RFJ REVISTA FACULTAD DE JURISPRUDENCIA

FACIAL RECOGNITION SYSTEMS UNDER THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT

Gabriela Villafuerte-Guerrero *University of Tartu*

ABSTRACT

The human eye can distinguish one person from another by identifying them on their face, physical appearance, or other characteristics that make a person unique. Nowadays, technology allows us to make exact identifications using Facial Recognition Systems (FRS). A computer does not perceive a face but learns a set of data representing various pixels. Consequently, the human eye is improved and replaced, and now this process can be completed automatically using pattern recognition technology.

In this regard, the European Commission refers to the Artificial Intelligence Act (AIA) as a proposal that promises to establish a general framework with many essential requirements for AI-based systems. Numerous concerns are up in the air, from how to tackle these problems to what courses of action the developers of the AI systems should take. This research aims to debate the treatment of Facial Recognition Systems under the AIA. Consequently, it will analyze the prohibitions of certain Artificial Intelligence practices and the classification of high-risk AI systems that directly impact the use of FRS. Next, the problem of bias will be examined, with specific emphasis on the development stage of an AI system and human oversight, which is essential to achieve bias mitigation.

The implications of using algorithms daily can either open or close opportunities for people. In that sense, it stands to reason to instruct Artificial Intelligence to be intelligent enough to not discriminate against anyone based on gender, race, religion, sex, or any other factor.

RESUMEN

El ojo humano puede distinguir a una persona de otra identificándola por su rostro, apariencia física u otras características que hacen a una persona única. Hoy en día, la tecnología permite realizar identificaciones exactas utilizando Sistemas de Reconocimiento Facial (SRF). Una computadora no percibe un rostro, sino que aprende un conjunto de datos que representan varios píxeles. En consecuencia, el ojo humano se mejora y se reemplaza, y ahora este proceso puede completarse automáticamente utilizando tecnología de reconocimiento de patrones.

En este sentido, la Comisión Europea se refiere a la Ley de Inteligencia Artificial (LIA) como una propuesta que promete establecer un marco general con muchos requisitos esenciales para los sistemas basados en IA. Existen numerosas preocupaciones sobre cómo abordar estos problemas y qué medidas deben tomar los desarrolladores de los sistemas de IA. Esta investigación tiene como objetivo debatir el tratamiento de los Sistemas de Reconocimiento Facial bajo la LIA. En consecuencia, se analizarán las prohibiciones de ciertas prácticas de Inteligencia Artificial y la clasificación de los sistemas de IA de alto riesgo que impactan directamente en el uso de SRF. A continuación, se examinará el problema del sesgo, con énfasis específico en la etapa de desarrollo de un sistema de IA y la supervisión humana, que es esencial para lograr la mitigación del sesgo.

Las implicaciones del uso diario de algoritmos pueden abrir o cerrar oportunidades para las personas. En ese sentido, es razonable instruir a la Inteligencia Artificial para que sea lo suficientemente inteligente como para no discriminar a nadie en función de género, raza, religión, sexo u otro factor.

PALABRAS CLAVE: Reconocimiento Facial, Legislación de IA, Discriminación Algorítmica, Regulación de Alto Riesgo, Tecnología de Identificación, Sesgo en IA

KEYWORDS: Facial Recognition, AI Legislation, Algorithmic Discrimination, High-Risk Regulation, Identification Technology, Bias in AI

JEL CODE: K24; O33

RECIBIDO: 26/04/2024
ACEPTADO: 04/09/2024
DOI: 10.26807/rfj.v1i15.497

Overview of Facial Recognition Systems

The Facial Recognition System (FRS) approach was brought into the world when Computer Science developed a method for detecting, analyzing, and categorizing facial patterns (Schroff, Kalenichenko & Philbin, 2015). This journey began in the 1990s when digital cameras replaced traditional film-based photography systems; consequently, the development of computer-readable photographs allowed for immediate data storage and retrieval (Baio, 2014). Through the years, this idea has been improved, and nowadays, FRS works by collecting and processing biometric data and then technically sorting it to make it unique from the others (Huang, 2012). According to Leslie (2020), "using machine learning techniques, the algorithm was trained on a large dataset of face and nonface images to narrow the space of all possible rectangular shapes to the most important ones" (p. 10). The outcome of this incredible technological application has resulted in Facial Recognition Systems, which rely on the fact that a person's face can be unforgettable and identified based on its appearance (Leslie, 2020).

