T20 Policy Brief

G20 BRASIL 2024

T20 Brasil 2024 Let's rethink the world

Task Force 05

INCLUSIVE DIGITAL TRANSFORMATION

Building a Facial Recognition Accountability Checklist for the Public Sector

Luã Cruz, Coordination of the Telecommunication and Digital Rights Program, Idec (Brazil)

Marina Fernandes de Siqueira, Lawyer of the Telecommunication and Digital Rights Program, Idec (Brazil)

Disha Verma, Associate Policy Counsel, Internet Freedom Foundation (India)

TF05

Abstract

Nations advancing in technology and leading digital transformations must prioritize AI deployment respecting human rights. This policy brief suggests an assessment toolkit for countries to align with G20 goals, fostering AI innovation responsibly and respecting fundamental and human rights. Influenced by international experiences, our proposal addresses facial recognition technologies (FRT), aiming to strike a balance between innovation and individual and group rights protection.

In light of the evolving landscape of technological advancement and the increasing deployment of facial recognition technologies (FRT), it is imperative to establish a comprehensive and responsible framework that aligns with human rights principles.

We draw inspiration from previous T20 intelligence and other sources, including Idec's and InternetLab's Guide for Private Sector Use of Facial Recognition, Access Now's report "Bodily harms: how AI and biometrics curtail human rights", IFF's Project Panoptic, and EDRi's report The Rise and Rise of Biometric Mass Surveillance in the EU, adapting them to the context of public sector implementation. Countries' experiences will also inform our work, such as USA's NTIA and the Council of Europe. This synthesis enables us to present a text aimed at enhancing the governance of FRT in the public domain.

Recognizing FRT risks, we advocate for responsible adoption and participative data governance. Our framework, integrating case studies and principles, offers a comprehensive guide for the G20, focusing on sustainable and inclusive digital development. While acknowledging challenges in public spaces, our criteria development for FRT in public services emphasizes, for instance, impact assessments to prevent discrimination. In summary, our submission distills international FRT experiences,

deriving meaningful lessons, and proposes a forward-thinking checklist for the public sector's standards in FRT use and procurement, prioritizing non-use where necessary.

Keywords: Facial recognition technology; Artificial Intelligence; Transparency.

Diagnosis of the issue

Facial recognition technologies (FRTs) are becoming increasingly common in various aspects of daily life globally, including banking, payments, security, and education. These technologies can range from simple face detection for counting customers, to identifying specific individuals or conducting long-term surveillance – with or without consent. Despite some public awareness of FRT limitations, its widespread use remains largely unnoticed and unregulated. Certain segments of the tech industry resist oversight, fearing it may stifle growth and innovation. However, there is mounting pressure for regulation, with even some tech companies desiring clear guidelines for a level playing field. Despite the challenges, regulating FRTs is deemed feasible, important, and timely.

In India and Brazil, different "Panoptic" projects monitor the growing development and implementation of FRT for public security. The projects demonstrate how FRT represents a high cost to the state and, at the same time, fails to deliver the efficiency and accuracy promised. It presents risks of incorrect identification (false positives) and identification failure (false negatives). In the former case, FRT poses significant threats to privacy rights, data protection, freedom, and non-discrimination, and may even presume guilt, especially among minority groups. In the latter, it can lead to exclusion and consequent rights violations.

By reproducing gender binary and algorithmic racism, FRT puts already vulnerable groups at-risk – women, transgender and non-binary individuals, and historically oppressed/marginalized/racialized groups. An approach that respects human rights acknowledges the need to ban FRT in mass surveillance contexts, for instance for public security purposes.

