

# ETHICAL CHALLENGES OF FACIAL RECOGNITION IN PUBLIC SPACES

**Dr. Sarvesh Kumar Shahi**

Assistant Professor-II

KIIT School of Law

KIIT Deemed to be University, Bhubaneswar, Odisha, India

## Abstract

Facial recognition technology is increasingly used in publicly accessible environments such as streets, transport hubs, airports, stadiums, shopping districts, campuses, and government facilities. These systems can compare faces captured by cameras with reference images in order to verify identity, locate a person of interest, or produce candidate matches. Supporters argue that the technology may assist with security, missing-person searches, access management, and the investigation of serious offences. Yet public-space deployments are ethically distinct from voluntary one-to-one verification because they may capture and analyse the biometric information of many people who have not chosen to participate.

This study uses a qualitative, literature-based approach to examine the ethical challenges associated with facial recognition in public spaces. It reviews privacy, consent, proportionality, accuracy, demographic fairness, transparency, accountability, freedom of expression and assembly, data retention, and institutional governance. The analysis follows the lifecycle of a public-space facial recognition deployment: purpose definition, legal authority, watchlist design, image collection, biometric comparison, human review, intervention, record retention, audit, and remedy. It also considers how public and private organisations share responsibility when surveillance infrastructure is operated across complex urban environments.

The study finds that the ethical acceptability of facial recognition depends on more than technical accuracy. A system may perform well in a laboratory yet still create unjustified monitoring, unequal burdens, weak due process, or chilling effects in public life. Ethical deployment requires a narrowly defined purpose, an evidence-based necessity assessment, strict temporal and geographic limits, independent oversight, meaningful public transparency, bias and performance testing, trained human review, secure deletion practices, and accessible remedies for affected individuals. The paper concludes that facial recognition in public spaces should be treated as a high-impact sociotechnical practice, not merely as a camera upgrade.

**Keywords:** Facial Recognition, Public Surveillance, Biometric Data, Privacy, Algorithmic Bias, Human Rights, Accountability, Consent, Ethical Governance, Artificial Intelligence

## 1. INTRODUCTION

Facial recognition technology (FRT) uses computational methods to detect a face in an image or video stream and compare its features with another image or a database of enrolled identities. Its uses range from device unlocking and border control to police investigations, retail security, access control, and event management. The ethical concerns are especially acute when FRT operates in public spaces because it may process the faces of people who are simply travelling, working, shopping, attending a public event, or exercising civic rights. Live facial recognition differs from an ordinary camera system because it can turn an image into biometric

information that is capable of linking a person to a watchlist or identity record [3, 5].

Public-space facial recognition is often presented as a tool for safety and efficiency. In limited contexts, it may help authorities identify a missing person, locate a suspect subject to lawful process, or manage secure entry to a restricted area. However, a claim of utility does not resolve the central ethical question: whether the scale, intrusiveness, and consequences of the surveillance are justified in relation to a specific public purpose. The assessment must take account of people who are not suspected of wrongdoing, the possibility of false matches, the cumulative effect of repeated monitoring, and the unequal

impact that errors may impose on particular groups [8, 10].

Unlike conventional identification checks, public-space FRT can function without a direct interaction between the organisation and the person being scanned. Notice may be limited, consent may not be meaningful, and a person may have no practical way to avoid the monitored area. The technology may also involve several actors: camera owners, software vendors, security contractors, data controllers, law-enforcement agencies, and public authorities. This distributed environment can make it difficult to determine who is responsible for data quality, watchlist governance, technical testing, human decisions, and redress when harm occurs.

This paper examines facial recognition through an ethical governance perspective. It reviews the key literature and regulatory principles, identifies the major risks of public-space deployment, and develops a practical framework for evaluating whether a proposed use is necessary, proportionate, fair, transparent, and accountable. The purpose is not to assume that every application should be treated identically, but to clarify the safeguards that must be considered before, during, and after any high-impact biometric surveillance activity.

## 2. LITERATURE REVIEW

Research on facial recognition has developed alongside advances in computer vision, machine learning, camera infrastructure, and large-scale biometric databases. Technical work often focuses on detection accuracy, false match rates, false non-match rates, image quality, and the performance of one-to-one verification or one-to-many identification systems. Independent testing has shown that performance varies with system design, image conditions, demographics, and operational thresholds. This means that a reported accuracy figure cannot be treated as a universal guarantee of reliable identification in a crowded, uncontrolled public setting [8, 9]. Ethical and legal scholarship has expanded the analysis beyond accuracy. Researchers emphasize that biometric surveillance can interfere with privacy, data protection, dignity, equality, freedom of movement, expression, assembly, and association. Even where a system does not produce an arrest or other

formal intervention, broad scanning may change how people experience public life. The concern is therefore not only whether a match is correct, but whether it is legitimate to identify or track people at scale in the first place [6, 11, 22].

