

55MUNVII SOCHUM



STUDY GUIDE

TABLE OF CONTENTS

Introduction to SOCHUM

- The Social, Humanitarian and Cultural Committee
- Areas of Work
- Mandate and Limitations
- The Agendas

Agenda A: Addressing Biocolonialism

- Introduction to the Agenda
- Key Terms and Definitions
- History and Background
- Social, Political and Economic Dimensions
- Specific Research and Analysis
- Past UN Actions
- Case Studies
- Questions a Resolution Must Answer (QARMA)

Agenda B: Addressing Algorithmic Discrimination

- Introduction to the Agenda
- Key Terms and Definitions
- History and Background
- Social, Political and Economic Dimensions
- Specific Research and Analysis
- Past UN Actions
- Case Studies
- Questions a Resolution Must Answer (QARMA)

Bibliography

INTRODUCTION TO SOCHUM

THE SOCIAL, HUMANITARIAN AND CULTURAL COMMITTEE

The Social, Humanitarian and Cultural Committee (SOCHUM) is the Third Committee of the United Nations General Assembly. Established in 1945 together with the General Assembly itself, the Committee played a significant role in the drafting of the Universal Declaration of Human Rights (UDHR), which the General Assembly adopted in 1948.

The Committee is concerned with the fundamental rights and freedoms to which every individual is entitled. A substantial portion of its work consists of the examination of human rights questions, including the consideration of reports submitted by the special procedures of the Human Rights Council, which was established in 2006 as the successor to the Commission on Human Rights.

AREAS OF WORK

The Committee deliberates upon a broad range of social and humanitarian matters, including:

- the advancement of women and the protection of children;
- the rights of Indigenous Peoples;
- the treatment of refugees and migrants;
- the promotion of fundamental freedoms and the elimination of racism and racial discrimination;
- the right of peoples to self-determination;
- questions of social development, including those relating to youth, the family, ageing and persons with disabilities;
- crime prevention, criminal justice and international drug control.

The Committee regularly adopts resolutions on matters closely related to the present agendas, among them the rights of Indigenous Peoples, the right to privacy in the digital age, and the elimination of racism and racial discrimination.

MANDATE AND LIMITATIONS

As a Main Committee of the General Assembly, SOCHUM deliberates upon questions within its competence, considers reports, and adopts draft resolutions that are subsequently forwarded to the plenary of the General Assembly.

Resolutions adopted in this manner constitute recommendations addressed to Member States. They carry considerable political and moral authority and may contribute to the development of international standards; however, they are not legally binding in the manner of a treaty, and the Committee possesses no enforcement powers comparable to those of the Security Council.

THE AGENDAS

Agenda A: Addressing Bio colonialism: Protecting the Genetic Privacy and Indigenous Data Sovereignty of Native Populations.

Agenda B: Addressing Algorithmic Discrimination in Immigration and Asylum Systems.

Both agendas concern a common problem: the manner in which emerging technologies that collect and process personal data, whether genetic material or biometric and digital records, may adversely affect vulnerable populations when they are deployed without adequate consent, transparency and accountability.

AGENDA A

Addressing biocolonialism: protecting the genetic privacy and indigenous data sovereignty of native populations

INTRODUCTION TO THE AGENDA

For several centuries, Indigenous Peoples have been subjected to colonial systems that appropriated their lands, natural resources, cultural property and traditional knowledge, frequently without their consent. Advances in biotechnology and genetic research have introduced a further dimension to this pattern: the collection and use of genetic material and biological information derived from Indigenous populations.

This phenomenon is commonly described as **biocolonialism**. The term denotes circumstances in which biological resources, genetic information or traditional knowledge are obtained, studied or commercialised within unequal relationships, in the absence of adequate consent, recognition, control or benefit-sharing for the communities concerned. Although biocolonialism is not a formally defined legal concept, it is widely employed in scholarship and advocacy to describe the persistence of colonial patterns through modern scientific practice.

Genetic research is nonetheless of considerable value. It advances the understanding of hereditary disease, informs the development of new therapies and may contribute to the reduction of health inequalities. Where it is appropriately governed, Indigenous participation in research can improve the quality of healthcare available to Indigenous communities and strengthen their representation within the scientific enterprise.

Genetic research also raises serious ethical and human rights concerns:

Genetic information is inherently relational. It is deeply personal, yet it also discloses information concerning biological relatives and, in certain cases, entire communities.

Individual consent is distinct from collective consent. An individual may consent to the provision of a sample for a particular study without being aware

that the sample may subsequently be employed in unrelated research, transferred to other institutions or incorporated into commercial databases.

Genetic data possesses commercial value. Samples may give rise to pharmaceutical products, patents and other profitable applications. Where contributing communities receive little information and no meaningful benefit, research relationships risk reproducing historical inequalities.

Regulation has not kept pace with scientific development. Genetic data may be retained for decades, replicated and analysed by means of technologies that did not exist at the time of collection.

The principle of **Indigenous data sovereignty** has emerged in response to these concerns. It holds that Indigenous Peoples are entitled to exercise authority over the collection, use and dissemination of data pertaining to their peoples, lands and cultures.

Contemporary Context

The cost of sequencing a human genome has declined dramatically since the completion of the Human Genome Project, from billions of United States dollars to a few hundred. Genetic data is consequently collected on an unprecedented scale by hospitals, national biobanks, universities, pharmaceutical companies and direct-to-consumer ancestry testing companies, and millions of individuals have already submitted biological samples to commercial testing services.

This expansion generates novel risks for Indigenous communities. Genetic databases may now be linked with other datasets, analysed by means of artificial intelligence and transmitted across jurisdictions almost instantaneously. An Indigenous individual who uploads their genetic data to a publicly accessible database simultaneously discloses information concerning relatives and the wider community, none of whom have been consulted. At the same time, the commercial value of genetic data has risen considerably, intensifying pressure to obtain samples from populations regarded as under-represented in existing datasets, a category that includes many Indigenous Peoples.

According to United Nations estimates, approximately 476 million Indigenous persons reside in more than 90 countries. Although they constitute roughly six per cent of the global population, they are disproportionately represented among the

poorest and most marginalised segments of society, which renders questions of equity, consent and benefit-sharing particularly acute.

The central question of this agenda is therefore the reconciliation of the benefits of scientific research with the rights of Indigenous Peoples, such that Indigenous Peoples participate in research as rights-holders and decision-makers rather than solely as sources of samples and data.

KEY TERMS AND DEFINITIONS

Biocolonialism: The exploitation of biological resources, genetic information or traditional knowledge originating from Indigenous communities without adequate consent, meaningful participation or equitable benefit-sharing.

Indigenous Peoples: Distinct communities possessing historical continuity with pre-colonial societies and strong attachments to ancestral territories. They frequently maintain their own languages, traditions, knowledge systems and political institutions.

Genetic Privacy: The protection of information derived from an individual's DNA against unauthorised collection, analysis, disclosure or use. Because DNA also reveals information concerning relatives, it warrants a higher standard of protection than ordinary personal data.

Indigenous Data Sovereignty: The right of Indigenous Peoples to determine how data concerning their communities, identities, lands, resources and knowledge is collected, stored, accessed, interpreted and used.

Indigenous Data Governance: The rules, procedures and community-led processes by which Indigenous data is managed, including the approval of research and the regulation of access, storage, publication and commercial use.

Genomic Data: Information derived from the study of the genetic material of an individual or population, which may reveal inherited traits, susceptibility to disease and population history.

Genetic Resources: Biological materials containing functional units of heredity that are of actual or potential value. The Convention on Biological Diversity (CBD) regulates certain of these resources but does not comprehensively govern human genetic data.

Traditional Knowledge: Knowledge, practices and skills transmitted across generations within Indigenous communities, including knowledge relating to medicinal plants, agriculture and ecosystems.

Biological Samples (Biospecimens): Materials such as blood, saliva or tissue obtained from living organisms, which may be stored for extended periods and reused in subsequent studies.

Informed Consent: Voluntary agreement to participate in research, given after the provision of clear information concerning its purpose, procedures, risks, benefits and potential future uses.

Free, Prior and Informed Consent (FPIC): The principle that Indigenous Peoples should be able to reach decisions freely, before an activity commences, and on the basis of full information. Its precise legal application depends upon the relevant framework and circumstances, and it does not operate as a universal requirement for every research activity.

Collective Rights and Community Consent: The principle that Indigenous Peoples hold certain rights collectively as well as individually. Community engagement may therefore supplement, rather than replace, individual consent.

Genetic Discrimination: Unjust differential treatment of individuals or groups on the basis of genetic information, ancestry or inherited health risk, for instance in employment, insurance or healthcare.

