IDOS German Institute of Development and Sustainability

IDOS POLICY BRIEF 19/2025

Global Frameworks for Regulating Facial Recognition Technology and Artificial Intelligence

Adaptive and Inclusive Governance

Kerem Öge & Manuel Quintin

Summary

Despite growing awareness, the global regulation of facial recognition technology (FRT) remains fragmented, much like the governance of Artificial Intelligence (AI). International initiatives from the United Nations (UN), Organisation for Economic Co-operation and Development (OECD), and World Economic Forum (WEF) provide guiding principles but fall short of enforceable standards. On 27 July 2025, UN tech chief Doreen Bogdan-Martin warned that the world urgently needs a global approach to AI regulation, as fragmented efforts risk deepening inequalities.

This policy brief explores how FRT challenges existing governance frameworks due to its rapid development, complexity and ethical implications. Our research shows that delays in regulation are not only caused by the rapid pace of technological change but also by whose voices are included in the debate. In FRT debates, early warnings from civil society about privacy and rights were sidelined until echoed by governments and major tech firms. This lack of representation, as much as the rapid pace of innovation, helps explain why regulation so often lags behind public concerns. To better govern FRT, the policy brief proposes an adaptive and inclusive model that balances flexibility with democratic legitimacy. Adaptive governance, marked by decentralised decision-making, iterative policy learning, and responsiveness, helps address the uncertainties and evolving risks of narrow AI applications like FRT. Inclusivity is equally critical in legitimising FRT governance.

We propose three policy recommendations to national regulators, multilateral bodies and regional policymakers for future AI governance: (1) require transparent labelling of AI systems, (2) reframe AI as a societal issue, not just a security tool, and (3) embed civil society in AI governance forums. Taken together, these actions would promote a more proactive, equitable and context-sensitive framework for regulating AI globally. These recommendations are particularly timely ahead of the AI Impact Summit, scheduled for February 2026 in Delhi, which will bring global policymakers together to shape an international vision for AI governance that includes FRT.

Background

AI is at the centre of global debates on ethics and policy, echoing past technological shifts from the printing press to the internet that sparked uncertainty over risks and benefits (Acemoglu & Johnson, 2023). Emerging technologies are hard to govern because they develop rapidly and exceed the capacity of existing laws and institutions to respond. To explore this gap between technological progress and regulatory change, this policy paper focuses on a specific subset of AI: FRT. It specifically builds on the FRAMENET (2025) project, which tracks the evolution of global public debates through systematic discourse analysis. Beyond its immediate implications, FRT regulation serves as a test case for building coherent multilateral norms and ensuring consistency across regimes, challenges that also shape climate, health and digital governance.

FRT is a biometric system that verifies identity by matching facial features from images or video with stored databases, using machine learning as a form of narrow AI. The rapid expansion of FRT raises serious civil and human rights concerns. FRT systems can undermine privacy by harvesting large amounts of personal data from surveillance or social media without consent (Leong, 2019). Certain applications of this technology exhibit algorithmic bias, especially against women and people of colour, raising concerns about its reliability in law enforcement (Buolamwini & Gebru, 2018).

In authoritarian regimes, FRT enables digital repression by monitoring citizens, suppressing dissent, and controlling minority populations. In democracies, legal oversight is often weak, and private companies may share surveillance data with law enforcement without accountability (Frantz et al., 2020). These concerns have grown with the increasing use of real-time facial recognition, whereby police cameras scan crowds to match faces against undisclosed watchlists. These developments have prompted citizens, civil society and activists to call for stronger regulation, echoing wider demands for global AI governance. Yet the form such governance should take remains unclear. Traditional approaches fall short not only in keeping pace with rapid technological change and its ethical implications but also in including diverse voices in the debate. This policy paper explores two central questions: How should FRT be regulated? And what can FRT debates teach us about governing broader AI technologies?

We begin by evaluating existing regulatory approaches and identifying their key limitations. Next, based on our original research, we explore how shifts in FRT discourse highlights the need for adaptability and inclusivity. Finally, we propose clear frameworks to enhance global governance strategies that can effectively address the challenges posed by AI. We argue that the case of FRT offers important insights into how we might govern broader AI systems.