Recent governance literature treats FRT as a sociotechnical system rather than a standalone algorithm. Its impacts depend on image source quality, database composition, watchlist criteria, thresholds, operator training, escalation policies, records management, procurement terms, and oversight arrangements. Bias can arise from data collection, model design, deployment context, and institutional practices. A governance approach must therefore assess the entire decision pathway from camera capture to any human action taken after a candidate match [14, 17, 18].

### 2.1 FACIAL RECOGNITION IN PUBLIC-SPACE ENVIRONMENTS

- Public-space FRT may be deployed through fixed CCTV cameras, mobile cameras, body-worn devices, drones, venue entry systems, or footage analysed after an event.
- The technology can be used for verification, identification, or categorisation. These functions have different risks and should not be treated as ethically equivalent.
- Live deployments may compare many passing faces with a watchlist in real time, whereas retrospective deployments analyse recorded footage after an incident.
- Public uses often involve people who have not enrolled, are not the target of the operation, and may be unable to avoid the monitored location without altering ordinary daily activities.

### 2.2 ETHICAL RISKS OF FACIAL RECOGNITION

- Privacy and autonomy are affected when facial images are converted into biometric identifiers without a meaningful opportunity to choose or refuse.
- False matches can lead to questioning, denial of access, reputational harm, stress, or disproportionate police attention, especially when operators over-rely on algorithmic outputs.
- Demographic performance differences and unequal surveillance patterns can intensify existing discrimination and expose

marginalised communities to greater scrutiny.

- Poor transparency can prevent individuals from knowing where FRT is used, what data are retained, how decisions are made, and how to challenge errors.
- Chilling effects may arise where people believe that attendance at protests, religious gatherings, labour meetings, political events, or other lawful activities can be recorded and identified.

## 2.3 GOVERNANCE AND REGULATORY PRINCIPLES

- Human-rights and data-protection approaches require a lawful basis, a defined purpose, necessity, proportionality, data minimisation, security, and accountability.
- Regulatory guidance increasingly distinguishes consent-based, one-to-one uses from wide-area surveillance that captures people in public spaces without direct participation.
- The European Union AI Act places particular restrictions on real-time remote biometric identification in publicly accessible spaces for law-enforcement purposes, while other frameworks require robust impact assessment and oversight [4, 5].
- Independent testing, public reporting, clear human decision authority, and accessible complaint mechanisms are essential where a system can affect liberty, mobility, or equal treatment.

## 3. OBJECT OF STUDY

The present study examines facial recognition systems used in publicly accessible spaces as high-impact biometric surveillance

environments. The object of study is not a single vendor, city, or deployment. Instead, it considers the ethical requirements that arise across different public settings where cameras may capture large numbers of individuals and compare their facial features with a reference source. The analysis focuses on the relationship between technical operation and social consequence, including how system design, policy choices, and institutional power affect people who are scanned or identified.

The theoretical basis of the study is grounded in the principle that any use of biometric identification in public life should preserve human dignity, equality, and the ability to move, speak, assemble, and participate without unnecessary observation. This requires more than a privacy notice or an accuracy claim. A legitimate deployment must be supported by a clear purpose, an evidence-based assessment of necessity, a limited scope, safeguards against discrimination, meaningful human control, transparent governance, and a realistic route for correction and remedy. The study therefore treats FRT as an interconnected system of cameras, data, algorithms, operators, policies, and public accountability.

## 3.1 PUBLIC-SPACE DEPLOYMENT CONTEXTS AND ETHICAL REQUIREMENTS

The study considers representative public-space contexts that show how purpose, risk, and safeguards may vary across facial recognition deployments. These contexts are selected because they illustrate the practical difficulty of applying biometric technology in locations used by diverse and often non-consenting populations.

