that it complies with the principles of legality, necessity, proportionality, transparency and accountability.

## References


Akhtar, M. (2020). Police use of facial recognition technology and the right to privacy and data protection in Europe. NAVEIÑ REET: *Nordic Journal of Law and Social Research, 1*(9), 324–344. https://doi.org/10.7146/nnjlsr.v1i9.122165

Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics,* 2, 377–387. https://doi.org/10.1007/s43681-021-00077-w

Bu, Q. (2021). The global governance on automated facial recognition (AFR): Ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review, 2*, 113–145. https://doi.org/10.1365/s43439-021-00022-x

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In S. A. Friedler & C. Wilson (Eds.), *Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Proceedings of Machine Learning Research, 81*, 77–91). PMLR. https://proceedings.mlr.press/v81/buolamwini18a.html

Cebreros, J. (2025). Facial recognition technology and wrongful arrests in the digital policing era. *Washington Law Review Online,* 100, 33. https://digitalcommons.law.uw.edu/wlro/vol100/iss2/1/

Council of Europe, Consultative Committee of Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). (2021). *Guidelines on Facial Recognition*. https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html

Council of Europe. (2021). *Ensure that Facial Recognition Does Not Harm Fundamental Rights.* https://www.coe.int/en/web/data-protection/-/ensure-that-facial-recognition-does-not-harm-fundamental-rights

Drozdowski, P., Rathgeb, C., & Busch, C. (2021). Demographic fairness in face identification: The watchlist imbalance effect. In *2021 International Conference of the Biometrics Special Interest Group (BIOSIG).* IEEE. https://doi.org/10.1109/BIOSIG52210.2021.9548291

Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., & Busch, C. (2020). Demographic bias in biometrics: A survey on an emerging challenge. *IEEE Transactions on Technology and Society, 1*(2), 89–103. https://doi.org/10.1109/TTS.2020.2992344

European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, art. 4(14) and art. 9. The Regulation defines biometric data and establishes special protection for biometric data processed for the purpose of uniquely identifying a person.

Ferguson, A.G. (2021). Facial recognition and the Fourth Amendment. *Minnesota Law Review*, *105*(3), 1105–1210. https://doi.org/10.24926/265535.4104

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test Part 3: Demographic effects (NISTIR 8280)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Hasan, M. R., Guest, R., & Deravi, F. (2023). Presentation-level privacy protection techniques for automated face recognition: A survey. *ACM Computing Surveys, 56*(13s), 1–27. https://doi.org/10.1145/3583135

Howard, J. J., Laird, E. J., Sirotin, Y. B., Rubin, R. E., Tipton, J. L., & Vemury, A. R. (2022). Evaluating proposed fairness models for face recognition algorithms. In *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society. Association for Computing Machinery.* https://doi.org/10.1145/3514094.353415 fairness

Krishan, K., Kanchan, T., & Ahuja, M. S. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon, 8*(3), e09086. https://doi.org/10.1016/j.heliyon.2022.e09086

National Institute of Standards and Technology, OSAC Facial & Iris Identification Subcommittee (2024). *Framework for Implementing Passive Live Facial Recognition*. (OSAC Technical Guidance Document 0008). National Institute of Standards and Technology.

Rotaru, I.-G. (2016). Plea for Human Dignity. Scientia Moralitas. Human Dignity - A Contemporary Perspectives, 1, 29-43.

Sun, Z., & Liu, Z. (2025). Ensuring privacy in face recognition: A survey on data generation, inference and storage. *Discover Applied Sciences, 7*, Article 441. https://doi.org/10.1007/s42452-025-06987-2

Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. *Frontiers in Big Data, 7*, 1337465. https://doi.org/10.3389/fdata.2024.1337465

Yew, R.-J., & Xiang, A. (2022). Regulating facial processing technologies: Tensions between legal and technical considerations in the application of Illinois BIPA. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1017–1027). Association for Computing Machinery. https://doi.org/10.1145/3531146.3533163