To better understand the functioning of Facial Recognition Systems, it is essential to focus on the following components. First, data collection and processing involve gathering facial images and converting them into a format the system can analyze. This step is crucial as it lays the foundation for how the system identifies and verifies individuals. The quality and accuracy of this data significantly impact the system's overall performance. Second, biometric data refers to the unique physical characteristics of an individual, such as facial features, which the FRS uses to identify and authenticate people (Almotiri, 2022). While facial images are part of this biometric data, they alone are not considered a special category of personal data under the General Data Protection Regulation (GDPR). This leads us to the third component: technical means. According to Recital 51 of the GDPR (2016), facial images only become a special category of personal data when processed through specific technical methods that enable unique identification or authentication. For instance, simply taking a photo does not make it special category data (European Union, 2016). However, when an

FRS processes that photo to identify or verify a person uniquely, it elevates the data's sensitivity (Almotiri, 2022). The GDPR's distinction is essential because it highlights that not all uses of facial images are equally sensitive. The application of advanced technical means transforms these images into biometric data that requires greater protection due to the potential for misuse or discrimination (Almotiri, 2022).

Artificial Intelligence Act (AIA)

The proposed Artificial Intelligence Act by the European Parliament and Council is the legal backdrop to analyze and comprehend what biometric data entails and how Facial Recognition Systems are ruled. Article 3, numeral 33 of the AIA, clarifies the definition of biometric data as personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopy data (2024). That is why biometric data is unique; this processing enables accurate person-to-person identification. In the same way, Facial Recognition Systems analyze unique facial patterns and attributes to distinguish between people with a high degree of accuracy (AIA, 2024).

Although the scope of the AIA includes European Union Member States, Recitals 25 and 26 of these legal frameworks mention the exclusion of the United Kingdom, Ireland, and Denmark. This means these countries are not bound by the rules stated in Article 5 of the AIA regarding prohibited AI practices (AIA, 2024). Article 5 of the Artificial Intelligence Act explicitly refers to prohibited artificial intelligence practices, including real-time remote biometric identification in publicly accessible spaces for law enforcement purposes. This prohibition aims to prevent the misuse of AI technologies that could infringe on individual privacy and fundamental rights (AIA, 2024).

Real-Time Facial Recognition System

According to Recital 8 of the Artificial Intelligence Act, real-time systems instantly gather and identify biometric data through inputs like video footage or cameras (AIA, 2024). These techniques rely on real-time or near-real-time

inputs, such as video footage, camera, or other visual equipment. Another important element is the place where the data is collected. In that sense, Recital 9 of the AIA stated the notion of publicly accessible that should be analyzed case by case (AIA, 2024). The concept of publicly accessible places is physical sites open to the public, except for private spaces like residences, offices, and clubs. Access restrictions don't necessarily mean surveillance and online places are excluded (AIA, 2024).

In addition, a facial recognition system at an airport checkpoint is an example of a real-time facial system. A camera captures a live image of a passenger's face as he approaches the checkpoint and compares it to a database to identify the person. This comparison and identification procedure occurs instantaneously (Libin, Xiaoyu, Yang, Lei y Jiaqi, 2024).

In the case, Beghal v. United Kingdom, border officers used real-time face recognition technology to identify a traveler whose partner was involved in terrorist activities (European Court of Human Rights [ECHR], First Section, 2016). The European Court of Human Rights decided such methods conformed with Article 8, paragraph, as they followed national legislation for public security and national defense interests. The case was deemed legal under Art. 8, paragraph 2 ECH for public security and defense interests (European Court of Human Rights [ECHR], First Section, 2016). This example significantly illustrates the usefulness of a real-time FRS, comparing live images to a database for identification based on their appearance and behavior when that person could threaten a country's internal security. Nevertheless, note that FRS should not instill a sense of continual surveillance.

Post Remote Facial Recognition System

Post Remote FRS compares biometric data that has already been obtained using a predefined template through photos or video. Then, the technology compares facial pictures based on a predefined biometric template through photos or video recorded by closed-circuit television, cameras, or private devices (Suganthy et al., 2022). In the case of C-212/13 of the

European Court of Justice, Mr. Ryneš installed a surveillance camera on his private property and used the footage to identify two suspects who broke his window (Court of Justice of the European Union, Fourth Chamber, 2014) The matter was brought to the European Court of Justice, which decided that using a surveillance camera on private property for personal or safety reasons is acceptable under the European Union legislation (Court of Justice of the European Union, Fourth Chamber, 2014). This decision underscores the legitimacy and practicality of using Post Remote FRS for personal security purposes, demonstrating its value in enhancing safety and aiding in identifying perpetrators. It highlights how technological advancements, when used responsibly, can significantly contribute to personal and public security while maintaining compliance with legal standards (Court of Justice of the European Union, Fourth Chamber, 2014).