Existing regulation of facial recognition technology

New technologies like AI are marked by rapid growth, novelty and uncertainty, often outpacing the capacity of governments to respond (Tinnirello, 2022). Regulation lags because governance systems move slowly, authority is fragmented, industry lobbying delays action, and few institutions anticipate emerging risks. Beyond these structural barriers, governance is highly context specific. In FRT, regulation reflects not just technical features but also shifting political and social views of surveillance (Büthe et al., 2022), producing wide variation across the globe. For example, despite being a global leader in FRT development, the United States (US) lacks comprehensive federal legislation, leading to a fragmented regulatory landscape with varying rules across states. In contrast, the European Union (EU) stands out with its AI Act, which places strict limits on facial recognition, including a ban on real-time public use, except under narrowly defined exceptions (Stix, 2024). In China, while the state deploys FRT with minimal accountability, its use by private entities is subject to strict regulation. India has moved ahead with a national FRT system, again under weak oversight, while in Latin America, the technology is largely deployed without clear safeguards.

Table 1: International initiatives on FRT

Organisation/Initiative	Strengths	Limitations
World Economic Forum (WEF)	Provides multi-stakeholder principles and convenes industry–government dialogue	Non-binding, limited legitimacy beyond private sector, weak follow-up mechanisms
United Nations Interregional Crime and Justice Research Institute (UNICRI)	Focus on human rights in law enforcement use of AI and FRT, offers toolkits for police forces	Narrow scope, limited uptake, non-enforceable
Council of Europe (Convention 108+)	Legally binding framework on data protection, strong privacy safeguards	Regional in scope, limited reach beyond Europe
UN Model Protocol for Law Enforcement Officials (2023)	Explicitly links surveillance technologies, including FRT, to human rights in the context of peaceful protest	Non-binding, depends on voluntary adoption, no enforcement mechanism
Global Privacy Assembly	Sets principles and expectations to guide responsible use of personal data, including FRT, by regulators worldwide	Soft law: relies on voluntary adoption, uneven implementation across jurisdictions

Source: Authors' compilation

Meanwhile, international efforts to set shared FRT standards have gained momentum. Examples include the WEF and the United Nations Inter-regional Crime and Justice Research Institute (UNICRI), which proposed policy frameworks aimed at setting responsible boundaries for the use of FRT. The Global Privacy Assembly has endorsed principles and expectations to guide the appropriate use of personal information in FRT applications. Additionally, the Council of Europe's updated Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+) emphasises the right to privacy and safeguard personal data. The UN has also introduced a practical toolkit for law enforcement officials to promote and protect human rights, particularly in the context of the use of digital technologies in peaceful protests. These initiatives are promising.

Yet, as Table 1 demonstrates, their impact remains limited, hindered by the lack of enforceable standards and inclusive participation. Given these constraints, it is crucial to examine the key policy debates that continue to shape, and at times hinder, meaningful progress.

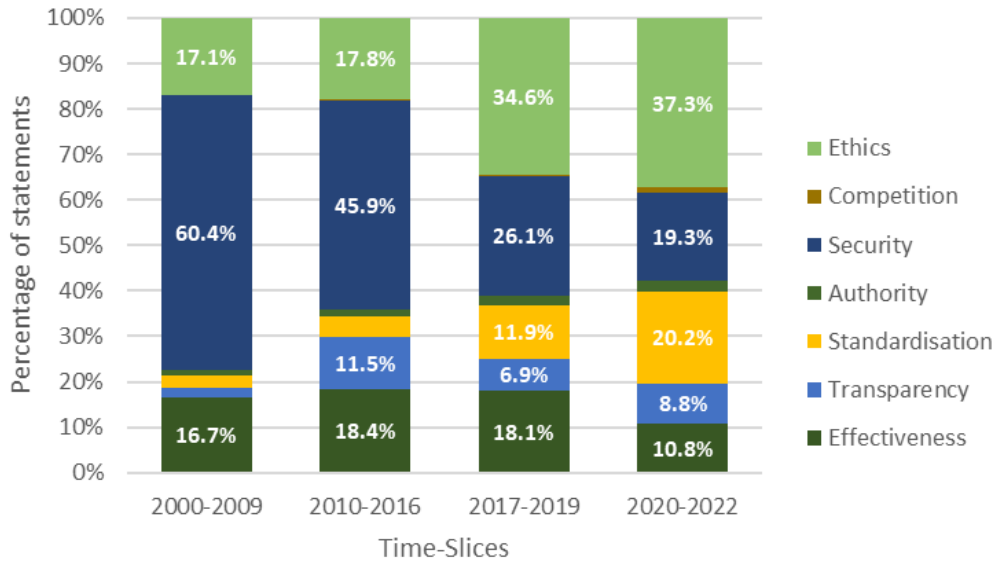
Evolution of debates on facial recognition technology