De-identification: The removal of direct identifiers, such as names, from data. It reduces privacy risks but does not guarantee anonymity, since genetic data may be linked with other datasets.

Anonymisation: The processing of data such that individuals can no longer reasonably be identified. In genetic research, complete anonymisation is exceptionally difficult to achieve.

Benefit-Sharing: The equitable distribution of the benefits arising from research, which may include monetary payments, healthcare programmes, training, partnerships or access to findings.

Biopiracy: A widely used term for the unfair or unauthorised appropriation of biological resources or traditional knowledge. It does not constitute a defined

offence under international law, but it denotes concerns regarding exploitation and intellectual property.

Biobanking: The systematic collection and long-term storage of biological samples and associated data for research purposes.

Genetic Ancestry Testing: DNA analysis employed to estimate ancestral origins. Its results depend upon reference databases and cannot of themselves determine Indigenous identity, which also involves culture, community recognition and self-identification.

Indigenous Intellectual and Cultural Heritage: Traditional knowledge, cultural expressions, symbols and practices, certain of which may be sacred or restricted by customary law.

CARE Principles: A framework for Indigenous data governance comprising Collective Benefit, Authority to Control, Responsibility and Ethics.

OCAP® Principles: Ownership, Control, Access and Possession; a framework developed by First Nations in Canada to give effect to their authority over their data.

FAIR Principles: A data-management framework providing that data should be Findable, Accessible, Interoperable and Reusable. It is frequently considered in conjunction with the CARE Principles.

Research Reciprocity: Research relationships characterised by mutual respect that yield genuine and enduring benefits for the communities involved.

Secondary Use: The use of samples or data collected for one purpose in a different study; for example, the use of a sample collected for diabetes research in a subsequent study of ancestry.

Data Sovereignty and Data Security: Data sovereignty concerns the question of who determines how data is used, whereas data security concerns technical protection, such as encryption. A dataset may be technically secure yet employed in ways to which a community has not consented.

HISTORY AND BACKGROUND

Colonialism and the Exploitation of Indigenous Peoples

Biocolonialism is closely connected to the broader history of colonialism, in the course of which Indigenous Peoples were frequently deprived of control over their lands, resources, cultural heritage and knowledge. Colonial institutions commonly regarded Indigenous communities as objects of study or administration rather than as equal partners.

Traditional knowledge concerning medicinal plants, agriculture and local ecosystems was at times documented by outside parties and subsequently exploited for scientific or commercial purposes, with little or no involvement of the communities concerned. Modern genetic research has given rise to new forms of the same concern: the issue is no longer confined to the physical collection of materials but extends to continuing control over the information derived from them.

Early Anthropological and Genetic Research

During the nineteenth and twentieth centuries, researchers collected human remains, biological specimens and information concerning Indigenous communities, frequently under unequal conditions and with minimal consultation. Institutions retained and studied these materials for decades, while the communities concerned were often unaware of their location or of the purposes for which they were being used. Many communities subsequently sought the repatriation of ancestral remains. This history accounts for the considerable importance that Indigenous organisations now attach to consent, transparency and community authority.

Key Milestones

1948: Universal Declaration of Human Rights (UDHR). Established the foundational principles of dignity, equality and non-discrimination, although it does not refer to genetic data.

1966: International Covenant on Civil and Political Rights (ICCPR). Article 17 protects the right to privacy; Article 27 protects the cultural rights of minorities.

1989: ILO Convention No. 169. A binding treaty concerning the rights of Indigenous and tribal peoples and the duty of consultation, ratified by a comparatively small number of states.

1990–2003: Human Genome Project. Substantially increased the scientific and commercial value of genetic data and raised new questions concerning consent, ownership and commercialisation.

Early 1990s: Proposal of the Human Genome Diversity Project. Envisaged the collection of

DNA from Indigenous groups worldwide and encountered strong opposition from numerous Indigenous organisations.

1992: Convention on Biological Diversity (CBD). Article 8(j) addresses traditional knowledge relevant to biodiversity and encourages equitable benefit-sharing. The Convention does not, however, govern human DNA.

1997: UNESCO Universal Declaration on the Human Genome and Human Rights.

Declared that the human genome in its natural state shall not give rise to financial gain and that genetic research must respect human dignity.

2003: UNESCO International Declaration on Human Genetic Data. Set out principles governing consent, confidentiality and the use of human genetic data.

2007: United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Recognised the rights of Indigenous Peoples to self-determination, cultural heritage and free, prior and informed consent. It is a declaration rather than a treaty.

2010: Havasupai Tribe settlement (United States). Became a landmark case concerning consent and the secondary use of genetic samples.

2010 (in force 2014): Nagoya Protocol. Established rules governing access to covered genetic resources and the sharing of benefits arising from their use, including associated traditional knowledge.

2019: CARE Principles. Promulgated by the Global Indigenous Data Alliance to place Indigenous rights at the centre of data governance.

2025: Study of the Expert Mechanism on the Rights of Indigenous Peoples on Indigenous data (A/HRC/60/66). Linked Indigenous data rights directly to the right to self-determination.

2026: Draft Participatory Framework of the World Health Organization. Provided practical guidance on respectful engagement with Indigenous Peoples in health and biodiversity research.

The Rise of Modern Genomics

The Human Genome Project (1990–2003) transformed medicine and population genetics. Biological samples and genetic data acquired considerable value for universities, hospitals, biotechnology companies and governments. Nevertheless, many Indigenous populations remained under-represented in genetic datasets, even as research findings were employed to advance claims concerning their ancestry, health and history. This produced a dilemma that persists to the present day: how Indigenous participation in research may be increased without the repetition of extractive practices.

Controversial Research Projects

Several research projects undertaken in the 1990s and 2000s have shaped Indigenous perspectives on genetic research.

The Human Genome Diversity Project (HGDP). In the early 1990s, a group of scientists proposed the collection of DNA samples from several hundred Indigenous and geographically isolated populations, in part to preserve a record of human genetic diversity before these groups were absorbed or ceased to exist as distinct populations. Numerous Indigenous organisations objected strongly. They contended that the project treated Indigenous Peoples as biological specimens rather than as living peoples, that it prioritised the collection of their DNA over their pressing needs in respect of health and land rights, and that it could result in the patenting of their genetic material. Critics referred to it pejoratively as "the Vampire Project". The controversy contributed to the establishment of Indigenous advocacy organisations, including the Indigenous Peoples Council on Biocolonialism.

The Nuu-chah-nulth case (Canada). In the early 1980s, researchers collected blood samples from members of the Nuu-chah-nulth First Nations in British Columbia in order to investigate rheumatoid arthritis, a condition of high prevalence in the community. The study did not identify the genetic cause it sought. The samples were, however, subsequently transferred to other countries and employed in studies of ancestry and human migration without the further consent of the community. Following sustained efforts by the Nuu-chah-nulth, the remaining samples were returned in 2004. The case is frequently compared with that of the Havasupai Tribe.

The Genographic Project. Launched in 2005 by the National Geographic Society and its partners, this project sought to trace ancient patterns of human migration through the collection of DNA, including from Indigenous communities.

Indigenous organisations expressed concern that the project could undermine their own accounts of origin and be invoked to contest their land claims, and the matter was raised before the United Nations Permanent Forum on Indigenous Issues.

These cases illustrate a recurring pattern: research regarded by external researchers as benign or beneficial was experienced by the communities concerned as a violation of trust, culture and identity.

Indigenous Data Sovereignty Movements

From the late twentieth century onwards, Indigenous organisations increasingly asserted authority over data concerning their communities. In Canada, First Nations developed the OCAP® principles; internationally, the Global Indigenous Data Alliance promulgated the CARE Principles in 2019. In the 2020s, debates surrounding large precision-health initiatives, including in Canada, demonstrated the necessity of agreement on consent, governance and benefit-sharing prior to the commencement of research.

SOCIAL, POLITICAL AND ECONOMIC DIMENSIONS

Social Dimension

The social consequences of biocolonialism extend well beyond the individual research participant. Genetic findings concerning ancestry may contradict a

community's own account of its origins, as occurred in the Havasupai case, and thereby affect collective identity, spiritual belief and cultural continuity. Research on stigmatised conditions, such as mental illness or consanguinity, may attach negative labels to an entire people. In many Indigenous cultures, blood, tissue and ancestral remains possess sacred significance, so that their unauthorised use is experienced as a cultural and spiritual harm rather than merely a breach of privacy. The cumulative legacy of such practices has produced deep mistrust of medical and scientific institutions, which in turn depresses participation in research and perpetuates the under-representation that limits the medical benefits available to Indigenous communities.