Prohibited AI activities related to Facial Recognition Systems

The use of "real-time" remote biometric identification for law enforcement purposes in public spaces is generally not allowed, except for three tightly regulated situations outlined in Recital 19, Article 5 (d), and Annex III of the Artificial Intelligence Act. These situations are:

> (**i**) focused search for possible crime victims, such as missing children.
> (**ii**) preventing an imminent threat to the safety of people, such as attacks by subversive groups.
> (**iii**) detecting perpetrators or suspects of criminal offenses punishable for the threshold at least three years of imprisonment or detention, as established in Article 2(2) of Council Framework Decision 2002/584/JHA62. (AIA, 2024)

The last situation entails 32 criminal offenses considered serious enough to justify using real-time biometric identification. These offenses include participation in criminal organizations, terrorism, human trafficking, sexual exploitation, rape, and kidnapping, among others. However, this threshold may not be stringent enough for certain significant offenses, particularly

those related to the use of Artificial Intelligence (Council of the European Union, 2002).

However, creating a fixed list of offenses can lead to future problems. For instance, crimes such as the creation of child pornography with the assistance of AI are barely regulated (Niedbała, 2023). In such cases, real-time facial recognition technologies might not be justifiable for identifying a minor or their perpetrator in an investigation. This highlights the need for flexibility and adaptability in regulations to address emerging AI-related crimes effectively (Niedbała, 2023).

Moreover, the ever-evolving nature of technology and criminal activities necessitates a regulatory framework that can swiftly adapt to new challenges. A rigid, exhaustive list of offenses may become outdated as new forms of cybercrime, and AI-assisted crimes emerge (AllahRakha, 2024). Therefore, it is crucial to have a dynamic and inclusive approach to regulation, ensuring that all serious threats are adequately covered while allowing for the inclusion of new offenses as they arise. This consideration opens possibilities for future AI systems for large-scale remote identification in online environments.

In the case Peck v. The United Kingdom, the police intervened in a suicide attempt by recognizing a pedestrian who was unaware he was being recorded by closed-circuit television (European Court of Human Rights, Fourth Section, 2003). The Court ruled that this conduct violates the right to privacy guaranteed in Art. 8 of the European Convention on Human Rights. The police identification, in this case, was appropriate. However, the subsequent consequences in which the individual involved could be recognized based on his facial appearance had an impact on his lifestyle by classifying him as a person who tried suicide (European Court of Human Rights, Fourth Section, 2003). In a related study, the European Parliament's Policy Department has established that when public authorities use recognition technologies, they should be disclosed, proportionate, targeted, limited to specific objectives, restricted in time under Union law, and have due regard for human dignity, autonomy, and fundamental rights outlined in the Charter (European Court of Human Rights, Fourth Section, 2003).

The use of real-time face recognition can be beneficial in detecting dangerous individuals, but it should never violate people's rights and freedoms. However, the AIA endorses the use of real-time remote FRS only when the nature of the situation may result in damage (AIA, 2024). In this context, it is convenient that the AIA contains a prior authorization requirement provided by a competent authority when real-time remote biometric technology is employed in public areas. Other prohibited AI practices concerning Facial Recognition Systems include the application of social scoring If the technology of FRS is used to categorize someone, then it must be considered a prohibited activity. This is like a domino; if one action happens, then the whole FRS activates its features, but what the developers and users must watch out for is that the application does not harm or discriminate no one (AIA, 2024).

Nevertheless, what is questionable is the complete or partial authorization, which may be difficult to fulfill because biometric data gathering, comparison, and identification occur instantly. The question of effectively obtaining consent for data processing remains unresolved. Additionally, getting express approval from everyone passing across public spaces won't be easy. The same applies to the naive but reasonable expectation of anonymity in public areas. Case-by-case analysis based on circumstances is necessary to prevent detrimental impacts on fundamental rights.