Regulating AI tools like FRT presents a difficult challenge. Public debate, fuelled by growing awareness and diverse perspectives, has significantly shaped regulatory responses. Our discourse network analysis of more than 4,000 news articles from the *Financial Times*, *New York Times*, Agence France-Presse, Associated Press, and Reuters, published between 2000 and 2020, reveals how framing of FRT evolved over time and how these shifts aligned with regulatory developments (Öge & Quintin, forthcoming).

We find that from 2000 to 2009, FRT was framed mainly as a security tool, with debate centred on effectiveness rather than ethics. Between 2010 and 2016, concerns about bias and transparency grew, and civil society voices gained visibility, a shift we describe as desecuritisation. This coincided with the EU's GDPR, which raised standards for data protection.

Figure 1 shows the evolution of frames in our global dataset, highlighting the decline of security framing and the rise of ethics and rights concerns over this period.

Figure 1: Evolution of FRT frames



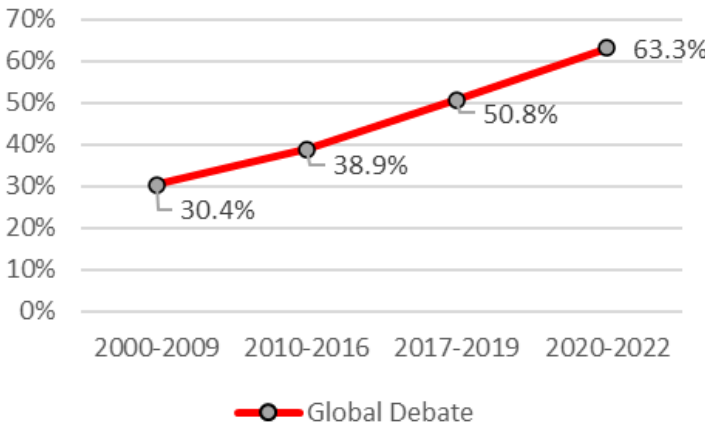
Source: Authors' compilation from original dataset

Since 2017, ethical concerns have dominated. Racial bias and police use of FRT have become central themes, and tech companies are echoing civil society demands, some even imposing moratoriums.

Figure 2 illustrates this rise in anti-FRT framing in our global dataset. At first glance, the timeline suggests a simple pattern: rising concerns lead first to negative sentiments and then to regulation, as seen with the GDPR and the eventual adoption of the 2024 AI Act by the EU. Yet our data show a more nuanced story. Critical voices have been present in the debate since the beginning. For instance, in the US, NGOs such as the American Civil Liberties Union (ACLU) raised ethical concerns as early as the 2000s, but these were sidelined under a securitised framing. As such, regulation lagged not only because technology advanced too quickly but also because early voices lacked representation.

Closing this gap requires more than just faster legislation. It demands inclusive governance structures that bring diverse voices, especially those from civil society, into policymaking from the outset. Without them, early warnings will be ignored, and regulation will continue to lag behind public needs. The next section explores how these problems can be addressed.