Political Dimension

Politically, the agenda concerns the relationship between states and Indigenous Peoples and, in particular, the right to self-determination. The extent to which Indigenous institutions are recognised as holding authority over research and data varies considerably between states, and the legal status of UNDRIP and of free, prior and informed consent remains contested in certain jurisdictions. Genetic ancestry findings may also acquire political significance where they are invoked in disputes concerning land rights, membership of Indigenous nations or entitlement to state recognition. At the international level, negotiations on access to genetic resources and on digital sequence information reflect a broader division between biodiversity-rich developing states and research-intensive industrialised states, while the cross-border transfer of genetic data raises unresolved questions of jurisdiction and accountability.

Economic Dimension

Genetic data has become a significant economic asset within the pharmaceutical, biotechnology and precision-medicine industries. The returns generated by patents, licensing arrangements and commercial databases accrue predominantly to research institutions and corporations located in high-income states, whereas the communities from which samples or traditional knowledge originate frequently receive little or no share of those returns. Indigenous communities often lack the financial resources and specialist legal expertise necessary to negotiate equitable research agreements on equal terms. The emergence of digital sequence

information has further complicated benefit-sharing, since genetic sequences may be exploited commercially without physical access to the source material. Conversely, Indigenous-led biorepositories and research enterprises demonstrate that genetic data may also serve as a basis for community economic development where control remains with the community.

SPECIFIC RESEARCH AND ANALYSIS

Forms of Biocolonialism

Biocolonialism is not confined to the physical removal of resources; it may equally arise through unequal control over data, knowledge, research decisions and profits. Its principal forms are as follows:

Collection without meaningful consent: researchers may fail to explain the objectives, risks and potential future uses of a study, or may disregard community concerns and cultural protocols.

Unauthorised secondary use: samples collected for one study are subsequently employed in other research to which participants did not consent.

Commercialisation without equitable benefit-sharing: research gives rise to patents or profitable products, while contributing communities receive no meaningful return.

Loss of control over genetic data: once digitised, data may be replicated and disseminated across numerous institutions, frequently without the knowledge of the communities concerned.

Misrepresentation of identity: ancestry findings may be employed to advance broad claims regarding a people's origins, notwithstanding that genetics alone cannot determine cultural belonging or community membership.

Unequal research partnerships: external institutions commonly control funding, expertise and publication, leaving communities with little capacity to shape the research agenda.

Genetic Privacy: Principal Risks

Genetic privacy is considerably more difficult to protect than many other categories of personal data:

Re-identification: genetic data from which names have been removed may nonetheless be matched with other datasets so as to identify individuals.

Familial information: the DNA of one individual discloses information concerning relatives who have not consented to participation.

Sensitive group-level findings: studies may yield conclusions concerning the ancestry or health risks of an entire community, which may be misinterpreted or employed to stigmatise it.

Cross-border transfers: the movement of data between states with divergent privacy regimes impedes consistent protection.

Long-term storage: samples may be retained for many years, raising the question of whether the original consent remains valid.

Technical measures such as encryption and controlled access may mitigate certain of these risks, but they do not substitute for legitimate and accountable community governance.

Traditional Knowledge, Biopiracy and Benefit-Sharing

Many Indigenous communities possess long-standing knowledge concerning plants, medicines, agriculture and ecosystems. Scientific research founded upon this knowledge may yield genuine benefits; difficulties arise, however, where such knowledge is used without permission, acknowledgement or an equitable share of the resulting benefits.

The CBD and the Nagoya Protocol provide frameworks governing biodiversity-related genetic resources and associated traditional knowledge. Not every dispute concerning traditional knowledge constitutes a breach of a specific treaty obligation; the applicable legal framework, the consent arrangements in place and the rights of the community concerned determine the position in each instance.

Notable Biopiracy Disputes

Although the Havasupai case concerns human DNA, many of the most prominent disputes involve traditional knowledge relating to plants. They demonstrate the capacity of the patent system to permit external parties to claim ownership of knowledge that communities have employed for centuries.

Neem (India): The neem tree has been employed in India for centuries as a natural pesticide and medicine. In 1994, the European Patent Office granted a patent on a method of using neem oil as a fungicide to the United States Department of Agriculture and a United States company. Indian farmers' organisations and international campaigners challenged the patent on the ground that the method already formed part of Indian traditional knowledge. The patent was revoked in 2000, and the decision was upheld on appeal in 2005.

Turmeric (India): In 1995, the United States Patent and Trademark Office granted a patent for the use of turmeric in wound healing. India's Council of Scientific and Industrial Research challenged the patent by submitting documentary evidence, including ancient Sanskrit texts, demonstrating that this use was already well established. The patent was cancelled in 1997.

Hoodia (Southern Africa): A plant compound was patented on the basis of the traditional knowledge of the San peoples, which subsequently led to a benefit-sharing agreement. This case is examined in detail among the case studies below. These disputes prompted several developing states to establish traditional knowledge databases, most notably India's Traditional Knowledge Digital Library, which enables patent examiners to determine whether a claimed invention in fact constitutes existing traditional knowledge.

Principal Arguments in the Debate

The debate on this agenda is characterised by substantial arguments on both sides.

Arguments in favour of broader genetic data sharing:

- Open data accelerates medical discovery, which may benefit all populations, Indigenous communities included.
- The under-representation of Indigenous Peoples in research diminishes the effectiveness of medicine for these populations.
- Stringent regulation may discourage researchers from engaging with Indigenous communities altogether.
- De-identification and security measures are capable of reducing privacy risks.
- Benefit-sharing may be secured through funding and partnership arrangements without restricting access to data.

Arguments in favour of strong Indigenous control:

- Indigenous Peoples possess a right to self-determination, which encompasses decisions concerning the use of data about them.

Past research has frequently harmed Indigenous communities, such that trust must be re-established before data is shared.

- Genetic findings may affect entire communities, rendering individual consent alone insufficient.
- Genetic data can rarely be rendered fully anonymous, and technical security is not equivalent to community control.
- In the absence of genuine control, undertakings regarding benefit-sharing are frequently weak or remain unfulfilled.

Much of the contemporary debate concerns the conditions under which research with Indigenous communities may legitimately proceed, rather than a binary choice between prohibition and unrestricted access.

Indigenous-Led Initiatives

Indigenous Peoples have not merely resisted harmful research; they have also established their own systems of responsible research and data governance. Notable examples include the following:

Te Mana Raraunga (New Zealand): the Māori Data Sovereignty Network, founded in 2015, which advances Māori rights and interests in data and has articulated principles of Māori data governance.

Maiaṃ nayri Wingara (Australia): an Aboriginal and Torres Strait Islander data sovereignty collective that has formulated principles of Indigenous data governance in Australia.

The San Code of Research Ethics (South Africa): published by the South African San Council in 2017, it was among the first codes of research ethics developed by an Indigenous people in Africa. It requires of researchers respect, honesty, justice, fairness and care.

The Native BioData Consortium (United States): a tribally led, non-profit biorepository and research organisation established to enable tribes to store and govern their own biological samples and data on tribal land.

SING (Summer Internship for Indigenous Peoples in Genomics): a training programme established in the United States in 2011 that instructs Indigenous students and community members in genomics, enabling communities to participate in research as experts rather than solely as subjects.

These initiatives indicate that the objective of Indigenous data sovereignty is not the obstruction of science, but rather the conduct of science on equitable terms and the development of Indigenous research capacity.

International Legal and Ethical Frameworks

Universal Declaration of Human Rights (1948). Provides the foundation for the principles of dignity, equality and human rights; it does not, however, specifically regulate Indigenous genetic data.

International Covenant on Civil and Political Rights (1966). Protects privacy (Article 17) and the cultural rights of minorities (Article 27), but does not establish a comprehensive regime for the governance of genetic data.

ILO Convention No. 169 (1989). Protects the rights, institutions and consultation entitlements of Indigenous and tribal peoples; it is binding only upon those states that have ratified it.

Convention on Biological Diversity (1992). Addresses biodiversity, traditional knowledge and benefit-sharing, but does not constitute a framework for human genetic data.

UNESCO Declarations (1997 and 2003). Set out principles concerning human dignity, consent and the use of human genetic data. They are non-binding and give limited attention to the collective rights of Indigenous Peoples.

United Nations Declaration on the Rights of Indigenous Peoples (2007). Recognises self-determination, cultural heritage and participation. As a declaration rather than a treaty, its implementation varies considerably between states.

Nagoya Protocol (2010). Establishes rules for covered genetic resources and associated traditional knowledge, but does not comprehensively govern human genomic data.

CARE Principles. Provide an Indigenous-centred framework for data governance and collective benefit; they are voluntary rather than binding.

OCAP® Principles. Support First Nations authority over data in Canada; they are specific to First Nations and are not of universal application.