High-Risk Facial Recognition Systems

The European Council has proportionated a risk-based approach pyramid and next steps for High-Risk AI System Providers. Therefore, the regulatory framework identifies four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk. In the same line, Article 6 (2) and Annex III of the AIA listed eight specific areas identified as high-risk, which are subjects of an ex-ante conformity assessment. The first consideration is the use of biometric data and the categorization of natural persons. In the same way, FRS operates using biometric data, which is why they are classified as a high-risk AI system (AIA, 2024). Throughout this context, it is convenient to review and correct that if AI systems represent a risk to health, safety, or

fundamental rights, they should be examined and subjected to oversight, according to Art. 7 AIA (2024).

The legal framework rightly stipulated that high-risk AI systems must undergo a preliminary conformity evaluation before being placed on the market. That assessment should comply with the following criteria: (i) the intended purpose of the AI system, (ii) how widely it has been or is likely to be used, (iii) whether it has caused harm or impacts adverse effects, (iv) the potential extent of harm to many people, (v) the people potentially harmed as a result of an AI system, (vi) the impact of special vulnerability on the inequality of power (vii) the ease of reversal the output produced by an AI system (viii) existence of effective remedial and preventive measures in existing Union law. It is questionable that factor (iii) shifts the burden of proof on the user, which is problematic and hard to accomplish in practice because the developer has access to technical means (AIA, 2024). In this context, reports or documentation must demonstrate it to the competent authorities. Additionally, the top layer of Art. 7 states that the Commission has the authority to carry out delegated acts to update the list of high-risk AI systems. From this perspective, it is perceived to be promising since it opens the door to new conditions in which AI systems can be developed (AIA, 2024).

Throughout a high-risk AI system's lifecycle, it must establish, implement, and record its processes, and it must be up to date. The baseline requirements are grounded in the High-Level Expert Group on Artificial Intelligence's Ethical Guidelines for Trust AI (2019). The AIA Art. 9 (2) similarly introduces requirements appropriate to risk management procedures. Also, Art. 64 (2) AIA states that high-risk AI system providers will provide access to the AI system's source code upon a justified request by the surveillance authorities (2024).

Regarding the governing activities of building AI technologies, the system supplier is the only one responsible for evaluating and managing the AI system. The assessment process provided in Article 43 of the Proposal appears to be unbalanced. This imbalance stems from the lack of independent oversight, as the system supplier, who has a vested interest in the commercial

success of the technology, is solely responsible for ensuring compliance with regulatory standards. Without third-party evaluation, there is a risk of biased assessments and insufficient accountability (Zhong, 2024).

The Joint opinion of the European Data Protection Board and European Data Protection Supervisor emphasizes that an ex-ante third-party compliance evaluation for high-risk AI must typically be carried out for high-risk AI (2021). One of the advantages of this strategy is that integrating third-party oversight, particularly for high-risk systems, ensures that high-risk AI systems work consistently for their intended purpose and fosters user confidence (European Data Protection Board & European Data Protection Supervisor, 2021). Although a third-party conformity assessment for high-risk processing of personal data is not mandated under the GDPR, the full spectrum of risks posed by AI systems is still not entirely understood. Implementing a general requirement for third-party conformity assessments for all high-risk AI systems would significantly enhance legal certainty and boost user confidence (European Data Protection Board & European Data Protection Supervisor, 2021).

The next point to consider is that those risks must be explained to the user. They should receive proper information and training to understand the consequences and limitations of AI technology (European Data Protection Board & European Data Protection Supervisor, 2021). Foremost, if the user understands any AI system's consequences, limitations, and hazards, he will have control and power over it. On the other hand, if a user is technologically illiterate or does not care about the harm an AI system might create, it will almost surely cause difficulties, which is why users must actively participate (European Data Protection Board & European Data Protection Supervisor, 2021).

According to the AIA, a risk-based approach should be used, with legal intervention adapted to the precise level of danger (2024). Testing should occur before, during, and after-market launch to ensure that the AI system performs its intended purpose and does not pose a high risk. According to the AIA, a risk-based approach should be used, with legal intervention adapted

to the precise level of danger (2024). The AI system's goal is to not go beyond the reason it was developed, and testing will ensure that high-risk AI systems perform for their intended purpose (AIA, 2024).

