COMMITTEE: Human Rights and the Digital World

ISSUE: To what extent can States and international organisations promote the digital inclusion of refugees, particularly through access to education and information, while ensuring the protection of their personal data and fundamental rights?

CHAIRS: Charlotte DAUCHEZ, Yasen GOSPODINOV et Lois GARCIA

INTRODUCTION



Hello everybody, my name is Yasen Gospodinov. I am 17 years old and I am in the English section at the Lycee International of Ferney-Voltaire in France. I've been part of MUN since 2024 and was a delegate in previous conferences.

This year, our committee will focus on human rights and more specifically for this research report, refugee rights and access to technology. Many refugees still struggle to access the internet, digital devices, and online services due to high costs, language barriers, and limited digital literacy. Furthermore, while these technologies can improve access to education and aid, they often require refugees to share sensitive personal information. If this data is misused or shared for surveillance or migration control, it can put refugees at serious risk. The challenge is to use technology to support refugees while protecting their privacy and rights.

KEY WORDS

Refugee Rights

Refugee rights are the legal rights and protections guaranteed to asylum seekers and refugees under international law. These include the right to seek protection to prevent those in danger being returned to their country of origin (the principle of non-refoulement), and access to essential services such as healthcare, education, housing, and employment.

Non Refoulement

Non refoulement is a fundamental principle of international refugee law. It prohibits states from returning refugees or asylum seekers to a territory where they would face persecution, torture, or other serious dangers. Protecting personal data is essential to enforcing this principle, as information leaks could lead to individuals being exposed and their families becoming subject to potential harm.

Digital Inclusion

Digital inclusion means ensuring that all individuals have equal opportunities to access and use digital technologies. For refugees, this includes affordable internet access, suitable devices, digital skills, and online services available in languages they understand. Without digital inclusion, many refugees struggle to access education, employment, healthcare, or government services.

Biometric Data[1]



Biometric data refers to unique physical characteristics such as fingerprints, facial recognition, or iris scans used to identify an individual. Humanitarian organisations often use biometrics to register refugees and distribute aid. Because biometric data is permanent and can not be changed,

[1] " A glowing fingerprint on a dark circular scanner surface with concentric rings.
by George Prentazas https://unsplash.com/fr/photos/empreinte-digitale-lumineuse-sur-scanner-circulaire-SRFG7iwktDk

managing it requires strict cybersecurity and privacy protections.

Function Creep

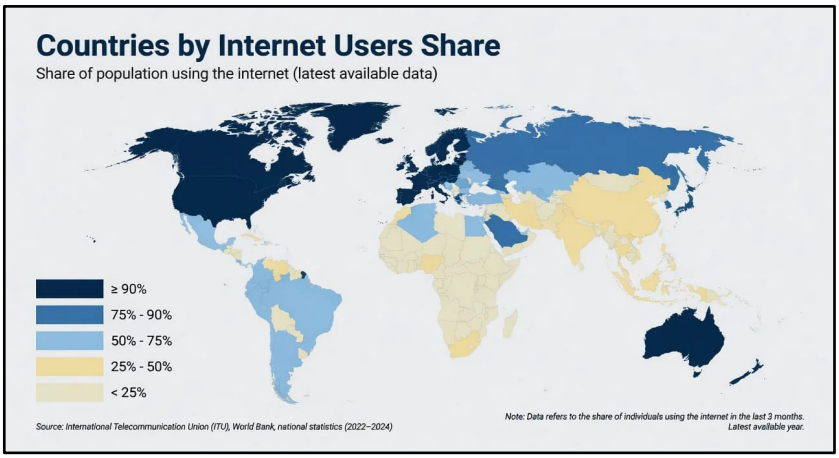
Function creep occurs when information collected for one purpose is later used for another without the person's clear consent. For example, data gathered to distribute humanitarian aid could later be accessed by immigration or law enforcement authorities to track, locate or report individuals, creating severe concerns about privacy, security and trust.

Algorithmic Decision-making

Algorithmic decision-making refers to computer systems that help make decisions by analysing data. These systems are increasingly used in visa applications, asylum procedures, and border management. While they can improve efficiency, they may also reproduce existing biases if they are not carefully designed and monitored.