These instruments differ in legal status and scope: declarations and voluntary frameworks do not carry the binding force of treaties, and neither the CBD nor the Nagoya Protocol extends to human DNA in general.

Principal Challenges for the International Community

Individual consent and collective interests: samples are obtained from individuals, yet the resulting findings may affect entire communities, and Indigenous Peoples govern themselves through diverse institutions.

Open science and data sovereignty: the open sharing of data accelerates scientific progress, but unrestricted access may conflict with privacy and cultural protection.

Unequal access to benefits: researchers and corporations possess the financial resources and expertise necessary to convert samples into discoveries, whereas communities typically exercise far less influence over the outcomes.

Divergent national legislation: states protect genetic data and Indigenous rights in markedly different ways, which complicates international research collaboration.

Deficit of trust: historical exploitation has rendered many communities wary of research, and trust depends upon transparency, enduring relationships and accountability rather than upon a single act of consent.

Key Stakeholders and Positions

States with significant Indigenous populations. States such as Canada, Australia, New

Zealand and the United States are principally concerned with the interaction between Indigenous rights, national research programmes and existing domestic legislation. All four voted against UNDRIP in 2007 but subsequently endorsed it. These states are generally receptive to Indigenous data governance, while tending to favour non-binding instruments and national approaches over binding international obligations.

Latin American states. States such as Bolivia, Ecuador and Peru attach particular importance to biodiversity, traditional knowledge and the constitutional recognition of Indigenous rights. They have generally been strong proponents of free, prior and informed consent, benefit-sharing and protection against biopiracy. Bolivia incorporated UNDRIP into its national legislation in 2007.

Biodiversity-rich developing states. These states are principally concerned with the inequitable exploitation of their genetic resources and traditional knowledge by wealthier states and corporations. They have consistently supported robust access and benefit-sharing regimes, including the Nagoya Protocol and the development of new rules concerning digital sequence information.

Research-intensive and biotechnology states. These states prioritise scientific progress, open science and the competitiveness of their biotechnology industries. They generally favour voluntary guidelines over binding rules and emphasise the benefits of data sharing. The United States is not a party to the CBD.

African states. African states have expressed concern regarding the exploitation of genetic resources and the limited capacity of domestic health research institutions. They have generally supported capacity-building, equitable research partnerships and the strengthening of African-led research governance.

Indigenous organisations and civil society. These actors emphasise self-determination, cultural protection and community consent. They have called for Indigenous authority over data, adherence to free, prior and informed consent, and the return of samples obtained without consent.

Universities, biobanks and corporations. These institutions are concerned with access to samples, the availability of funding and legal certainty. They generally support clear and workable regulation but may resist rules perceived as obstructing research.

UNDRIP was adopted in 2007 by a recorded vote of 144 in favour, 4 against (Australia, Canada, New Zealand and the United States) and 11 abstentions. Each of the four states that voted against the Declaration has since endorsed it.

PAST UN ACTIONS

The United Nations has addressed questions relating to biocolonialism through instruments and bodies concerned with human rights, the rights of Indigenous Peoples, the protection of biodiversity and the governance of data. No single United Nations treaty, however, comprehensively regulates Indigenous genetic privacy and data sovereignty; the relevant measures each address a portion of the issue.

Adoption of the United Nations Declaration on the Rights of Indigenous Peoples (2007)

On 13 September 2007, the General Assembly adopted the United Nations Declaration on the Rights of Indigenous Peoples, which has since served as the principal international framework for Indigenous rights. Although it is a declaration rather than a treaty, it established important standards. The provisions of greatest relevance to this agenda are:

Article 3 (Self-determination): the right of Indigenous Peoples freely to determine their political status and to pursue their economic, social and cultural development.

Article 11 (Cultural heritage): the right to practise and revitalise cultural traditions, including redress for cultural, intellectual, religious and spiritual property taken without free, prior and informed consent.

Article 19 (Participation and consent): the obligation of states to consult and cooperate in good faith with Indigenous Peoples, through their own representative institutions, in order to obtain their free, prior and informed consent before adopting measures that may affect them.

Article 24 (Traditional medicines and health): the right to traditional medicines and to the maintenance of health practices.

Article 31 (Cultural and intellectual heritage): the right to maintain, control, protect and develop cultural heritage, traditional knowledge and associated intellectual property.

The Third Committee has subsequently adopted resolutions on the rights of Indigenous Peoples on a regular basis, reaffirming the Declaration and calling for its implementation.

Study of the Expert Mechanism on the Rights of Indigenous Peoples (2025)

In 2025, the Expert Mechanism on the Rights of Indigenous Peoples (EMRIP) published its study *Right of Indigenous Peoples to Data, Including with Regard to Data Collection and Disaggregation* (A/HRC/60/66). The study characterised Indigenous data as a cultural, strategic and economic resource, potentially encompassing information concerning language, culture, genetic characteristics, environments and resources. It recommended:

- meaningful Indigenous participation in the collection and analysis of data;
- Indigenous access to data concerning their communities;
- the protection of sensitive personal information and traditional knowledge;
- the recognition of Indigenous authority over data governance;
- increased Indigenous participation in national statistical institutions;
- support for Indigenous-led data systems and measures to address digital inequality.

The study constitutes one of the United Nations sources most directly relevant to this agenda, although it is an expert study rather than a binding instrument.

Work of the Permanent Forum on Indigenous Issues

The United Nations Permanent Forum on Indigenous Issues (UNPFII), an advisory body to the Economic and Social Council, has addressed Indigenous issues relating to development, culture, the environment, education, health and human rights. The Forum has repeatedly emphasised that reliable data is necessary for the identification of discrimination and inequality, while cautioning that data collection may cause harm where Indigenous Peoples are excluded from decisions

concerning their representation. The Forum also considered Indigenous concerns regarding the Genographic Project.

The Convention on Biological Diversity and the Nagoya Protocol

The Convention on Biological Diversity, opened for signature in 1992, addressed traditional knowledge relevant to biodiversity in Article 8(j). The Nagoya Protocol, adopted in 2010 and in force since 2014, established rules governing access to covered genetic resources and the fair and equitable sharing of benefits; its Article 12 addresses traditional knowledge associated with genetic resources. These instruments apply where Indigenous knowledge of plants or medicines is employed in research or commercial products, but they do not govern human genetic information.

Digital Sequence Information and the Cali Fund

The Parties to the CBD have also addressed digital sequence information (DSI), namely genetic sequences stored digitally in online databases. Because such sequences may be exploited without physical access to the source organism, numerous developing states contended that corporations were circumventing benefit-sharing obligations. In 2022, the Kunming-Montreal Global Biodiversity Framework provided for the establishment of a multilateral mechanism for sharing the benefits arising from the use of DSI. In 2024, at the sixteenth meeting of the Conference of the Parties in Cali, Colombia, the Parties launched the Cali Fund, which invites corporations that derive profit from DSI to contribute a portion of those profits, with a share designated for Indigenous Peoples and local communities. The Cali Fund concerns non-human genetic resources, and contributions to it are largely voluntary.

UNESCO Declarations on Human Genetic Data

UNESCO adopted two declarations of direct relevance to human genetics. The *Universal Declaration on the Human Genome and Human Rights* (1997) affirmed that the human genome is, in a symbolic sense, the heritage of humanity, that individuals must not be reduced to their genetic characteristics, and that the human genome in its natural state shall not give rise to financial gain. The *International Declaration on Human Genetic Data* (2003) established principles concerning

prior, free and informed consent, confidentiality, and the conditions governing the collection, storage and use of human genetic data. Both instruments are non-binding and neither fully addresses the collective rights of Indigenous Peoples; they nonetheless demonstrate that the United Nations system has recognised genetic data as a category of particular sensitivity.

World Health Organization Participatory Framework (2026)

In August 2026, the World Health Organization published an unedited final draft of its

Participatory Framework for Respectful Engagement with Indigenous Peoples on Biodiversity, Health and Traditional Knowledge Systems. The Framework translated international standards into practical guidance, emphasising self-determination and free, prior and informed consent, Indigenous data sovereignty, reciprocity and shared governance, the protection of traditional knowledge, and accountability. It constitutes practical guidance rather than a binding instrument.

Limitations of Existing Measures

Fragmentation: human rights, biodiversity, privacy and research ethics are governed by separate instruments, and no single comprehensive framework exists.

Uneven national implementation: states differ in their legislation, resources and recognition of Indigenous rights.

Cross-border data flows: genetic data moves between jurisdictions, which impedes effective oversight.

Limited community resources: many communities lack the financial means and expertise required to negotiate complex research agreements.

Accountability gaps: international recommendations do not of themselves translate into effective national protections.