Biases Problem in Facial Recognition Systems

To tackle bias in AI, we must understand that it relies on algorithms and data. It requires two components in the broadest sense: a code that formalizes a problem in mathematical terms and data that is a set of input variables the machine can learn from (Liu, 2024). The AIA mentions a few times that potential bias might have discriminatory effects, which is one reason the FRS are classified as high-risk (2024). Nevertheless, there are no concrete measures for bias mitigation. Under Art. 10 (5) of the AIA, it is mentioned briefly that providers may use personal data for bias monitoring, detection, and correction (2024).

In that sense, a query should be asked. Does the algorithm discriminate consciously or unconsciously? Before delving into the specifics, it is important to bear in mind that the inherent characteristics of an algorithm include the ability to separate or discriminate information to produce a result. However, if this operation leads to discrimination, whether intentional or unintentional, of one of the legally protected groups, including sex, religion, race, ethnicity, age, and sexual education, then law and technical means need to work on a solution. Machine-learning algorithms have been proven to produce discriminatory outcomes even when not explicitly told to do so (Mishra et al., 2024). Undoubtedly, discrimination comes from a source called biased training data or unequal ground truth. Consequently, it is logical to have a biased outcome if the data set content is discriminatory. Because of this, quality input must be technically guaranteed to produce a decent result (Edgar et al., 2021).

The consequences of bias in FRS can significantly influence the user's rights. For instance, according to the National Institute of Standards and Technology (2019), face recognition systems demonstrate various levels of accuracy across different demographic groups, revealing false positive rates for Asian and Black faces in facial recognition systems (Pangelinan et al.,

2024). The previous fact highlights the negative impact that biased FRS can have. Bias is a consequence of disproportionate preference. The AIA aims to address this issue by outlining and harmonizing important rules for designing and developing AI systems before they hit the market.

A comprehensive approach is necessary to effectively mitigate bias in the use of AI-based systems. Bias arises from disproportionate preferences, which is why the Artificial Intelligence Act specifies essential rules for designing and developing AI systems before they reach the market and standardizes the way post-market controls are conducted. Additionally, an inclusive approach must be integrated into the process, involving both AI developers and decision-makers in corporate boards. Ultimately, the goal is to transition from algorithmic discrimination to achieving true algorithmic fairness, where data is meticulously vetted and cleansed of any biases to ensure equitable outcomes.

CONCLUSION

The identified challenges and opportunities in using Face Recognition Systems suggest that their treatment should be extensive, from system developers to end users. In this sense, the AIA emphasizes the control of AI products, systemic risks, and bias issues to standardize the implementation of this technology.

Therefore, various legal instruments with different approaches should be considered when applying FRS. For example, Regulation of the of the European Parliament and of the Council 2016/679 addresses protecting data subjects when a person's biometrics are collected and processed (2016). However, the AIA excludes liability provisions, making it unclear if users might sue for damages. The AIA encourages Member States to introduce their provisions into their legislation.

As previously stated, the solution should be integral. For instance, system developers must comply with relevant technical documentation before

releasing an AI product in conformity with the standards outlined in the AIA. Also, developers should bear in mind the difference between real-time, post-remote FRS, and high-risk AI activities because the characteristics, methods of application, and systemic risk are different and important to introduce in the development phase. From this perspective, many benefits can be obtained if the system developers achieve those requirements because biometric data collected from FRS is unique among all users; an asset of such value requires all the protection technology can deliver.

Also, leaving the self-assessment to the developers is questionable because they may fail to set a suitable threshold since they are the ones who impose the assessment and develop the system. Therefore, they are unlikely to demand high compliance standards. In the case of FRS, if the technology is used for good purposes, such as identifying criminals, it is justified. Therefore, ensuring that the identification made by the FRS does not result in individual bias or confusion is essential.

This research encourages the design of Facial Recognition Systems starting from the development stage because the input data determines the quality of an AI system. Undoubtedly, discrimination comes from a source called biased training data or unequal ground truth. Consequently, it is logical to have a biased outcome if the data set content is discriminatory. Because of this, quality input must be technically guaranteed to produce a decent result. Indeed, moving away from algorithmic discrimination and toward algorithmic fairness, where the data may be free of biases, is one possible answer.

Thus, developers should ensure high-quality data through community feedback, which helps refine and enhance the system's accuracy and reliability. Therefore, it is essential to deploy FRS in high-risk activities with trained personnel who understand the implications and potential misuse of this technology. The main goal must be to establish trustworthy technology in which FRS can be employed under legitimate circumstances and to take advantage of Artificial intelligence technologies that have the potential to make people's lives easier.

