International Journal of Law, Ethics and Social Sciences

Article

In the Age of Facial Recognition, Where Do Our Rights Belong?

Yiqing Shi [1,*]

[1] The Experimental High School Attached to Beijing Normal University, Beijing, China
* Correspondence: Yiqing Shi, The Experimental High School Attached to Beijing Normal University, Beijing, China

Abstract: Facial recognition has moved from the laboratory and the checkpoint into ordinary urban life, and the question it raises is no longer technical but political: who may hold the human face, and on what terms? This paper compares how the European Union, the United States, China, India, and a range of developing economies govern facial recognition, and asks why jurisdictions that increasingly share a common regulatory vocabulary-risk-based classification, contextual differentiation, necessity and proportionality, transparency and accountability-still diverge so sharply over the rights they treat as foundational. It argues that these divergences express deeper choices about whether privacy is an inherent right or one interest among many, and about whether rules should be unified and strict or fragmented and flexible. The paper then traces the costs of that divergence: digital borders that obstruct cross-border trade, the concentration of technological power, differing rules on cross-border data flows, and contested standards of fairness. It concludes that global governance should protect a shared moral boundary, namely no large-scale and indiscriminate surveillance and no permanent digital record of ordinary life, while leaving room for institutional diversity.

Keywords: facial recognition; privacy; personal data protection; risk-based regulation; comparative law; algorithmic accountability

1. Introduction

The age of facial recognition has arrived quietly.

Cameras in London may be quietly recognize people on the street. The Smart Nation initiative in Singapore will be applied to recognize faces in daily life [1]. In many Chinese cities, people are already used to using their faces to pay, enter subway stations or even pick up packages. However, there is a problem with this convenience: do I still consider myself the same? And what exactly do governments and companies do with my face data?

Different places around the world have very different answers [2-6]. All of the above are different modes of regulation that can be considered social experiments, and they provide a worldwide laboratory for observing how technology changes society and, at the same time, how society establishes rules for technology.

2. The Growing Global Consensus on Risk, Context and Necessity

Although the national laws are different, policymakers around the world are starting to use the same regulatory "language" (As shown in Table 1).

Received: 30 August 2026
Revised: 22 October 2026
Accepted: 05 November 2026
Published: 12 November 2026

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Table 1. Convergence Principles in Global Governance of Facial Recognition.

Principle	Core Idea	Brief Interpretation and International Example
Risk-based regulation	The higher the risk, the stricter the control.	Facial recognition is not treated as a single category of technology; instead, its risks are assessed based on how and where it is used.
Contextual differentiation	Privacy expectations depend on context.	Being recorded in a public restroom feels fundamentally different from being filmed in a sports stadium, and many legal systems now acknowledge this distinction.
Necessity and proportionality	Technology should not be used when less intrusive alternatives can achieve the same goal.	Facial recognition must be genuinely necessary for a legitimate purpose, such as locating a criminal suspect, and should not exceed what that purpose requires.
Transparency and accountability	Surveillance systems should not operate as "black boxes."	It must be clear who is using the technology, how it is used, and who is responsible when harm occurs.

The above reasons show that digital government is changing. Instead of prohibiting or permitting the technology entirely, many countries are adopting a "traffic light" approach to safely advance the development of the technology and not shut down the road [4].

3. The Rights Behind Facial Recognition and Choices in Regulatory Style

Although the regulations in many countries are the same, their backgrounds in history, culture and institutions are different.

Is privacy an inherent right, or one interest among many?

According to the General Data Protection Regulation (GDPR) in the EU, facial data falls under the category of "special categories of personal data" and generally needs explicit consent for processing; however, there are some exemptions [7]. It shows that people believe that privacy is a basic right guaranteed to all in life [8,9].

China has released a Personal Information Protection Law and particular regulations on facial recognition [10-12]. The framework is more focused on balancing people's right to know with the goals of cybersecurity and public interest, so the rights of individuals are considered in the larger system of governance [13].

India is a more complicated case. The Puttaswamy case of the Supreme Court of India established the right to privacy in the Constitution [14,15]. Aadhaar is a large-scale project in India to improve the distribution of welfare benefits and promote financial inclusion, so at present, the focus is on administrative efficiency and the achievement of development goals.

Should regulation be unified and strict, or fragmented and flexible?

The EU wants uniform rules and actively spreads its standards around the world. The US is a federation and has no national facial recognition law; thus, only the individual states regulate it.

China has a different type. Regulations are issued centrally and rolled out uniformly across the country from the top down promptly. The first is the institution-led model.

4. Rules-And the Problems They Produce

4.1. Regulatory Barriers and Difficult Trade-Offs

Governance Rules protect the rights of people and also regulate the economy. Divergent Standards will be a "digital border" to restrict cross-border trade. A company planning to use facial recognition technology in both the EU and China will have to meet

two very different regulatory systems. With time passing, the two will be in competition to lead the new-technology revolution around the world.