| S. No. | Public-Space Setting                      | Typical Deployment Purpose                                  | Main Ethical Concern                                             | Essential Safeguard                                                             |
|--------|-------------------------------------------|-------------------------------------------------------------|------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 1      | Transport hubs and airports               | Security screening, missing-person response, access control | Continuous monitoring of travellers and false match consequences | Narrow purpose, high match threshold, human verification, retention limits      |
| 2      | Streets, public squares, and city centres | Police watchlist scanning or post-event investigation       | Mass surveillance, weak notice, chilling of civic participation  | Specific legal authority, geographic and time limits, independent authorisation |
| 3      | Stadiums and large events                 | Crowd safety, ticket fraud, exclusion                       | Function creep from safety to broad                              | Clear event-specific policy, alternatives for                                   |

|   |                                          | enforcement                                         | behaviour monitoring                                           | non-consenting visitors, deletion schedule                                          |
|---|------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 4 | Retail and commercial districts          | Loss prevention, access control, customer analytics | Private entities identifying people without meaningful consent | Strict necessity test, transparent signage, no secondary marketing use, audit trail |
| 5 | Educational and health-adjacent campuses | Entry management, security alerts                   | Power imbalance and impact on vulnerable communities           | Voluntary alternatives where possible, heightened safeguards, independent review    |

### 3.2 STUDY OBJECTIVES

- To examine the ethical implications of facial recognition technology used in publicly accessible spaces.
- To identify the privacy, fairness, autonomy, transparency, and human-rights risks associated with biometric surveillance.
- To compare ethical requirements across transport, policing, commercial, event, and campus settings.
- To evaluate the importance of legal authority, necessity, proportionality, data minimisation, human review, and remedy.
- To develop a practical governance framework for responsible evaluation of public-space facial recognition systems.

### 4. RESEARCH METHODOLOGY

The study adopts a qualitative and literature-based research methodology. It synthesises peer-reviewed scholarship, technical evaluation reports, data-protection guidance, human-rights materials, legal decisions, and governance frameworks relevant to facial recognition. This approach is appropriate because the research question concerns the ethical relationship between biometric surveillance, public space, and institutional decision-making rather than the measurement of a single technical outcome. The analysis uses a comparative framework to examine how ethical requirements differ according to deployment purpose, population exposure, data source, intervention risk, and accountability arrangements.

The methodological framework follows the lifecycle of a public-space FRT deployment. It considers the formulation of a public purpose, the identification of legal authority, the creation or use of a watchlist, image capture, biometric comparison, candidate-match

review, human intervention, data retention, independent audit, and complaint handling. The study also examines how public participation, procurement controls, and transparency obligations affect the legitimacy of systems operated by public bodies, private contractors, or partnerships between them.

### 4.1 RESEARCH DESIGN (QUALITATIVE ANALYTICAL APPROACH)

- The study follows a qualitative and comparative design based on ethical, technical, legal, and policy literature on facial recognition.
- The analysis compares public-space settings according to exposure of non-targeted people, purpose limitation, data sensitivity, and consequences of error.
- The study uses a lifecycle perspective that links technical design decisions with public accountability and human-rights outcomes.
- Findings are interpreted through ethical governance principles rather than through experimental testing or a population survey.

### 4.2 ETHICAL GOVERNANCE FRAMEWORK

- Necessity and proportionality are used to assess whether facial recognition is genuinely required for a defined purpose and whether less intrusive options are available.
- Privacy and data protection are assessed through lawful basis, data minimisation, security, retention limits, purpose limitation, and restrictions on secondary use.
- Fairness is assessed through demographic performance testing, watchlist quality, unequal deployment patterns, and safeguards against discriminatory impact.

- Accountability is assessed through clearly assigned responsibility, independent oversight, documentation, audit logs, and meaningful individual remedy.
- Human control is assessed through operator training, clear escalation rules, prohibition of fully automated adverse action, and documented review of candidate matches.

#### 4.3 PUBLIC-SPACE AND INSTITUTIONAL CONTEXT

- The study considers deployments in transport hubs, public streets, event venues, retail districts, campuses, and other locations where people may enter for ordinary activities.
- Facial recognition is treated as a process involving images, facial templates, watchlists, match scores, operator decisions, logs, and retention policies.
- Access and intervention are evaluated in relation to public safety, commercial security, civic participation, equality, privacy, and due process.
- Institutional capacity is considered through governance policies, procurement standards, technical expertise, oversight arrangements, funding, and staff training.

#### 4.4 PARAMETERS OF ANALYSIS

The following ethical and governance parameters are evaluated:

- Clarity of purpose, evidence of necessity, and availability of less intrusive alternatives
- Scope of image capture, population exposure, watchlist design, and data minimisation
- Algorithmic performance, demographic differentials, threshold setting, and false-match management
- Human review procedures, intervention rules, documentation, and auditability
- Transparency, public notice, consultation, contestability, and individual remedy
- Legal, ethical, and human-rights appropriateness of the deployment and its institutional governance

#### 4.5 PROCEDURE OF STUDY

- Review research, standards, court decisions, regulator guidance, and human-rights materials relating to facial recognition and public surveillance.