Figure 2: Evolution of anti-FRT frames (as % of total frames)



Source: Authors' compilation from original dataset

How to regulate facial recognition technology

The regulation of FRT requires the navigation of the inherent complexity of technological ecosystems, marked by rapid innovation, diverse stakeholders, nested decision-making structures and global interdependencies (Orsini et al., 2020; Walby, 2009). These dynamics reveal the limitations of traditional governance models and highlight the inadequacy of rigid, hierarchical approaches. This section explores how adaptive governance, grounded in flexibility and inclusivity, can bridge the gaps of traditional frameworks and incorporate diverse societal voices.

Adaptive and inclusive governance

Adaptive governance manages uncertainty and change through decentralised decision-making, stakeholder participation, continuous learning and policy flexibility (Dietz et al., 2003; Folke et al., 2005). It is especially relevant for digital governance and AI, where collaborative approaches are needed to keep pace with rapid technological change and evolving citizen demands (Wang et al., 2018).

Adaptive governance emphasises continuous learning, allowing objectives and policies to be revised as new insights emerge (Juhola, 2023). This approach suits the uncertainties of FRT's evolving capabilities, impacts, and unintended consequences. The EU's AI Act illustrates this model with its risk-based approach to algorithms, which enables iterative policy cycles that adjust to new evidence and public feedback. It shows this dynamism through its review clause (Article 112), which allows updates based on technological change, social shifts and stakeholder input. Adaptive governance also allows policymakers to balance safeguards with flexibility to support innovation (Griffin, 2003). In FRT, adaptive frameworks can be resilient and responsive, addressing immediate threats while enabling responsible use. The AI Act reflects this balance by prohibiting real-time biometric identification in public spaces while allowing narrow exceptions, such as for preventing terrorist attacks (EU, 2024).

Ultimately, adaptive governance offers a proactive and resilient way to regulate FRT, evolving with the technology while avoiding the limits of rigid hierarchies. Can this model be implemented globally? As a case study, the EU AI Act offers a progressive, rights-based framework with potential to shape global norms, but its global adoption is constrained by divergent political systems, uneven capacities, and the absence of unified enforcement. Effective adaptive governance, nationally and multilaterally, must account for political and social diversity and adopt a pluralistic approach that accommodates different values and capacities. This requires genuine inclusivity and transparency, ensuring that civil society and affected communities are part of national and global AI governance.

Civil society plays a key role in making this pluralistic approach work. By raising early concerns about privacy, bias and surveillance, NGOs often anticipate risks before states or companies respond. Proactively including these voices in regulatory debates can narrow the gap between technological change and effective governance, ensuring that regulation is both timely and socially legitimate. Empirical case studies reinforce this argument. Datta and Chaffin (2022) illustrate how the integration of local knowledge in the decision-making process allows for a more efficient and adaptive regulatory responses. Drawing on local insights allows policymakers to address issues like privacy violations or wrongful identification before they escalate. Early, context-specific interventions and transparency can prevent public backlash and build trust in both the technology and its regulators. At the macro-level, Ulnicane et al. (2021) show that governance of new technologies benefits from involving a wide range of stakeholders. The inclusion of diverse social groups can reduce regulatory lag and strengthen legitimacy.

Given AI's rapid evolution, varied interpretations, and increasing geopolitical rivalries among the US, the European Union, and China, a single global framework based on the EU AI act is unlikely. More effective governance would

combine the protection of rights with contextual flexibility and international coordination. Transparency and inclusivity remain essential as shared principles that can build trust across divides, while adaptive governance offers a pluralistic path forward by allowing regional variation within common ethical baselines.

Moving forward: lessons for governing artificial intelligence

The case of FRT offers broader lessons for AI governance. Despite efforts at all levels, regulation has struggled to keep pace with fast-moving technologies, a challenge that is especially clear with generative AI, the use of which is outstripping the development of legal and ethical norms. Yet our analysis shows that adaptive and inclusive governance of FRT is possible in specific contexts. This section sets out key policy recommendations to support a global governance framework for AI.

Recommendation 1: Set transparency as a minimum ethical AI standard

The experience with FRT shows the urgent need for minimum ethical standards in AI governance. Existing frameworks such as the GDPR, the EU AI Act, and local moratoriums in the US remain fragmented, allowing companies like Clearview AI to exploit loopholes by scraping personal images across borders (Shepherd, 2024). Without internationally agreed norms, domestic rules are easily circumvented.