OVERVIEW

Technology has transformed the way refugees access protection and humanitarian assistance. Digital tools such as biometric registration, digital identity systems, and mobile applications are widely used to distribute aid, provide healthcare and education, and verify identities.



Examples of these include the WFP's SCOPE for food assistance, the UNHCR's registration portals for refugee status, and various mHealth apps used for remote medical consultations. As seen in the UNHCR's 2024 global report[2], 91% of refugees and asylum seekers were individually registered by the UNHCR or national authorities in 98 countries that year, demonstrating the growing use of digital systems in humanitarian assistance. What is more, during the COVID-19 pandemic, online learning also became an essential resource for many refugee students. Despite the benefits of digital tools, many refugees still face a digital divide due to limited access to devices, reliable internet, and digital skills. Certain groups are more severely impacted than others, including women and girls who may face gender-based disparities in access, and elderly refugees who often struggle with lower levels of digital literacy. Additionally, people with disabilities and those living in remote settlements [3] with poor infrastructure face even greater barriers to accessing these essential services. According to a press release by the UNHCR, "nearly half of all refugee children remain out of school", highlighting the importance of digital access for education. At the same time, the growing collection of personal data has raised concerns about privacy, surveillance, and data security. Several States and regional authorities have introduced biometric and automated technologies in border management and immigration procedures. These systems have raised questions



[2] Page 153/264 in the UNHCR's global report
[3] Réseau de femmes (NoW) à l'UIT-D, https://www.itu.int/itu-d/sites/digital-inclusion/fr/

concerning privacy, transparency, discrimination and access to effective remedies. Border control in most countries use technology such as facial recognition and artificial intelligence in border management and asylum procedures, prompting debates about transparency, discrimination, and the protection of human rights.

RELEVANT TREATIES AND EVENTS

In order to specify the importance of these treaties, and mainly who's issuing them, here is an explanation on the power dynamics between the main actors on this problem:

States can improve internet access for refugees, they can build infrastructure, lower costs, and include refugees in digital programmes, however, they cannot guarantee that every refugee will have a device or internet access.

UN agencies can provide funding, advice, and coordination, they can connect governments, NGOs, and companies, however, they cannot force States or companies to take action.

NGOs can provide devices, digital training, and internet access in refugee communities, they can also identify local needs, however, they cannot replace governments or provide nationwide services.

Technology companies can provide networks, devices, software, and technical support, they can also offer cheaper services and training, however, they cannot replace governments or decide who receives refugee protection.

Now, onto the relevant treaties:

International Legal Framework

1951 Convention Relating to the Status of Refugees (28 July 1951): The foundation of international refugee law, guaranteeing refugee rights and the principle of non-refoulement, including in digital asylum procedures, although it's imperative to note that the original convention wasn't tied to said technology, as it predates the digitalisation period. The convention was therefore adapted over the course of the modernisation and digitalisation of the world to include guidelines to protect refugees.

General Data Protection Regulation (GDPR) (Regulation adopted 27 April 2016; applied from 25 May 2018): The EU's data protection law requires organisations to collect only necessary personal data and protect it from misuse.

UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR (1 July 2015): Sets standards for collecting, storing, and protecting refugees' personal data during humanitarian operations.

International Framework For Coorperation

Global Compact on Refugees (17 December 2018): Promotes international cooperation to improve refugees' access to education, employment, and digital services.

Amnesty International – Defending the Rights of Refugees and Migrants in the Digital Age (18 June 2024): Calls for stronger safeguards against the misuse of technologies such as AI, facial recognition, and biometric databases in migration management.

The Giga Initiative: The Giga Initiative was launched by UNICEF and the International Telecommunication Union (ITU) in September 2019 to expand internet access and reduce the digital divide for refugees and other vulnerable groups.

POSSIBLE SOLUTIONS

Digital technology will continue to shape refugee protection in the coming years, meaning the challenge is not whether technology should be used, but how it can be used responsibly. Governments, humanitarian organisations, international institutions, and private companies all have a role to play in creating digital systems that improve lives while protecting fundamental rights.

1. Separate Humanitarian Data from Immigration Enforcement

Information collected to provide healthcare, education, financial assistance, or humanitarian aid should not automatically be shared with immigration or law enforcement authorities. Establishing clear legal barriers between humanitarian services and migration enforcement would help refugees trust the organisations supporting them and reduce the risk of personal data being misused.

