

FORUM: HUMAN RIGHTS COUNSEL (HRC)

**QUESTION OF: THE USE OF FACIAL RECOGNITION TECHNOLOGY IN
IMMIGRATION SYSTEMS AND ITS IMPLICATIONS FOR PRIVACY,
NON-DISCRIMINATION, AND STATE SOVEREIGNTY**

MAIN CHAIR: MATHILDE BENEVENTI

DEPUTY CHAIR: SELMA AL-KHAFAJI LINDØE

MAIN CHAIR EMAIL: BENEVENTIMATHILDE@GMAIL.COM

DEPUTY CHAIR EMAIL: SELMALINDOE2@GMAIL.COM

TABLE OF CONTENTS

- I. Description of the Issue**
- II. Definition of Key Terms**
- III. Major Countries and Organisations Involved**
- IV. Previous Attempts to Solve the Issue**
- V. Possible Solutions**
- VI. Questions Delegates Should Consider during Research**
- VII. Relevant UN Treaties and Events**
- VIII. Useful Links**
- IX. Sources**

I. Description of the Issue

Facial recognition technology (FRT) is a type of biometric system that analyses a person's facial features to identify or verify them, usually by comparing an image to a database of stored faces. In immigration systems, FRT is used at border checkpoints, airports, visa centres, detention facilities, and refugee registration sites to check identities, detect "imposters," and

link individuals to digital files and travel histories. Governments often present these systems as tools to increase efficiency, reduce queues, prevent identity fraud, and strengthen border security in the face of irregular migration and transnational crime.

However, using FRT in migration is not just a technical question but a political and ethical one that directly affects privacy, non-discrimination, and state sovereignty. Privacy is affected because facial images become biometric data that can be stored, searched, and shared across agencies and borders, often without meaningful consent from migrants who depend on these systems to move or seek protection. Non-discrimination is at stake because FRT has been shown to perform differently across skin tones, genders, and age groups, and because it is often deployed in ways that focus surveillance on racialised and marginalised communities. State sovereignty is involved because border control is a core expression of sovereign power, but it is now exercised through complex, data-driven infrastructures that may rely on foreign technology suppliers, regional databases, and international organisations, raising questions about who really controls the data and decisions.

At many borders, FRT is part of broader “smart borders” programmes that combine facial recognition with fingerprints, iris scans, watchlists, and risk-profiling algorithms. These systems can automatically flag people as “risky” or “suspicious” based on opaque criteria, which can shape who is questioned more intensely, who is denied boarding, or who is fast-tracked. For migrants and refugees, errors or biases in these systems are not minor inconveniences; they can mean denial of entry, delays in asylum registration, family separation, or even removal to countries where a person may face harm. Because migrants often lack access to legal aid and information, they may not know that a negative decision is based on an algorithmic match, or how to challenge it.

Data retention and sharing are also problematic. Once a face is converted into a biometric template and stored in an immigration database, it may be kept for years and copied into other systems for policing or intelligence purposes. In some cases, biometric data collected in humanitarian or migration contexts has been shared with security agencies or even with authorities in people’s countries of origin, which can put refugees and dissidents at risk. This “function creep” transforms FRT from a border management tool into a wider surveillance infrastructure that follows people beyond the border itself.

From a legal perspective, many human rights and data protection frameworks treat biometric data as “sensitive” and require strict safeguards such as necessity, proportionality, and purpose limitation. Yet in practice, emergency narratives around terrorism, irregular migration, or public health can be used to justify broad and long-lasting FRT deployments at borders with limited scrutiny. Oversight is further weakened by the fact that many border procedures are opaque, occur in “no man’s land” spaces such as transit zones, and involve people who may not be citizens and thus have fewer political channels to complain.