Global governance should therefore rest on a core set of shared ethical principles. While full consensus on values is unlikely, agreement on minimum standards is achievable. The upcoming AI Impact Summit in Delhi in February 2026 provides an opportunity to advance this agenda by building consensus on transparency as a global baseline. These standards should define permissible data practices, require transparency in model development, and establish enforceable international rules.

The first step is mandatory transparency requirements for AI systems. Our research shows that transparency has been central to shaping the GDPR and the EU AI Act (Öge & Quintin, forthcoming). Unlike contested human rights arguments, transparency norms are broadly acceptable, even in authoritarian settings (Öge, 2017). AI models should be accompanied by standardised documentation covering training datasets, intended use, testing methods, known risks and deployment contexts.

Such disclosures must be enforced through coordinated mechanisms involving national regulators and multilateral bodies such as the OECD, UN and G20. Recent AI summits in London, Seoul and Paris provide platforms to build consensus. Collaboration of this kind is essential to ensure meaningful oversight and prevent regulatory arbitrage.

Recommendation 2: Frame AI as a societal issue, not just a security tool

Securitised framing narrows debate and sidelines early concerns from civil society. When AI is treated mainly as a security issue, it is removed from normal politics and limitations are placed on who can participate (Wæver, 1993). Our research shows that desecuritisation of FRT coincided with greater visibility of rights-based concerns and broader civil society representation (Öge & Quintin, 2024). This shift also overlapped with regulatory innovations such as city-level moratoriums in the US and rights-focused frameworks in the EU.

San Francisco's 2019 ban on government use of FRT illustrates this dynamic. Civil society reframed the issue as being related to civil liberties and racial justice rather than public safety, enabling the city's Board of Supervisors to pass one of the first moratoriums. This shows how shifting the debate beyond security can create space for broader participation and concrete regulatory change. To sustain this approach, multilateral forums, city authorities and parliaments should actively desecuritise AI debates.

Recommendation 3: Embed civil society in AI governance forums

The FRT case shows that framing shapes regulation by determining who participates and whose perspectives are legitimised. Narrow, technical framings prioritise state actors and experts, excluding broader societal voices and reinforcing power asymmetries.

To strengthen democratic oversight and regulatory durability, UN-led working groups, as well as regional organisations, must broaden AI policy debates. Framing AI around issues such as data governance, accountability and transparency creates space for more inclusive participation and more coherent regulation.

Reducing technical barriers is also essential. Governance processes should avoid exclusive expert forums, as seen in some Global AI summits, and adopt participatory approaches that reflect AI's cross-sectoral impacts. Embedding civil society and affected communities into global regulatory forums ensures that ethical concerns are sustained and societal impacts are recognised. In sum, systematically including civil society helps guard against narrow security or technical framings, enhances legitimacy and supports adaptive, inclusive governance capable of keeping pace with technological change.

References

Acemoglu, D., & Johnson, S. (2023). *Power and progress: Our thousand-year struggle over technology and prosperity*. Hachette UK.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of the First Conference on Fairness, Accountability and Transparency. *Proceedings of Machine Learning Research, 81,* 77–91.

Büthe, T., Djeffal, C., Lütge, C., Maasen, S., & Ingersleben-Seip, N. v. (2022). Governing AI – attempting to herd cats? Introduction to the special issue on the governance of artificial intelligence. *Journal of European Public Policy, 29*(11), 1721–1752.

Datta, A. W., & Chaffin, B. C. (2022). Evolving adaptive governance: Challenging assumptions through an examination of fisheries law in Solomon Islands. *Ecology and Society*, *27*.

Dietz, T., Ostrom, E., & Stern, P. C. (2003). The struggle to govern the commons. *Science*, *302*(5652), 1907–1912.

EU. (2024). *EU Artificial Intelligence Act*. European Union. https://artificialintelligenceact.eu/the-act/

Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, *30*(1), 441-473.