2. Strengthen Data Protection Standards

Organisations working with refugees should apply strong security measures such as encryption, secure storage, regular cybersecurity audits, and data minimisation practices. Collecting only the information that is strictly necessary reduces the impact of possible data breaches and better protects vulnerable populations. International standards should also be harmonised so that refugee data receives the same level of protection regardless of where it is stored.

3. Expand Digital Inclusion

Providing internet access alone is not enough. Refugees also need affordable devices, reliable connectivity, and digital literacy training. Educational programs should be offered in several languages and adapted to different levels of experience, allowing refugees to safely access online education, employment opportunities, healthcare, and public services. Partnerships between governments, NGOs, schools, and technology companies can help make these programmes more accessible.

4. Increase Transparency and Oversight of Artificial Intelligence

Delegates should evaluate the role of artificial intelligence in asylum decisions, ensuring that technology does not replace human judgment. Governments using AI systems for migration management should publish clear information about how these systems work, allow independent audits, and provide effective ways for individuals to challenge automated

decisions. Where technologies such as facial recognition or predictive risk assessment cannot be shown to operate fairly and accurately, their use should remain limited or suspended until independent evaluations confirm they respect human rights.

5. Promote International Cooperation

Refugee movements often involve several countries, making international cooperation essential. States should exchange good practices on digital inclusion, cybersecurity, and data protection while working through organisations such as the UNHCR, ITU, UNICEF, and the International Organisation for Migration. Developing common international guidelines would reduce differences between national systems and provide more consistent protection for displaced people worldwide.

QUESTIONS TO CONSIDER:

How can states expand digital access without creating new surveillance risks?

How can refugees give meaningful consent to data collection when access to essential services depends on providing personal information?

Should there be international rules limiting how governments can use biometric data collected by humanitarian organisations?

When should biometric data be collected, and who should be permitted to access it?

How can artificial intelligence improve asylum systems without creating discrimination or reducing transparency, and what safeguards should be put in place?

What responsibilities should technology companies have when their digital services are used in migration management?

How can the international community ensure that refugee camps and informal settlements receive the same level of digital access as urban communities?

What measures can governments adopt to improve digital inclusion while fully respecting refugees' right to privacy?

Who should finance digital infrastructure in communities hosting refugees?

CASE STUDIES:

UNHCR's Instant Network Schools programme provides digital learning for refugees and host communities. As of January 2026, it was operating 164 learning centres in six countries and had benefited more than 382,000 students and 6,800 teachers since 2013. This shows the potential of digital education, but access to devices, connectivity and digital skills can still limit participation.
[4]

In Jordan, the World Food Programme uses iris scans to verify refugees receiving food assistance. In 2022, WFP provided monthly assistance to around 462,000 refugees in Jordan. Biometric verification can make aid distribution more efficient and reduce duplicate registrations, but it also creates concerns about protecting sensitive biometric data and controlling who can access or share it.[5]

The UK Home Office tested two AI tools in 2024: one to summarise asylum interviews and another to search country-policy information. The interview-summary tool saved an average of 23 minutes per case, while the policy-search tool saved around 37 minutes. However, 9% of the AI-generated summaries were found to contain inaccurate or missing information, and 23% of users said they were not fully confident in the summaries that passed the initial check. This shows both the potential efficiency gains and the need for human oversight as we cannot completely rely on technology.[6]

[4] Page 16: https://www.unhcr.org/kenya-instant-network-schools.html

[5] Under "what is the verification process:https://help.unhcr.org/jordan/en/frequently-asked-questions-unhcr/wfp/

[6] Points 5.1 and 7:https://www.gov.uk/government/publications/evaluation-of-ai-trials-in-the-asylum-decision-making-process/evaluation-of-ai-trials-in-the-asylum-decision-making-process

BIBLIOGRAPHY

United Nations. Convention Relating to the Status of Refugees (28 July 1951).
Explains the legal rights of refugees and establishes the principle of non-refoulement.
https://www.unhcr.org/1951-refugee-convention

European Union. General Data Protection Regulation (GDPR) (27 April 2016; applicable from 25 May 2018).
Explains the legal standards for collecting, using, and protecting personal data.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