There are numerous examples of human rights violations resulting from the use of FRT. In Bahia (Brazil), the low accuracy rate contrasts with numerous cases of false positives, leading to the unjust arrest of black individuals (Falcão 2021). The Argentine justice system recognized the unconstitutionality of the facial recognition system used by the Government of the City of Buenos Aires, which allowed access to biometric data of non-targeted individuals, such as political leaders, activists, unionists, judges, businesspeople, and journalists (Frente a Cano 2022). Similarly, in Brazil, the Federal Police discovered that criminal organizations had access to public sector intelligence and monitoring programs – even though these systems did not contain FRT, it is possible to observe how the fragility of the systems and security flaws jeopardize human rights (Ribeiro 2023). In the European Union, contrary to the recommendations of the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB), the use of biometrics for mass surveillance is normalized by law enforcement (EDRi 2021). In India, too, the use of FRT is ubiquitous and unregulated, and is widely deployed by police forces to identify criminals, create biometric databases, stifle protests, and profile and police minority groups more heavily (IFF 2022).

Prohibiting biometric recognition technologies that enable mass and discriminatory surveillance is the subject of various civil society campaigns and Open Letters, such as #TireMeuRostodaSuaMira (Brazil) and Ban Biometric Surveillance (Global).

This policy also focuses on other forms of FRT use by the public sector, such as identity validation for accessing public services. In Brazil's digital ID system, for instance, citizens providing biometric data to the "Gov.br" platform can gain access to federal documents/IDs, participate in public consultations, or register complaints about public services. However, without alternative options for identity validation and specific restrictions on services requiring biometric ID, data collection could be considered

coercive. Many residents fear surveillance risks or breaches, leading to privacy violations. This concern has become evident following incidents such as when the government shared biometric data with financial institutions, a practice that only ceased after complaints from civil society organizations.

Recommendations

We offer recommendations for the safe and responsible adoption of facial recognition technologies by the public sector that respects human rights, drawing from various documents on FRT such as the Open Letter “Calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance” (2021), Idec’s and InternetLab's “Guide for Private Sector Use of Facial Recognition” (2019), Access Now’s report “Bodily harms: how AI and biometrics curtail human rights” (2023), IFF's and CESeC's Project Panoptic, EDRi’s report “The Rise and Rise of Biometric Mass Surveillance in the EU” (2020) and UN General Assembly’s resolution “Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development” (2024). The policymakers, lawmakers, and controllers at all levels of government around the world should:

Prohibit biometric recognition technologies that enable mass and discriminatory surveillance: Stop using facial recognition and remote biometric technologies for mass surveillance or discriminatory targeted surveillance of religious, ethnic, and racial minorities, political dissidents, and other marginalized groups. For that, the use of these technologies for surveillance of public and publicly accessible spaces by private and public entities should also be prohibited;

Prioritize specific law-making: Before implementing FRT systems in any other context, governments must prioritize enacting specific legislation to regulate surveillance technologies and FRT. Moreover, overarching data protection laws of every country must endeavor to accord a higher status of protection to facial biometric data as compared to other personally identifiable information;

Perform privacy impact assessments: Before implementing facial biometrics systems, the controller must conduct a data protection impact assessment due to the risk to the rights and freedoms of individuals. The results of this assessment should ensure compliance with the overarching data protection legislation. In cases where the assessment demonstrates a high risk, the controller should not proceed with the facial recognition technologies initiative;

Ensure transparency and accountability in data processing: It is necessary to ensure transparency in the processing of biometric data. The public sector must provide transparency in reports that detail all their public contracts (including those that are suspended, in progress, or under construction) for the supply of these technologies;

Ensure transparency and accountability in public-private models: While contracting with private technology providers to implement FRT systems, governments must create clear accountability mechanisms and ensure complete transparency in the partnership, so that citizens have access to necessary technical information and robust grievance redress systems in case of harm;

Provide complete and accurate information to the data subjects: Information related to the data collected, the specific purposes and methods of processing, the possibilities of sharing with third parties; the rights of data subjects over their data, the risks involved in this data processing, and the security measures adopted to mitigate them, must all be clearly articulated to data subjects;

Take consent of data subjects to legitimize the processing of data: Obtaining consent should occur before the start of image capture, which therefore depends on a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the data subject's agreement to the processing of personal data;