Many developing countries are using facial recognition technology to improve the efficiency of government services and reduce costs. Weak Institutional Supervision will result in abuse of power and increased inequality [16]. The other is that there will be a "digital Leviathan" and thus less freedom.

4.2. Shared Global Challenges

All societies have faced some problems along the way.

The Concentration of Technological Power. How to prevent governments and large enterprises from using facial recognition technology indiscriminately to set up a "surveillance eye" [17,18]. Will there be independent supervisory bodies and mandatory algorithmic audits?

Cross-Border Data Flow. The face data is in the cloud and may be subject to the laws of several countries. EU's Adequacy Decisions and the US CLOUD Act and China's Data-Localisation Requirements are often in conflict.

Standards of Fairness. How should algorithmic bias be defined and measured? And who will set the standards: Technology companies, governments or international organisations?

5. Conclusion: Protecting the Shared Moral Boundary in a Diverse World

The EU has established a "wall of rights" around the world, the US continues its "market-oriented experiment", China is promoting a "systematic governance project", and many developing countries have chosen pragmatic paths. Despite the differences mentioned above, a problem still exists: Are we willing to let technology change our traditional ideas of dignity, freedom and equality without our knowledge?

The final goal of global governance should be to protect what cannot be changed, even if there are differences. Three boundaries can be defended even across divergent regimes: (1) a prohibition on large-scale, indiscriminate surveillance of public space, reflected in Article 5 of the EU AI Act and in the necessity-and-minimal-impact requirement of China's 2025 Measures; (2) a bar on making facial verification the sole gateway to essential services, codified in China's Measures and increasingly recognised under EU non-discrimination law; and (3) limits on the permanent retention of facial records of ordinary life, grounded in GDPR data-minimisation and in S. and Marper v. the United Kingdom.

When young people, scholars, policymakers and ordinary people begin to think seriously about these issues, that very thinking becomes a source of hope. Therefore, although technology has advanced rapidly, people have not lost the will to question, choose and shape their own destinies.

References

1. R. Jiang et al., *Big Data Privacy and Security in Smart Cities*. Cham, Switzerland: Springer, 2022.
2. European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices," Version 2.0, EDPB, Brussels, Belgium, 2020. [Online]. Available: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
3. Council of Europe, Consultative Committee of Convention 108, "Guidelines on facial recognition," Council of Europe, Strasbourg, France, 2021. [Online]. Available: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html
4. European Parliament and Council of the European Union, "Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)," *Off. J. Eur. Union*, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
5. "TAKE IT DOWN Act," S. 146, 119th Cong., 2025. [Online]. Available: https://www.congress.gov/bill/119th-congress/senate-bill/146
6. Cyberspace Administration of China and Ministry of Public Security, "Measures for the security management of the application of facial recognition technology," Beijing, China, Mar. 2025. [Online]. Available: https://www.cac.gov.cn/2025-03/21/c_1744174262156096.htm

7. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 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)," *Off. J. Eur. Union*, vol. 59, no. L 119, pp. 1–88, 2016.
8. *Carpenter v. United States*, 585 U.S. 296, 2018.
9. *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, Eur. Ct. H.R. (Grand Chamber), Dec. 4, 2008.
10. X. Wang, "The right to data portability and distributive justice in data governance," *Global Law Rev.*, no. 6, pp. 5–22, 2021.
11. X. Ding, "Institutions and scenarios: Reconstructing facial recognition and facial image information protection," *Administrative Law Rev.*, vol. 155, no. 1, pp. 48–63, 2026.
12. D. Lao, "Fundamental goal and imputation mechanism of the personal information protection law system," *Tribune Political Sci. Law*, vol. 39, no. 6, pp. 3–17, 2021.
13. *Information security technology—Security requirements for facial recognition data*, GB/T 41819–2022, Standardization Administration of China, Beijing, China, 2022.
14. *Justice K. S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors.*, Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, Aug. 24, 2017.
15. M. Guruswamy, "Justice K.S. Puttaswamy (Ret'd) and Anr v. Union of India and Ors.," *Amer. J. Int. Law*, vol. 111, no. 4, pp. 994–1000, 2017.
16. J. van Dijk, *The Digital Divide*. Cambridge, U.K.: Polity Press, 2020.
17. K. A. Bamberger, "Regulation as delegation: Private firms, decisionmaking, and accountability in the administrative state," *Duke Law J.*, vol. 56, no. 2, pp. 377–468, 2006.
18. X. He et al., "Diff-Privacy: Diffusion-based face privacy protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 34, no. 12, pp. 13164–13176, 2024.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of Publisher and/or the editor(s). Publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.