CASE STUDIES

The Havasupai Tribe (United States)

The Havasupai are a small tribe of approximately 650 members residing at the base of the Grand Canyon in Arizona. Around 1990, approximately 200 tribal members provided blood samples to researchers from Arizona State University in the expectation that the research would explain the high prevalence of type 2 diabetes within the community. The consent form employed broad language referring to the study of the causes of "behavioral/medical disorders"; many participants possessed limited proficiency in English and understood the research to concern diabetes alone.

The diabetes research did not identify a genetic association. The samples were nevertheless distributed to other researchers and employed in numerous studies and academic publications, including research on schizophrenia, inbreeding and ancestry. Tribal members learned of these additional uses only years later. The ancestry research proved particularly harmful, since it indicated that the tribe's ancestors had migrated from Asia, in contradiction of the tribe's traditional belief that its people originated in the Grand Canyon. The research on inbreeding and schizophrenia was likewise regarded as stigmatising. In response, the tribe barred university researchers from its reservation, and in 2004 tribal members initiated legal proceedings.

Outcome. The dispute was settled in 2010. Arizona State University agreed to pay \$700,000 to 41 tribal members and to return the remaining blood samples. The university further agreed to provide other forms of assistance, including support for a health clinic and scholarships for tribal members.

Principal issues raised:

- whether participants understood the potential future uses of their samples;
- whether the consent documentation adequately disclosed additional research purposes;
- whether researchers took account of the community's cultural beliefs and expectations;
- how stored samples ought to be managed as new research questions arise.

The OCAP® Principles (Canada)

The First Nations Information Governance Centre promotes OCAP®, a framework developed by First Nations in Canada:

Ownership: First Nations hold a collective relationship to information concerning their communities.

Control: First Nations exercise authority over research and information management affecting them.

Access: First Nations may access data concerning their communities, including data held by external institutions, and may govern access to it.

Possession: physical custody of data constitutes a practical means of supporting control.

Significance. OCAP® departs from the assumption that research institutions automatically control all data they collect, demonstrating that data sovereignty concerns not merely cybersecurity but the question of who holds decision-making authority.

Limitation. OCAP® was developed specifically for First Nations in Canada and is not a universal model applicable to all Indigenous Peoples.

The CARE Principles (International)

The Global Indigenous Data Alliance promotes the CARE Principles in response to the concern that conventional data-sharing systems emphasise accessibility and reuse while neglecting Indigenous rights and unequal relations of power:

Collective Benefit: data practices should yield meaningful benefits for Indigenous communities.

Authority to Control: Indigenous Peoples should exercise authority over decisions concerning their data.

Responsibility: researchers and institutions should discharge their obligations to affected communities.

Ethics: data practices should respect Indigenous rights, values and cultural expectations.

The CARE Principles are designed to operate in conjunction with the FAIR Principles (Findable, Accessible, Interoperable, Reusable). Their central premise is that the ease with which data may be accessed does not render every use of that data appropriate, and that communities may possess legitimate grounds for restricting sensitive information.

The EMRIP Study on Indigenous Data (2025)

The study of the Expert Mechanism on the Rights of Indigenous Peoples (A/HRC/60/66) examined the relationship between data collection and disaggregation, on the one hand, and Indigenous rights and self-determination, on the other. Although it addressed Indigenous data generally rather than genetic privacy specifically, it advanced a proposition central to this agenda: that Indigenous data governance is a matter of self-determination rather than a purely technical question. The study supports community participation and safeguards throughout the data lifecycle.

Under-representation in Genomic Research

Indigenous populations have historically been under-represented in genetic studies. Where datasets predominantly represent particular populations, the resulting medical findings may be less accurate or less applicable for others. Increased participation may render research more inclusive; representation in the absence of appropriate governance, however, risks deepening mistrust and inequality. The underlying difficulty lies in increasing Indigenous participation without reproducing extractive practices.

The Hoodia Plant and the San Peoples (Southern Africa)

Background. For generations, San hunters in the Kalahari Desert have chewed the Hoodia plant to suppress hunger and thirst during extended hunts. Researchers at South Africa's Council for Scientific and Industrial Research (CSIR) studied the plant and isolated an appetite-suppressing compound, which the CSIR patented in the 1990s and licensed to corporations seeking to develop a weight-loss product for the global market.

Controversy. The San were not consulted when the patent was filed. Upon public disclosure, the patent was widely criticised as an instance of biopiracy, since the commercial value of the plant derived directly from San traditional knowledge.

Outcome. In 2003, the CSIR and the San concluded a benefit-sharing agreement entitling the San to a share of any future royalties. The anticipated commercial product was, however, never successfully brought to market, and the financial benefits received were consequently limited. The San subsequently drew upon this experience in developing the San Code of Research Ethics, published in 2017.

QUESTIONS A RESOLUTION MUST ANSWER (QARMA)

Consent and Community Participation

1. By what means can states ensure that Indigenous participants understand the purpose, risks and potential future uses of genetic research?
2. How should the secondary use of biological samples and genetic data be regulated?
3. How may individual informed consent be supplemented by appropriate community engagement?
4. How can Indigenous representative institutions participate meaningfully in decisions affecting their communities, with due respect for differing languages, customs and systems of decision-making?

Genetic Privacy and Data Security

5. What minimum safeguards should research institutions adopt for the protection of sensitive genetic information?
6. How can the risk of re-identification from de-identified datasets be reduced?
7. What rules should govern the transfer of genetic data across borders?
8. How should institutions respond to unauthorised access to, or misuse of, genetic data?
9. What rules should govern the storage, destruction or return of samples upon the conclusion of a project?

Indigenous Data Sovereignty

How can Indigenous communities exercise effective authority over data held by external institutions?

Should states support Indigenous-led data-governance bodies and community research protocols?

To what extent should the CARE Principles inform international recommendations?

How can data sovereignty be protected without the imposition of a single model upon culturally diverse communities?

Traditional Knowledge and Benefit-Sharing

How can states prevent the inequitable appropriation of traditional knowledge?

What benefit-sharing arrangements are appropriate where research gives rise to commercial products?

How may the CBD and the Nagoya Protocol be applied where relevant, without overstating their scope?

What support should be extended to Indigenous-led research, education and community health programmes?

International Cooperation, Accountability and Implementation

How can states cooperate notwithstanding differences in national privacy and research-ethics legislation?

What responsibilities should universities, corporations, research funders and public institutions bear?

How can open science and medical innovation be reconciled with the rights of Indigenous Peoples?

What reporting or review mechanisms could measure progress without the collection of unnecessary data concerning communities?

How can states with limited resources finance Indigenous-led research and provide the requisite training and infrastructure?

How can new measures complement, rather than duplicate, the work of existing United Nations bodies?

AGENDA B

ADDRESSING ALGORITHMIC DISCRIMINATION IN IMMIGRATION AND ASYLUM SYSTEMS

INTRODUCTION TO THE AGENDA

Algorithmic discrimination in immigration and asylum systems arises where automated decision-making (ADM) and artificial intelligence (AI) systems produce unjust or biased outcomes to the detriment of migrants and refugees.

Governments and border authorities increasingly employ such technologies, which range from risk-assessment algorithms and automated visa-triage tools to emotion detection and dialect recognition, in order to process large volumes of applications and to enforce border security. These systems are promoted as a means of accelerating procedures, reducing backlogs and rendering decisions more objective.

In practice, however, they frequently reproduce and amplify existing human biases. Predictive algorithms are trained on historical data generated by past law enforcement and border practices; they consequently tend to reflect existing inequalities and may unjustly classify persons of particular nationalities, ethnic groups or economic backgrounds as "high risk" or as likely to be fraudulent.

Contemporary Context

The number of persons forcibly displaced from their homes has reached unprecedented levels. The Office of the United Nations High Commissioner for Refugees (UNHCR) reported that more than 120 million people had been forcibly displaced worldwide by mid-2024 as a result of war, persecution, violence and human rights violations. Many states face substantial backlogs of asylum applications, and governments are subject to considerable political pressure to expedite procedures and to strengthen border control.

Technology companies present automated tools as a response to these pressures, and the global market for border security technology is now valued at tens of billions of United States dollars annually. Decisions formerly taken by human officials, such as the grant of a visa, the imposition of detention and the assessment of the credibility of an asylum claim, are consequently being shaped to an increasing extent by software.

The consequences of such decisions are grave. For an asylum seeker, an erroneous decision may result in return to a state in which they face torture or death; for a visa applicant, it may entail separation from family or the loss of educational opportunity. Since migrants and refugees frequently possess limited legal protection, limited financial means and limited familiarity with the language and legal system of the host state, they are particularly ill-equipped to challenge an unjust automated decision.

Mechanisms of Algorithmic Bias

Algorithms are not neutral merely by virtue of being automated. Bias may enter a system at several stages:

Biased data: where past decisions were unjust towards a particular group, an algorithm trained upon those decisions will learn to replicate that injustice.