REFERENCES

Almotiri, J. (2022). Face recognition using principal component analysis and clustered self-organizing map. *International Journal of Advanced Computer Science and Applications, 13*(3). https://dx.doi.org/10.14569/IJACSA.2022.0130361

Baio, C. (2014). A impureza da imagem: Estéticas intersticiais entre a fotografia analógica e digital. *Galáxia, 14*(28), 134-145. http://dx.doi.org/10.1590/1982-25542014219195

Council of the European Union. (2002). Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. Official Journal of the European Communities, L 190, 1-20. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584

Court of Justice of the European Union, Fourth Chamber. (2014). Judgment in Case C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, 11 December 2014. Retrieved from https://gdprhub.eu/index.php?title=CJEU_-_C-212/13_-_Franti%C5%A1ek_Ryne%C5%A1

Edgar, A., Duéñez-Guzmán, K. R., McKee, K., Mao, Y., Coppin, B., Chiappa, S., Vezhnevets, A., Bakker, M. A., Bachrach, Y., Sadedin, S., Isaac, W. S., Tuyls, K., & Leibo, J. Z. (2021). Statistical discrimination in learning agents. *arXiv: Learning*. https://doi.org/10.48550/arXiv.2110.11404

European Commission. (2021). Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain Union legislative acts. European Commission.

European Court of Human Rights [ECHR], First Section. (2016). Application no. 4755/16, Sylvie Beghal against the United Kingdom, lodged on 14 January 2016, communicated on 22 August 2016. Retrieved from https://hudoc.echr.coe.int/eng/?i=001-166724

European Court of Human Rights, Fourth Section. Peck v. The United Kingdom (Application no. 44647/98). Judgment. (2003). Available online: https://opil.ouplaw.com/display/10.1093/law:ihrl/3168echr03.case.1/law-ihrl-3168echr03

European Data Protection Board and European Data Protection Supervisor. (2021). Joint opinion on the proposal for a regulation on artificial intelligence (AI regulation). Retrieved from https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (AIA). Official Journal of the European Union, L 190, 12.7.2024.

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. (2021). Biometric recognition and behavioral detection techniques with a focus on their current and future use in public spaces. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

European Union. (2016). 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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

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

High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI.* European Commission. https://ec.europa.eu/digital-strategy/our-policies/ethics-guidelines-trustworthy-ai_en

High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI.

Huang, J. (2012). U.S. Patent Application No. 13/155,441.

Leslie, D. (2020). *Understanding bias in facial recognition technologies: An explainer.* The Alan Turing Institute. https://doi.org/10.5281/zenodo.4050457

Libin, X., Xiaoyu, L., Yang, L., Lei, N., & Jiaqi, W. (2024). Research on the application of CNN face recognition technology in the airport. *Advances in transdisciplinary engineering, 57,* 190-199. https://doi.org/10.3233/atde240470

Liu, Y. (2024). Unveiling bias in artificial intelligence: Exploring causes and strategies for mitigation. Applied and Computational Engineering, 76,124-133. https://doi.org/10.54254/2755-2721/76/20240576

Mishra, I., Kashyap, V., Yadav, N. K., & Pahwa, R. (2024). Harmonizing intelligence: A holistic approach to bias mitigation in artificial intelligence (AI). *International Research Journal on Advanced Engineering Hub (IRJAEH), 2*(7), 1978-1985. https://doi.org/10.47392/irjaeh.2024.0270

Niedbała, M. (2023). The problem of criminal liability for generating pornography using artificial intelligence. *Krytyka Prawa Niezależne Studia nad Prawem, 15*(4), 69-79. https://doi.org/10.7206/kp.2080-1084.639

Pangelinan, G., Krishnapriya, K. S., Albiero, V., Bezold, G., Zhang, K., Vangara, K., King, M. C., & Bowyer, K. W. (2024). Exploring causes of demographic variations in face recognition accuracy. En K. Bowyer (Ed.), *Computer vision* (pp. 1-21). Chapman and Hall/CRC.

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 815-823). IEEE. https://doi.org/10.1109/CVPR.2015.7298682

Suganthy, M., Manjula, S., Kavitha, M., & Anandhan, P. (2022). *Transmission of biometric feature using facial features securely for long distance biometric recognition system.* IEEE. https://doi.org/10.1109/ICESIC53714.2022.9783491

Zhong, H. (2024). Implementation of the EU AI act calls for interdisciplinary governance. *AI Magazine*. https://doi.org/10.1002/aaai.12183