Ensure special exclusion and protection of biometric data: Once the images are collected and the desired characteristics extracted, they should be deleted from databases. The retrieval then becomes impossible, even by the system developers. Furthermore, without prejudice to the use of other security measures, it is recommended that all (temporary) storage of facial images be in secure and encrypted environments. Ideally, the storage of this data should always be offline, and any connection used to access it should be encrypted;

Ensure that data collection serves specific purposes, prohibiting the secondary use of data: Data should be processed for specific purposes and the data subjects must be informed using clear and plain language. Government agencies, especially law enforcement agencies, must be prohibited from using and accessing data and information derived from the use of these technologies by private companies and other private actors, except for audits or compliance checks;

Ensure human oversight: Ensure human supervision and effective intervention in decision-making involving AI technology, particularly in high-risk applications such as citizenship exercise and border control;

Set up regulatory oversight bodies: governments should constitute decentralized oversight bodies comprising field experts, technicians, public officials and civil society to regulate and limit the use of FRT systems by law enforcement agencies, including police forces.

Prefer alternatives to facial biometrics: Using facial biometrics for identity validation should not be the sole means of identifying individuals. Facial biometrics should not hinder the exercise of citizenship and access to services or products. Alternatives to FRT must be provided to individuals who choose not to have their data collected;

Report security incidents: Security incidents should be investigated and immediately reported to public authorities, civil society, and data subjects, especially if they entail significant risk or harm. Responsible parties must provide appropriate reparation to individuals who were harmed by the use of these technologies;

Establish anti-discriminatory measures: In the development and use of such systems, protect individuals against the use of these technologies to make decisions regarding economic, social, and cultural rights, including housing, employment, social benefits, and healthcare;

Promote social participation: The public sector should promote social participation by all stakeholders to address concerns and ensure that the adoption of facial recognition technology reflects the public interest.

Resist AI integration in welfare services and policing: The stochasticity of AI and data learning algorithms only magnify and exacerbate inaccuracies inherent to FRT systems, leading to larger error margins. Such false negatives and positives can have grave repercussions on human rights, specifically in the context of delivering welfare services to beneficiaries and criminal identification, respectively. Governments should endeavor to eliminate AI-based FRT systems entirely from these two domains.

Scenario of outcomes

Law enforcement in protests, riots, and 'disruptive' environments: Law enforcement agencies often resort to surveillance tools such as FRT-enabled drones to monitor 'disruptive' events like protests, rallies, riots, and so on. Such systems are freely deployed under the guise of national security or public interest, to identify unruly protesters, disrupters, or miscreants. However, the negative effects of FRT-based surveillance on the human rights and liberties of individual protesters far outweigh its purported 'benefits' for public interest. Many jurisdictions recognise the right to protest as a constitutional guarantee. Surveillance tools, especially when used in an unregulated environment by police forces, can instill a chilling effect on this right, be wielded as an authoritarian tool to stifle dissent, and be used to indiscriminately profile and target participating individuals outside protests as well (Privacy International 2022). Here, the potential trade-off becomes national security and public interest, which can be remedied by employing alternate methods of law enforcement on strict grounds and only where necessary.

Roadblocks in ensuring human oversight: In many jurisdictions and across sectors, ensuring human oversight or human-in-the-loop while deploying FRT systems may pose challenges due to low levels of digital literacy, or paucity of human resources or funds. Secondly, though assigning human oversight to automated systems may solve for lack of accountability, it also may add a layer of bias. For instance, in policing contexts, FRT systems generate a probability match score, or a confidence score between an individual who is to be identified, and an existing database of identified 'criminals' (Goldberg 2021). Multiple possible matches are generated and listed on the basis of their likelihood to be the correct match with corresponding confidence scores. The final

identification, however, is done by a human analyst who selects one match from the list of matches generated by the technology. While the software releases several possible matches, the analyst conducting the search makes the final identification, allowing their own biases to creep into the final result wherein they may be prejudiced against a certain race, religion or community, based on which the system's decision-making may be affected. Here, the potential trade-off to human oversight becomes an additional layer of bias, which is a systemic issue independent of technology.