Biased design choices: the developers of a system determine which variables it takes into account, such as nationality or travel history, and these choices may embed discrimination directly within the system.

Proxy variables: even where race or religion are excluded, other variables such as postcode, language or occupation may function as substitutes and produce equivalent discriminatory outcomes.

Differential accuracy: a system may perform reliably for certain groups but poorly for others, as is the case with facial recognition systems that exhibit higher error rates for individuals with darker skin tones.

Feedback loops: where a system flags a particular nationality more frequently, officials investigate that group more intensively, detect more cases and thereby reinforce the system's classification of the group as "high risk".

Automation bias: human officials frequently place excessive reliance on computer-generated recommendations and endorse them without adequate

scrutiny, such that the presence of a "human in the loop" may not constitute an effective safeguard.

Algorithmic discrimination therefore threatens fundamental human rights standards, including the right to due process, the right to non-discrimination and the protection afforded to asylum seekers under international law, in particular the principle of non-refoulement.

KEY TERMS AND DEFINITIONS

Algorithmic Discrimination: Unjust treatment of individuals or groups resulting from automated processing, flawed design or biased training data.

Automated Decision-Making (ADM): Technology, including machine learning, that makes or supports administrative decisions without direct and meaningful human involvement.

Training Data Bias: Errors or imbalances in the historical data used to train AI systems, frequently reflecting past discrimination or the under-representation of particular groups.

Black Box Phenomenon: The opacity of complex algorithms, which impedes the ability of applicants and their legal representatives to understand the basis upon which a decision was reached.

Principle of Non-Refoulement: A fundamental principle of international refugee law prohibiting states from returning a refugee to a territory in which their life or freedom would be threatened.

Algorithmic Profiling: The classification of individuals into risk categories on the basis of characteristics such as nationality, gender or travel route, by means of statistical inference.

Proxy Discrimination: Discrimination arising where an ostensibly neutral variable, such as place of residence or occupation, correlates closely with a protected characteristic, such as race or nationality.

Biometric Surveillance: The automated collection and analysis of unique physical characteristics, such as the face, fingerprints or iris, for the purposes of identification and tracking.

Risk Assessment Triage: The use of automated tools to classify applications into high, medium or low-risk categories.

Natural Language Processing (NLP): AI techniques for the analysis of text and speech, employed in immigration procedures for dialect recognition and document verification.

Human-in-the-Loop: A requirement that a human official review, approve or override an automated recommendation.

Predictive Analytics: The use of historical data and statistical methods to forecast future behaviour, movement or risk.

Emotion Recognition and AI Lie Detection: Experimental technologies that purport to assess truthfulness from facial expressions, voice or physiological signals, the scientific validity of which is widely disputed.

Function Creep: The gradual extension of the use of data collected for one purpose to other purposes, such as law enforcement.

Data Sovereignty: The principle that data collected from individuals or communities remains subject to their consent, governance and legal protection.

HISTORY AND BACKGROUND

From Databases to Prediction

The use of digital tools in migration management commenced in the late 1990s and early 2000s. These tools principally comprised centralised databases, digital identity documents and shared border watchlists, which enabled authorities to verify identities rapidly against law enforcement records.

During the 2010s, states progressed from the storage of data to the active prediction of risk. Machine learning models were introduced to triage applications, calculate risk scores and flag cases for review. This transition was driven by political imperatives to reduce costs and backlogs and to manage increasing migration through automation.

By the late 2010s and early 2020s, border authorities had begun to deploy experimental AI tools, including dialect and accent recognition, facial recognition at checkpoints and predictive models for anticipating population movements. As

these tools proliferated, legal practitioners, non-governmental organisations and human rights bodies documented serious deficiencies. In the absence of adequate regulation, opaque algorithms operated with minimal public oversight, giving rise to concerns regarding arbitrary refusals and the erosion of due process for non-citizens.

Key Turning Points

2001: September 11 attacks. Migration became increasingly framed as a matter of national security, prompting the expansion of biometric databases, inter-agency data sharing and pre-arrival risk assessment.

2015: European migration crisis. The European Union introduced the "hotspot approach" and expanded systems such as Eurodac for the registration of arrivals at its external borders.

2018: Global Compacts on Migration and on Refugees. States agreed non-binding standards, including standards relating to data and legal identity, premised upon respect for human rights.

2018: iBorderCtrl pilot. An EU-funded automated deception-detection project for travellers was tested at borders in Hungary, Latvia and Greece, attracting widespread criticism.

2020: COVID-19 pandemic. Contactless, automated and exclusively online procedures became standard practice.

2020: Withdrawal of the United Kingdom's visa streaming tool. The first significant legal success against a nationality-based immigration algorithm.

2024: EU Pact on Migration and Asylum. The Screening Regulation rendered health, identity and security checks mandatory for irregular arrivals, relying extensively upon automated database checks and risk algorithms.

2024: EU Artificial Intelligence Act and Council of Europe Framework Convention on Artificial Intelligence. The first major legal frameworks for AI, both of which contain significant gaps in respect of migration.

2025: Commencement of the EU Entry/Exit System (EES). The European Union began progressively replacing passport stamps with the digital registration of the fingerprints and facial images of non-EU travellers.

2026: Eurodac upgrade and ETIAS launch. Expanded biometric collection and automated pre-travel screening.

SOCIAL, POLITICAL AND ECONOMIC DIMENSIONS

Social Dimension

The automation of immigration and asylum procedures carries significant social consequences for those subject to it. Digital-only procedures exclude individuals who lack smartphones, internet access, literacy or proficiency in the relevant language, thereby converting the digital divide into a barrier to protection. Profiling on the basis of nationality or ethnicity stigmatises entire populations and may reinforce xenophobic attitudes within host societies. Wrongful refusals may result in prolonged family separation, interrupted education and protracted uncertainty, with attendant psychological harm for persons who have frequently already experienced trauma. The replacement of human interaction with automated processes has, moreover, been described by displaced persons as dehumanising, and contributes to an erosion of trust in the institutions upon which they depend for protection.

Political Dimension

Politically, the agenda reflects a tension between the sovereign prerogative of states to control entry to their territory and their obligations under international human rights and refugee law. The securitisation of migration since 2001 has permitted states to invoke national security exemptions that shield border technologies from transparency and oversight. The externalisation of border control through cooperation with transit states, and the sharing of data with third countries, raises questions of accountability and of complicity in violations, including transnational repression by states of origin. Nationality-based visa profiling also bears upon relations between states, since countries of origin in the Global South regard such practices as discriminatory towards their nationals. Finally, the opacity of automated systems limits democratic and judicial scrutiny of decisions of considerable consequence.

Economic Dimension

The border security technology market, valued at tens of billions of United States dollars annually, has created powerful commercial incentives for the expansion of automated systems. Governments rely upon private contractors for the design and operation of these systems, and commercial confidentiality is frequently invoked to resist disclosure of source code and training data. Automation is promoted on the ground of cost efficiency, yet erroneous decisions generate substantial costs in the form of appeals, litigation and wrongful detention. Developing states that procure such technology, often through development assistance, may become dependent upon foreign vendors without acquiring the capacity to audit it. Discriminatory visa refusals also carry economic consequences, impeding the movement of students, workers, entrepreneurs and tourists, and thereby affecting remittances, trade and labour markets in both sending and receiving states.

SPECIFIC RESEARCH AND ANALYSIS

The Legal Baseline: The Right to Privacy

Article 12 of the Universal Declaration of Human Rights protects against arbitrary interference with privacy, family and home. This protection is given binding effect by Article 17 of the International Covenant on Civil and Political Rights and Article 8 of the European Convention on Human Rights (ECHR), which require any interference with privacy to be lawful, necessary and proportionate. The report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) entitled *The Right to Privacy in the Digital Age* (A/HRC/48/31, 2021) applied this test to profiling, automated decision-making and machine learning, and examined border management as one of the affected sectors.

The Structural Problem

According to OHCHR, border management is increasingly situated within security and enforcement frameworks that accord limited attention to human rights law. Migrants at borders are seldom in a position to defend their privacy, as states seek to collect ever greater quantities of data. The validity of consent at the border is questionable, since migrants frequently cannot realistically decline to provide their data.

In October 2021, the United Nations Special Rapporteur on contemporary forms of racism, E. Tendayi Achiume, found in report A/HRC/48/76 that non-citizens and stateless persons lack many of the legal protections afforded to citizens, while governments retain broad and frequently unreviewable powers at the border. The Special Rapporteur called for a moratorium on the procurement and use of surveillance technology in immigration enforcement.