- Identify recurring ethical risks involving privacy, consent, discrimination, accuracy, transparency, and civic freedoms.
- Compare representative public-space deployment contexts and the forms of harm that may arise in each setting.
- Map ethical requirements to governance practices involving data, algorithms, human operators, procurement, and oversight.
- Interpret the combined findings to formulate a rights-respecting governance framework.
- Develop practical recommendations for organisations considering any high-impact public-space facial recognition deployment.

#### 4.6 ANALYTICAL APPROACH

- Qualitative comparison of ethical risks and safeguards across different public settings and operational models.
- Interpretation of how technical accuracy, human review, and institutional policy combine to shape outcomes for affected persons.
- Assessment of the relationship between surveillance design, public trust, legal legitimacy, and democratic participation.
- Identification of governance practices that can be applied by public authorities, venue operators, technology vendors, and independent regulators.

#### 5. DATA ANALYSIS

The qualitative analysis indicates that public-space facial recognition cannot be assessed only by asking whether the software can match faces. The ethical significance of a deployment depends on who is scanned, why they are scanned, how long data are retained, what database is used, who reviews a candidate match, and what action follows. A technically accurate system may still be ethically unjustified when it scans an entire population to identify a small number of people without demonstrating that the same objective cannot be achieved through less intrusive means.

The comparative assessment shows that exposure is a central factor. A traveller entering a secure border-control lane may receive clearer notice and may be participating in an identity process linked to a defined travel purpose. A pedestrian in a public square, by

contrast, may be scanned without a direct interaction, may not know the system is operating, and may not have a practical alternative route. This difference affects the strength of consent, the expectation of privacy, and the burden on the organisation to justify necessity and proportionality [5, 12].

Accuracy remains ethically important because false matches can create serious individual consequences. Performance may vary according to image quality, lighting, camera angle, database conditions, demographic representation, and threshold settings. In a public setting, even a low error rate can affect many people when a large population is scanned. For this reason, candidate matches should never be treated as proof of identity. Systems require trained human reviewers, clear rules against automatic adverse action, records of review decisions, and regular independent testing using conditions relevant to the actual deployment [8, 9, 15].

The analysis also shows that fairness is not limited to statistical parity. Communities may experience unequal burden because cameras are placed more heavily in particular neighbourhoods, watchlists are created from uneven policing practices, or false-match interventions are concentrated among populations already subject to disproportionate surveillance. A fair governance model must examine both algorithmic performance and the social distribution of surveillance. It should include impact assessments, representative performance testing, deployment mapping, public reporting, and corrective action where unequal impacts are identified [14, 16, 17].

Finally, governance and accountability determine whether safeguards work in practice. Policies that exist only on paper cannot prevent function creep or misuse. Effective systems need a named accountable authority, documented decision rights, vendor obligations, audit logs, independent oversight, deletion schedules, and a complaint process that can lead to correction or remedy. Transparency should explain not only that FRT is used, but also the purpose, location, time period, legal authority, watchlist category, data retention, human-review process, and the results of audits in an accessible form.

## 6. DISCUSSION

The analysis confirms that facial recognition in public spaces is a governance challenge as much as a technical one. It can provide benefits in carefully limited situations, but its capacity to identify people at scale changes the character of public surveillance. Traditional CCTV records activity for later review; FRT can convert a passing face into a biometric query. This creates a heightened risk that ordinary, lawful presence in public becomes a source of data for identification, tracking, or future analysis. The ethical baseline should therefore be higher than the baseline applied to ordinary video recording.

A central lesson is that public notice alone is not enough. Signs may inform people that cameras are present, but they do not necessarily provide a realistic choice, explain the operation of a watchlist, or protect against discriminatory or disproportionate use. Consent should not be presumed merely because an individual walks through a monitored street, station, or shopping district. Where power is unequal or avoidance is impractical, the organisation must rely on a strong legal and ethical justification rather than on a formalistic claim of participation.

The strongest governance approach is layered. It combines a precise legal mandate, documented necessity and proportionality, strict limits on purpose and scope, careful watchlist governance, local performance testing, human review, data-security controls, public transparency, independent authorisation for sensitive uses, audit, and remedy. The framework must also regulate procurement. Vendors should not be allowed to retain facial data for unrelated product development, change models without review, or conceal material information needed for independent assessment. Contractual terms should support auditability, security, deletion, and accountability throughout the system lifecycle. Public trust depends on whether institutions treat people as rights holders rather than as passive sources of biometric data. Consultation with affected communities, civil-society organisations, data-protection experts, and technical specialists can improve policy design and identify harms that are invisible in a narrow security analysis. In high-risk settings such as protests, political events, religious

gatherings, and areas involving children or vulnerable populations, a presumption against broad facial recognition surveillance is ethically justified unless an exceptional, clearly evidenced, and independently authorised need can be demonstrated.