At the same time, some states and international organisations argue that FRT can have benefits for migrants if designed responsibly. For example, FRT can help prevent duplicate registrations, support secure distribution of aid, and provide people without formal documents with a recognised digital identity. The debate therefore is not only about whether FRT should be used, but how, where, and with what limits and safeguards. For MUN delegates, the key challenge is to explore how states can use FRT in ways that respect privacy and equality while retaining legitimate control over borders and fulfilling obligations under international law.

II. Definition of Key Terms

Facial Recognition Technology (FRT): An automated system that analyses facial features from an image or video to identify or verify a person against one or more images in a database.

Biometric Data: Personal data obtained from specific physical or behavioural characteristics (such as face, fingerprint, or iris) that can uniquely identify a person.

Privacy: The right of individuals to be protected against arbitrary or unlawful interference with their private life, including how their personal and biometric data is collected, stored, used, and shared.

Non-discrimination: The principle that all people must be treated equally in law and practice, without unjustified distinctions based on race, ethnicity, nationality, gender, religion, or migration status.

State Sovereignty: The authority of a state to exercise control over its territory and population, including the power to regulate entry, stay, and removal of non-nationals, subject to international legal obligations.

Smart Borders: Border management systems that rely on digital technologies such as biometrics, databases, and algorithms to monitor, profile, and manage the movement of people.

III. Background Information

The use of biometrics in migration management expanded rapidly after the early 2000s, driven by security concerns, technological advances, and political pressure to control irregular migration. States and regional blocs have created large databases for visas, asylum, border crossings, and law enforcement, and FRT has been added to these systems as camera quality and algorithms improved. International organisations working with refugees and displaced persons have also adopted biometric registration to issue IDs and manage aid delivery.

Criticism has grown in parallel. Human rights organisations, academics, and some regulators warn that FRT can normalise mass surveillance practices and reinforce discriminatory patterns of control. They highlight that migrants, asylum seekers, and stateless persons are often subjected to the most intrusive forms of biometric monitoring, despite being among the least able to refuse or seek remedies. This background sets the stage for current debates about whether FRT at borders should be strictly regulated, temporarily paused (moratorium), or banned in certain high-risk uses, such as real-time scanning of crowds

IV. Major Countries and Organisations

Involved

United States: The U.S. Customs and Border Protection (CBP) has rolled out facial recognition systems at many air, land, and sea ports of entry, making the country one of the most prominent

adopters of FRT for immigration and border control. The U.S. uses FRT for biometric exit and entry, identity verification, and risk assessment of travellers and migrants.

European Union and Schengen States: The EU is investing heavily in “smart borders,” integrating facial recognition into large-scale databases such as the Entry/Exit System and other interoperable information systems used by Schengen states for visas, border checks, and asylum procedures. EU agencies and member states treat FRT as a core component of modern external border management.

China: China deploys extensive facial recognition and other biometric tools for border control and internal movement management, linking border systems with broader national surveillance and public security infrastructures. This includes monitoring at land borders and key travel hubs, often in combination with AI-driven risk profiling.

India: India has been expanding the use of biometric and AI-enabled systems at its borders, including facial recognition within broader “smart fencing” and integrated border management projects along sensitive border regions. These deployments are tied to wider national digital identity initiatives and security strategies.

International and Regional Organisations: Regional bodies responsible for border management strategies and international organisations working on migration and refugee issues play a key role in shaping norms, funding, and technical standards around FRT and other border technologies. They promote advanced border management models based on biometric identity verification and interoperable data platforms, which strongly influence how states adopt facial recognition in immigration systems

V. Possible Solutions

- Create clear international and national rules that limit or prohibit high-risk uses of FRT in immigration, such as real-time scanning of crowds at borders or use for broad predictive profiling.