Categories of Data Collected

Border systems now collect fingerprints, facial images, iris scans, voice recordings and, in certain instances, gait patterns. Each biometric check extends the intrusion of the state into private life, and each leaves a record capable of disclosing confidential information. Concerns documented in this regard include:

the dignity of veiled Muslim women subjected to iris scans in stressful conditions; reports by the European Union Agency for Fundamental Rights (FRA) of the use of excessive force in the fingerprinting of asylum seekers.

Data Sharing with Countries of Origin

A failure of privacy becomes a failure of protection where the personal data of refugees or dissidents reaches the governments from which they fled. Where biometric records, location data or the content of asylum claims are disclosed to such a government, the safety of the individual is directly endangered.

Authoritarian states may employ such data for the purposes of transnational repression, including the harassment of persons abroad, the coercion of their return and the punishment of family members remaining in the country of origin. In this context, the failure to protect data may amount to a failure to protect life.

Consent, Data Minimisation and Function Creep

AI systems presented as objective may be experienced by displaced persons as exclusionary and dehumanising. The failure to receive a single digital notification may cause a refugee to forfeit a legal appointment, and linguistic or technical barriers may prevent an individual from completing an online form upon which their future depends. The Jesuit Refugee Service (JRS) Europe has documented such exclusion in Greece, Hungary and Malta, including cases of detained persons unable to communicate with the outside world or to understand their rights.

Scholars have further identified a "privacy disconnect", namely a divergence between privacy rules as formulated and their operation in practice. In light of the imbalance of power between migrants and states, reliance upon consent as a legal basis for data processing is increasingly contested. There is, in addition, a risk that predictive and biometric tools may be repurposed in the service of restrictive immigration policies.

AI Bias in Refugee Status Determination

AI may, in principle, reduce random error in asylum decisions through the identification of patterns. It equally risks replicating and amplifying human bias through biased data, flawed design and inadequate testing, and may give rise to proxy discrimination, whereby ostensibly neutral variables stand in for protected characteristics.

Refugee status determination presents particular difficulties for AI for the following reasons:

- statistical inference cannot establish the facts of an individual case;
- a pre-existing "culture of disbelief" already requires asylum seekers to overcome the scepticism of officials;
- asylum cases involve uncertainty and atypical circumstances, demanding human reasoning as to the most probable explanation;
- AI is poorly suited to the low thresholds of probability applied in asylum law, under which a reasonable likelihood of persecution may suffice;
- large language models may generate confident but inaccurate outputs rather than acknowledge uncertainty.

Digital Borders and Externalisation

Borders are increasingly relocating from physical checkpoints into software, mobile applications and biometric screening, at times far removed from the territorial frontier. Although digitisation promises certain improvements, it may obstruct access to asylum for persons unable to navigate digital barriers. Examples include:

- mandatory applications such as the CBP One application of the United States;

facial recognition systems that perform less accurately for darker-skinned and Black individuals;
the extraction of data from migrants' mobile telephones;
automated surveillance in refugee camps, such as those in Greece;
experimental deception-detection trials such as the EU-funded iBorderCtrl project. Critics contend that these tools may conceal discrimination behind claims of "technical error", weaken legal accountability and divert resources towards technology contracts and away from humanitarian assistance.

Evidence of Bias in Facial Recognition

Concerns regarding facial recognition are supported by empirical research. In 2018, the *Gender Shades* study by Joy Buolamwini and Timnit Gebru evaluated commercial facial analysis systems and found them to be substantially less accurate for women with darker skin than for men with lighter skin. In 2019, the United States National Institute of Standards and Technology (NIST) evaluated a large number of facial recognition algorithms and found that many produced higher rates of false matches for African, East Asian and other non-white faces than for white faces, although the magnitude of the disparity varied considerably between algorithms.

In the border context, such errors carry serious consequences. A false match may result in the misidentification of an individual as a person on a watchlist, while a failure to match may prevent an individual from completing an application, as has been reported in connection with the CBP One application.

Arguments For and Against Automation

Arguments in favour of automated border tools:

- They are capable of processing large volumes of applications rapidly and reducing protracted backlogs.
- They may reduce the influence of the personal prejudices of individual officials.
- Biometric systems may assist in preventing identity fraud and in tracing missing or trafficked children.

They assist states in managing security risks and discharging their duty to protect their populations.

Technology may enable procedures to be conducted online, without the necessity of travel to a consulate.

Arguments against automation, or in favour of strict limitations:

Expedition is of no value where decisions are unjust or erroneous, particularly where lives are at stake.

Automated tools may replicate and conceal the prejudices embedded in historical data on a considerably larger scale.

Biometric data is permanent; where it is misused or disclosed, individuals cannot alter their faces or fingerprints.

Security exemptions are frequently invoked to evade transparency, oversight and accountability.

Digital-only systems exclude persons without smartphones, internet access, literacy or proficiency in the relevant language.

Few states advocate a comprehensive prohibition of technology at borders. The principal debate therefore concerns which uses are acceptable, which safeguards are necessary, and which tools present risks so severe as to preclude their use.

Existing International Frameworks

EU Artificial Intelligence Act (2024): classifies AI systems employed in migration, asylum and border control as high-risk, subjecting them to requirements concerning data governance, accuracy, transparency and human oversight.

Council of Europe Framework Convention on Artificial Intelligence (2024): promotes a human-rights-based approach and impact assessment, including by means of the HUDERIA methodology.

EU General Data Protection Regulation (GDPR), Article 22: protects individuals against decisions based solely on automated processing that produce legal or similarly significant effects, although gaps in enforcement persist.

1951 Refugee Convention, 1967 Protocol and the ECHR: prohibit collective expulsion, arbitrary detention and refoulement; these obligations cannot be displaced by any algorithmic process.

Gaps in the Existing Frameworks

Outdated instruments: earlier treaties guarantee substantive outcomes such as non-refoulement and privacy but contain no procedural rules governing algorithmic risk assessment.

Exceptions within the EU AI Act: the Act prohibits no AI system specifically within the migration sector, excludes national security, and places migration systems in non-public registers.

Non-binding global instruments: most global AI frameworks are voluntary and contain no specific provisions concerning migration.

National security exemptions: the first binding AI treaty excludes activities relating to national security.

Weak agency-level rules: many internal agency guidelines lack binding legal force and fall outside the scope of data protection law.

Limitations of the EU Artificial Intelligence Act

No prohibition of emotion recognition at borders: Article 5 prohibits emotion recognition in workplaces and educational institutions on account of its unreliability and intrusiveness, but does not extend this prohibition to immigration, asylum or border control.

Non-public registration: high-risk systems must be registered in a public EU database, but systems employed in law enforcement, border control and migration are registered in a non-public section, limiting public scrutiny.

National security exemption: states may deploy unregulated AI systems by invoking national security.

Deferred enforcement: under the Digital Omnibus measures adopted in mid-2026, the binding deadlines applicable to high-risk systems listed in Annex III, which include border and migration tools, were deferred to December 2027, notwithstanding that the transparency obligations under Article 50 took effect in August 2026.

The Council of Europe Framework Convention on Artificial Intelligence

Adopted in 2024, the *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225) is the first legally binding international treaty concerning AI. Its signatories include the European Union, the United Kingdom, the United States, Canada, Japan, Israel, Switzerland and Ukraine. Article 3, however, excludes matters of national defence and national security. Since governments frequently characterise border management and security screening as matters of national security, they may thereby avoid the Convention's safeguards in their use of border surveillance technologies.

Major European Systems

ETIAS (European Travel Information and Authorisation System). ETIAS screens visa-exempt travellers by means of automated "risk indicators" derived from factors including age, sex, nationality, place of residence, education and occupation. Applications corresponding to a risk profile are referred for manual review. Critics have cautioned that reliance upon social, economic and national factors risks embedding proxy discrimination within border clearance procedures.

EUROSUR (European Border Surveillance System). Administered by Frontex, EUROSUR is a real-time network integrating satellite imagery, coastal sensors, vessel tracking and drones for the monitoring of the external borders of the European Union. Critics contend that the sharing of tracking data with the coast guards of third countries may facilitate interceptions and pushbacks before migrants reach waters in which they could claim asylum.

Eurodac and the biometric data of children. Under the reformed Eurodac Regulation, adopted as part of the 2024 EU Pact, the minimum age for the compulsory collection of fingerprints and facial images was lowered from 14 to 6 years. Proponents maintain that this measure assists in combating child trafficking, preventing family separation and tracing missing children. Critics regard it as coercive surveillance that treats migrant children as criminal suspects, is inconsistent with the United Nations Convention on the Rights of the Child, and exposes children to lifelong digital profiling.

Impacts on Vulnerable Groups

Children: AI-based age assessment using facial analysis, bone scans or radiography is frequently imprecise and may erroneously classify minors as adults, thereby depriving them of child protection safeguards.