## 7. CONCLUSION

This study examined the ethical challenges of facial recognition technology in public spaces. It showed that the central issues extend beyond recognition accuracy to include privacy, autonomy, fairness, transparency, accountability, freedom of expression and assembly, data governance, and due process. Public-space systems can expose large numbers of non-targeted individuals to biometric analysis, and their impact is shaped by the full operational chain of camera

placement, watchlist creation, algorithmic matching, human interpretation, intervention, retention, and oversight.

The analysis found that ethically responsible use requires a narrowly defined purpose, a credible necessity assessment, proportional limits, strong data protection, rigorous performance and bias testing, trained human review, public transparency, independent oversight, and accessible remedy. Where these conditions cannot be met, or where the deployment creates a high risk of mass surveillance or chilling of public participation, facial recognition should not be used. Organisations should approach FRT as a continuing ethical responsibility requiring review, evidence, and accountability from initial design through final deletion of data.

## 8. REFERENCES

1. United Nations. (1948). *Universal Declaration of Human Rights*. United Nations. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>
2. United Nations. (1966). *International Covenant on Civil and Political Rights*. United Nations Treaty Series, 999, 171. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
3. European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1-88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. European Parliament and Council. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
5. European Data Protection Board. (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0*. [https://www.edpb.europa.eu/system/files/2023-05/edpb\\_guidelines\\_202304\\_frtlawenforcement\\_v2\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf)
6. Office of the United Nations High Commissioner for Human Rights. (2022). *The right to privacy in the digital age (A/HRC/51/17)*. United Nations. <https://www.ohchr.org/en/privacy-in-the-digital-age>
7. Council of Europe. (2021). *Guidelines on facial recognition*. Consultative Committee of Convention 108. <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>
8. Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*. NISTIR 8280. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
9. National Institute of Standards and Technology. (2026). *Face Recognition Technology Evaluation (FRTE)*. <https://pages.nist.gov/frvt/html/frvt11.html>
10. National Academies of Sciences, Engineering, and Medicine. (2024). *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance*. National Academies Press. <https://doi.org/10.17226/27397>
11. European Union Agency for Fundamental Rights. (2019). *Facial recognition technology: Fundamental rights considerations in the context of law enforcement*. <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>
12. Information Commissioner's Office. (2021). *Information Commissioner's Opinion: The use of live facial recognition technology in public places*.

- <https://ico.org.uk/media2/migrated/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf>
13. *R (Bridges) v Chief Constable of South Wales Police and others* [2020] EWCA Civ 1058. Court of Appeal (Civil Division), United Kingdom.
  14. Garvie, C., Bedoya, A. M., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown Law Center on Privacy & Technology. <https://www.perpetuallineup.org/>
  15. Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1-15. <https://proceedings.mlr.press/v81/buolamwini18a.html>
  16. Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 429-435. <https://doi.org/10.1145/3306618.3314244>
  17. Barocas, S., & Selbst, A. D. (2016). *Big data's disparate impact*. *California Law Review*, 104(3), 671-732. <https://doi.org/10.15779/Z38BG31>
  18. Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 59-68. <https://doi.org/10.1145/3287560.3287598>
  19. Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). *Accountable algorithms*. *University of Pennsylvania Law Review*, 165, 633-705. [https://scholarship.law.upenn.edu/penn\\_law\\_review/vol165/iss3/3/](https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/)
  20. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76-99. <https://doi.org/10.1093/idpl/ix005>
  21. Citron, D. K., & Pasquale, F. (2014). *The scored society: Due process for automated predictions*. *Washington Law Review*, 89, 1-33. <https://ssrn.com/abstract=2376209>
  22. Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.
  23. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
  24. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
  25. Kindt, E. J. (2013). *Privacy and data protection issues of biometric applications: A comparative legal analysis*. Springer. <https://doi.org/10.1007/978-94-007-7522-0>
  26. Introna, L., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2(2/3), 177-198. <https://doi.org/10.24908/ss.v2i2/3.3373>
  27. Smith, M. L., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI and Ethics*, 2, 151-169. <https://doi.org/10.1007/s43681-021-00058-8>
  28. Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People: An ethical framework for a good AI society. *Minds and Machines*, 28, 689-707. <https://doi.org/10.1007/s11023-018-9482-5>
  29. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389-399. <https://doi.org/10.1038/s42256-019-0088-2>
  30. UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>