FRAMENET. (2025). *FRAMENET*. https://warwick.ac.uk/fac/soc/pais/research/projects/framenet/framenet/

Frantz, E., Kendall-Taylor, A., & Wright, J. (2020). *Digital repression in autocracies* (Users Working Paper 2020:27). V-Dem Institute, University of Gothenburg.

Griffin, D. (2003). *The emergence of leadership: Linking self-organization and ethics*. Routledge.

Juhola, S. (2023). Introduction to the handbook on adaptive governance. In *Handbook on Adaptive Governance* (pp. 1-13). Edward Elgar Publishing.

Leong, B. (2019). Facial recognition and the future of privacy: I always feel like… somebody's watching me. *Bulletin of the Atomic Scientists*, *75*(3), 109-115.

Öge, K. (2017). Transparent autocracies: The extractive industries transparency initiative and civil society in authoritarian states. *The Extractive Industries and Society, 4*(4), 816–824.

Öge, K., & Quintin, M. (2024). *The changing discourse on facial recognition technology*. Youtube. https://youtu.be/mzAzu4TchOY?si=oGJh_FjSyrMGgttH

Öge, K. & Quintin, M. (forthcoming). *Public Discourse on Facial Recognition in the European Union and the United States*. *Journal of Common Market Studies*.

Orsini, A., Le Prestre, P., Haas, P. M., Brosig, M., Pattberg, P., Widerberg, O., Gomez-Mera, L., Morin, J.-F., Harrison, N. E., & Geyer, R. (2020). Complex systems and international governance. *International Studies Review*, *22*(4), 1008-1038.

Shepherd, T. (2024). The Canadian Clearview AI Investigation as a call for digital policy literacy. *Surveillance & Society*, *22*(2), 179-191.

Stix, C. (2024). The ghost of AI governance past, present, and future: AI governance in the European Union. In J. B. Bullock, Y.-C. Chen, J. Himmelreich, V. M. Hudson, A. Korinek, M. M. Young, & B. Zhang (Eds.), *The Oxford Handbook of AI Governance* (pp. 937–958). Oxford University Press.https://doi.org/10.1093/oxfordhb/9780197579329.013.56

Tinnirello, M. (2022). *The global politics of artificial intelligence*. CRC Press.

Ulnicane, I., Eke, D. O., Knight, W., Ogoh, G., & Stahl, B. C. (2021). Good governance as a response to discontents? Déjà vu, or lessons for AI from other emerging technologies. *Interdisciplinary Science Reviews*, *46*(1-2), 71-93.

Wæver, O. (1993). *Securitization and desecuritization (volume 5)*. Centre for Peace and Conflict Research Copenhagen.

Walby, S. (2009). *Globalization and inequalities: Complexity and contested modernities*. Sage.

Wang, C., Medaglia, R., & Zheng, L. (2018). Towards a typology of adaptive governance in the digital government context: The role of decision-making and accountability. *Government Information Quarterly*, *35*(2), 306-322.

Dr. Kerem Öge is Assistant Professor in the Department of Politics and International Studies at the University of Warwick, United Kingdom.

Email: kerem.oge@warwick.ac.uk

Manuel Quintin is a PhD Candidate in the Department of Political Science at Université Laval, Quebec, Canada.

Email: manuel.quintin.1@ulaval.ca

The German Institute of Development and Sustainability (IDOS) is institutionally financed by the Federal Ministry for Economic Cooperation and Development (BMZ), based on a resolution of the German Bundestag, and the state of North Rhine-Westphalia (NRW) as a member of the Johannes-Rau-Forschungsgemeinschaft (JRF).

Suggested citation:
Öge, K., & Quintin, M. (2025). *Global frameworks for regulating facial recognition technology and artificial intelligence: Adaptive and inclusive governance* (IDOS Policy Brief 19/2025). IDOS. https://doi.org/10.23661/ipb19.2025

IDOS Policy Brief / German Institute of Development and Sustainability (IDOS) gGmbH

ISSN (Print) 2751-4455
ISSN (Online) 2751-4463

DOI: https://doi.org/10.23661/ipb19.2025

Tulpenfeld 6, 53113 Bonn
Email: publications@idos-research.de
https://www.idos-research.de

Printed on eco-friendly, certified paper.