- Make human rights and data protection impact assessments mandatory before deploying FRT in any migration context, with particular focus on discrimination, error rates, and access to asylum.
- Strengthen independent oversight by empowering courts, parliaments, and data protection regulators to review FRT systems used in immigration and to investigate complaints.
- Ensure transparency and due process by informing migrants when FRT is used, allowing them to access their data, and giving them effective ways to challenge decisions based on automated matching.
- Promote privacy-by-design and data minimisation in humanitarian and migration-related FRT systems, limiting data retention periods and preventing unnecessary sharing with security agencies or third countries

VI. Questions Delegates Should Consider during Research

- When, if ever, is it acceptable for states to use FRT on migrants and refugees at borders, and what safeguards are non-negotiable?
- Should certain uses of FRT in immigration (for example, real-time scanning in public spaces or camps) be banned outright, or only tightly regulated?
- How can states balance their sovereign right to control borders with their obligations not to violate privacy, equality, and the right to seek asylum?
- What mechanisms are needed so that migrants misidentified by FRT can correct errors and obtain remedies quickly?
- How should international organisations using biometrics in refugee and migration programmes design their systems to avoid exposing people to future harm?

VII. Relevant UN Treaties and Events

- International Covenant on Civil and Political Rights (ICCPR), especially provisions on privacy, non-discrimination, and fair procedures.
- International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), relevant to discriminatory impacts of FRT based on race or ethnicity.
- 1951 Convention Relating to the Status of Refugees and its 1967 Protocol, which set out states' obligations toward refugees, including non-refoulement and access to fair asylum procedures that can be affected by FRT.
- Debates in UN bodies and regional organisations on artificial intelligence, surveillance technologies, and human rights, which increasingly include references to biometric and facial recognition systems.

VIII. Useful Links

- European Parliamentary Research Service. "Artificial Intelligence at EU Borders." *European Parliament*, 2021,
[www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf).^[11]
- Delioglu, Fatma. "Technology at the Borders: Surveillance, Control and Resistance in EU Migration Governance." *Balsillie Papers*, 23 Feb. 2025,
balsilliepapers.ca/bsia-paper/technology-at-the-borders-surveillance-control-and-resistance

[nce-in-eu-migration-governance/](#)

- “A Facial Recognition Panopticon on Border and Migration Controls.” *Global Privacy Law Review*, vol. 5, no. 2, 2024,
kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/5.2/GPLR2024009.

UNHCR Global Data Service. “UNHCR Adopting Biometric Face Image Quality Standard for Refugee ID Documents.” *Biometric Update*, 13 Feb. 2025,
[www.biometricupdate.com/202410/unhcr-adopting-biometric-face-image-quality-standard-for-refugee-id-documents.\[1\]](https://www.biometricupdate.com/202410/unhcr-adopting-biometric-face-image-quality-standard-for-refugee-id-documents.[1])

IX. Sources

Delioglu, Fatma. “Technology at the Borders: Surveillance, Control and Resistance in EU Migration Governance.” *Balsillie Papers*, 23 Feb. 2025,
balsilliepapers.ca/bsia-paper/technology-at-the-borders-surveillance-control-and-resistance-in-eu-migration-governance/.

“Artificial Intelligence at EU Borders.” *European Parliamentary Research Service*, European Parliament, 2021,
[www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA\(2021\)690706_EN.pdf.\[11\]](https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf.[11])

“A Facial Recognition Panopticon on Border and Migration Controls.” *Global Privacy Law Review*, vol. 5, no. 2, 2024,
kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/5.2/GPLR2024009.

“UNHCR Adopting Biometric Face Image Quality Standard for Refugee ID Documents.”

Biometric Update, 13 Feb. 2025,

www.biometricupdate.com/202410/unhcr-adopting-biometric-face-image-quality-standard-for-refugee-id-documents.^[1]

Vedova, Irene De. “UNHCR and Biometrics.” *Lawless Zones, Rightless Subjects*, Cambridge UP, 2025, pp. 228-250,

www.cambridge.org/core/books/lawless-zones-rightless-subjects/unhcr-and-biometrics/CD8E625C4E7119518610D35FE977D85E.^[5]