Complete ban on FRTs may be seen to stifle innovation: Calling for a complete ban on FRTs in certain sectors may be seen as an attempt to stifle technological innovation and advancements. Given that the harms of FRT far outweigh its benefits, this trade-off is justifiable. For other sectors, robust regulation on the use of FRT by both public and private entities can provide the necessary checks and balances, while also making space for innovating on lawful and non-harmful uses of emerging technologies in selected domains.

References

Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF), and Instituto de Defesa de Consumidores (IDEC) 2021. *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance*. Acess Now. https://www.accessnow.org/wp-content/uploads/2022/08/BanBS-Statement-English.pdf

EDRi. 2021. *The Rise and Rise of Biometric Mass Surveillance in the EU*. EDRi. https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf

Falcão, Cíntia. Lentes Racistas: Rui Costa está transformando a Bahia em um laboratório de vigilância com reconhecimento facial. *The Intercept*, September 20, 2021. https://www.intercept.com.br/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-l aboratorio-de-vigilancia-com-reconhecimento-facial/

Frente a Cano. La justicia porteña declaró inconstitucional el sistema de reconocimiento facial. *Frente a Cano,* September 07, 2022. https://frenteacano.com.ar/la-justicia-portena-declaro-inconstitucional-el-sistema-de-rec onocimiento-facial/

Goldberg, Rebeca Darin. "You Can See My Face, Why Can't I? Facial Recognition and Brady", *Columbia Human Rights Law Review*, HRLR Online (April 12, 2021). https://hrlr.law.columbia.edu/hrlr-online/you-can-see-my-face-why-cant-i-facial-recognition-and-brady/

IFF. 2022. *Submission of comments on the draft discussion paper titled "Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology"*. IFF. https://drive.google.com/file/d/1fEEmMn0ActuTbgrhgjF4oLKpUF6DkA3i/view

Navarrete, Ana *et al*. 2023. *Biometria facial, acesso à saúde e direito fundamental à proteção de dados pessoais: nota técnica sobre o uso de dados biométricos em*

estabelecimentos de saúde suplementar. São Paulo: Idec. https://idec.org.br/sites/default/files/nt_biometria_facial_no_setor_de_saude_-_idec.pdf

Privacy International. 2022. *Restraining protest surveillance: when should surveillance of protesters become unlawful?*. United Kingdom: Privacy International. https://privacyinternational.org/sites/default/files/2023-01/PI-RPS-sp-v7-RGB_no_blan k.pdf

Ribeiro, Bruno. "PCC tinha acesso a sistema de câmeras do governo de SP, diz PF", *Metrópoles*, March 23, 2023. https://www.metropoles.com/sao-paulo/policia-sp/pcc-tinha-acesso-a-sistema-de-camer as-do-governo-de-sp-diz-pf

Simão, Bárbara., Fragoso, Nathalie., and Roberto, Enrique. 2020. *Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas*. São Paulo: InternetLab and Idec. https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

UN General Assembly. *A/78/L.49*. 11 Mar. 2024. https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf?token=IkJSZMy7H67KT396JA&fe=true

Wang, Xiaowei., Ahmed, Shazeda. 2023. *Bodily Harms: mapping the risks of emerging biometric tech.* Access Now. https://www.accessnow.org/wp-content/uploads/2023/10/Bodily-harms-mapping-the-ris ks-of-emerging-biometric-tech.pdf

G20 BRASIL 2024
BUILDING A JUST WORLD AND A SUSTAINABLE PLANET

T20 Brasil 2024
Let's rethink the world

Let's rethink the world

CEBRI
Rethink Tank

FUNDAÇÃO ALEXANDRE DE GUSMÃO

ipea
Instituto de Pesquisa Econômica Aplicada