UNHCR. Policy on the Protection of Personal Data of Persons of Concern to UNHCR (1 July 2015).
Explains how humanitarian organizations should collect, store, and protect refugees' personal data.
https://www.unhcr.org/what-we-do/data-and-publications/unhcr-data

UNHCR. Global Trends Report (11 June 2026).
Shows the latest statistics and trends on global forced displacement.
https://www.unhcr.org/global-trends

UNICEF & International Telecommunication Union (ITU). Giga Initiative (2019–present).
Shows how expanding internet access can reduce the digital divide affecting refugee education.
https://giga.global

Amnesty International. Defending the Rights of Refugees and Migrants in the Digital Age (18 June 2024).
Explains how AI, biometric systems, and digital surveillance can affect refugees' rights.
https://www.amnesty.org/en/documents/pol40/7654/2024/en/

Human Rights Watch. Reports on Digital Surveillance and Migration.
Shows examples of how digital technologies are used in migration management and their human rights implications.
https://www.hrw.org/topic/refugees-and-migrants

Access Now. Publications on Digital Rights and Privacy.
Explains the privacy and surveillance risks that digital technologies can pose to vulnerable populations.
https://www.accessnow.org

Refugee Studies Centre, University of Oxford. Research on Refugees and Digital Exclusion.
Explains how limited access to technology affects refugees' education, employment, and social inclusion.
https://www.rsc.ox.ac.uk

World Bank. Digital Development publications.
Shows how digital inclusion contributes to economic participation and long-term development.
https://www.worldbank.org/en/topic/digitaldevelopment

UNHCR Digital Learning Resources.
Explains key issues related to refugee protection and digital inclusion through educational videos and learning materials.
https://www.unhcr.org/education

Map of the Week: The Facial Recognition World Map (10 June 2026)
Shows the nations that include and utilise any sort of technology linked to facial recognition wherever that may be
https://ubiqueags.org/map-of-the-week-the-facial-recognition-world-map/

Facial Recognition in Airports 2026: Paperless Boarding and the End of Queues (March 16 2026)
Includes more in depth explanations and facts on which nations utilise said facial recognition devices at airports
https://pixidia.com/en/facial-recognition-airports-2026-biometric-boarding/

Case studies:

https://www.unhcr.org/kenya-instant-network-schools.html

https://help.unhcr.org/jordan/en/frequently-asked-questions-unhcr/wfp/

https://www.gov.uk/government/publications/evaluation-of-ai-trials-in-the-asylum-decision-making-process/evaluation-of-ai-trials-in-the-asylum-decision-making-process

Pictures:

Page 2:

”Une empreinte digitale lumineuse sur une surface de scanner circulaire sombre avec des lignes concentriques” by George Prentzas, https://unsplash.com/fr/photos/empreinte-digitale-lumineuse-sur-scanner-circulaire-SRFG7iwktDk

Page 3:

Top 100 Countries by Internet Users Share, 2026
https://statranker.org/economy/top-100-countries-by-internet-users-share-2026/

Réseau de femmes (NoW) à l'UIT-D,
https://www.itu.int/itu-d/sites/digital-inclusion/fr/

LIST OF KEY ACTORS INVOLVED:

Organizations and Institutions

- United Nations High Commissioner for Refugees (UNHCR)
- International Organization for Migration (IOM)
- United Nations Children's Fund (UNICEF)
- International Telecommunication Union (ITU)
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
- European Union (EU)
- African Union (AU)
- Association of Southeast Asian Nations (ASEAN)
- World Bank
- International Committee of the Red Cross (ICRC)
- Amnesty International
- Human Rights Watch
- Access Now
-Forum of Incident Response and Security Teams (FIRST)
-INTERPOL
-Google
-Meta
-Microsoft

P5 nations (The 5 permanent members of the UN security council):
United States, China, Russia, France, United Kingdom

Major Host & Transit Nations:
Türkiye, Bangladesh, Uganda, Ethiopia, Colombia, Pakistan, Jordan, Chad, Lebanon, Italy, Greece, Thailand, Malaysia

Countries of Origin:
Syria, Afghanistan, Ukraine, South Sudan, Venezuela, Democratic Republic of the Congo, Sudan, Iran, North Korea

Donor & Regional Support Nations:
Germany, Japan, India, Canada, Australia, Brazil, Egypt, Saudi Arabia, Switzerland, South Korea, Singapore, Rwanda, Niger