LGBTQI+ asylum seekers: automated credibility and emotion assessment tools may rely upon stereotypes concerning behaviour, trauma and relationships, resulting in unjust refusals.

Persons with disabilities: biometric systems and online portals may fail to accommodate physical impairments.

Stateless persons: application systems may lack a category for persons without a recognised nationality, resulting in arbitrary refusals.

Generative AI and Machine Translation

Authorities increasingly employ machine translation and generative AI to translate interviews, process evidence and draft decisions. Machine translation frequently misinterprets legal terminology, regional dialects and context. Cases in the United States demonstrate that translation errors may generate apparent inconsistencies in an applicant's account, which are subsequently relied upon to impugn their credibility. Generative AI employed to summarise evidence or draft decisions may, moreover, introduce fabricated content, commonly termed "hallucinations", into legal determinations.

Data Retention and Deletion

Biometric data, digital records and social media information collected from migrants are frequently retained indefinitely. Even after an individual has been granted asylum or citizenship, their data may remain accessible to police and border authorities. In the absence of clear statutory limits on retention, rules on deletion and separation between systems, such data may be cross-referenced across law enforcement databases, exposing individuals to lifelong surveillance and creating serious risks in the event of disclosure or transfer to their state of origin.

Capacity Gaps and Vendor Dependency in the Global South

Many developing states procure AI, predictive software and biometric systems from foreign private contractors, frequently through development assistance. Their institutions may lack the expertise, independent oversight bodies and computing infrastructure necessary to audit these systems or to examine their training data for locally relevant biases. These states consequently become dependent upon foreign vendors and are unable to verify whether the technology conforms to their own constitutional requirements or to international human rights law.

Existing Accountability Mechanisms

Public algorithm registers: pioneered nationally by the Netherlands and at municipal level by cities such as Amsterdam and Helsinki, these registers require authorities to publish a list of the algorithms in use, together with their purpose, level of risk and human oversight arrangements.

Algorithmic Impact Assessments (AIAs): mandatory reviews conducted prior to the deployment of a system, examining risks of discrimination, privacy impacts and compliance with human rights.

Independent audits: periodic technical and legal examinations by third-party bodies to monitor bias, accuracy and compliance throughout the operational life of a system.

Key Stakeholders and Positions

Member States of the European Union. These states are concerned with the management of arrivals, internal security and the application of the EU AI Act and the GDPR. They generally support the regulated use of technology subject to safeguards, while defending large-scale systems such as Eurodac, ETIAS and the EES. Within the Union, certain states advocate stricter migration control, whereas others favour stronger protection of rights.

The United States and the United Kingdom. Both states prioritise border security, the reduction of asylum backlogs and the use of private technology contractors. They have generally favoured flexible national approaches and voluntary guidelines over binding international rules, with particular emphasis upon security requirements.

Countries of origin. Many states in Africa, Asia and Latin America are concerned that their nationals are profiled as "high risk" on the basis of nationality and denied equitable access to visas. These states are likely to support robust anti-discrimination standards, transparency and limitations upon nationality-based profiling.

Transit and partner states. States such as Türkiye, Libya, Mexico and Niger are concerned with funding and partnership arrangements with destination states, as well as with sovereignty and institutional capacity. They may accept border technology within the framework of cooperation agreements, while resisting external control of, or criticism directed at, their own practices.

Technology-producing states. These states seek to protect their technology industries and export markets. They generally favour innovation-oriented regulation and may resist comprehensive prohibitions or the compelled disclosure of source code.

Developing states procuring technology. These states lack the capacity to audit imported systems and are dependent upon foreign vendors. They are likely to support capacity-building, technology transfer and international assistance with auditing.

UNHCR, OHCHR and civil society. These actors are concerned with refugee protection, non-refoulement, privacy and equality. They have called for moratoriums on high-risk tools, full transparency, human review and effective remedies.

PAST UN ACTIONS

United Nations bodies and civil society organisations have consistently maintained that algorithmic decision-making must comply with the 1951 Refugee Convention, its 1967 Protocol and international human rights law. They have emphasised that opaque "black box" algorithms prevent asylum seekers from ascertaining why they were flagged or refused, thereby depriving them of an effective legal remedy.

Reports to the Human Rights Council

A/HRC/44/57 (2020), *Racial discrimination and emerging digital technologies.*

In this report, the Special Rapporteur on contemporary forms of racism called for a human-rights-based and intersectional approach to examining the capacity of AI to reproduce racial, ethnic and national-origin inequalities, even where it appears neutral. The report recommended transparency and accountability in the use of technology in the public sector, independent oversight and auditable systems, and affirmed that private companies share responsibility for discriminatory outcomes. It indicated that migrants and refugees would be addressed in a separate report.

A/HRC/48/76 (2021), *Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement.* In this follow-up report, the Special Rapporteur demonstrated that automated risk assessment, biometric collection and predictive border tools restrict access to justice, weaken due process and risk violating the principle of non-refoulement, and called for a moratorium on the use of surveillance technology in immigration enforcement.

Third Committee Resolutions on the Right to Privacy in the Digital Age

The Third Committee has regularly adopted resolutions entitled *The right to privacy in the digital age*, including A/RES/75/176 and A/RES/77/211. These resolutions affirmed that the rights individuals enjoy offline must also be protected online, and identified arbitrary digital surveillance, the collection of data without informed consent, and profiling as threats to individual freedom. They called upon states to ensure transparency, protect personal data and provide effective legal remedies.

CERD General Recommendation No. 36 (2020)

In 2020, the Committee on the Elimination of Racial Discrimination (CERD) adopted General Recommendation No. 36 on preventing and combating racial profiling by law enforcement officials. The Recommendation expressly applied anti-discrimination law to machine learning and algorithmic profiling, cautioning that algorithms trained on biased historical data reinforce systemic racism. It called for human rights impact assessments, transparency, and stringent oversight or prohibition of technologies whose risks of discrimination cannot be mitigated.

The International Convention on the Elimination of All Forms of Racial Discrimination

The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), adopted by the General Assembly in 1965, constitutes the binding legal foundation of the prohibition of racial discrimination. It prohibits practices, including automated risk scoring, that produce racially discriminatory effects. Articles 2 and 5 require states to review, amend or rescind laws and procedures that create or perpetuate racial discrimination, and to guarantee equal treatment before tribunals and other organs of the state.

Global Governance of Artificial Intelligence

The General Assembly adopted resolution A/RES/78/265 on seizing the opportunities of safe, secure and trustworthy AI systems for sustainable development, and resolution A/RES/78/311 on enhancing international cooperation on capacity-building in AI. It further adopted the Global Digital Compact as part of the Pact for the Future in 2024, and subsequently established the Independent International Scientific Panel on AI and the Global Dialogue on AI Governance. Collectively, these measures called for inclusive, human-rights-centred AI and for global cooperation to mitigate algorithmic risks.

UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)

In 2021, all Member States of UNESCO adopted the Recommendation on the Ethics of Artificial Intelligence, which established a global standard founded upon fairness, non-discrimination, transparency, accountability and human oversight. The Recommendation introduced practical instruments, including Ethical Impact Assessments, to assist governments in preventing AI from reinforcing bias prior to its deployment in the public sector.

Global Compacts on Migration and on Refugees (2018)

In 2018, the General Assembly affirmed the Global Compact for Safe, Orderly and Regular Migration (GCM) and the Global Compact on Refugees (GCR), which established cooperative standards for humane migration governance. Objectives 1 and 4 of the GCM concern accurate data and legal identity. Both compacts require

digital identity systems, data processing and border controls to respect human rights, procedural fairness and refugee protection.

UNHCR Data Protection Policy and Business Responsibility

In 2022, UNHCR adopted its *General Policy on Personal Data Protection and Privacy*, which established stringent rules concerning the privacy, security and consent requirements applicable to the personal and biometric data of refugees and asylum seekers. In addition, the United Nations Guiding Principles on Business and Human Rights (UNGPs), endorsed by the Human Rights Council in 2011, require business enterprises, including the private companies that design government migration systems, to exercise human rights due diligence so as to ensure that their products neither cause nor contribute to violations at borders.

CASE STUDIES

United Kingdom: The Visa Streaming Tool and IPIC

The Home Office of the United Kingdom employed a visa "streaming tool" that assigned applicants to red, amber or green (high, medium or low risk) categories, in part on the basis of nationality. Following legal challenges brought by the Joint Council for the Welfare of Immigrants (JCWI) and the digital rights organisation Foxglove, the Home Office withdrew the tool in August 2020. Critics argued that the use of nationality as a proxy for risk had embedded structural bias within the software.

In 2024, investigative reporting disclosed a further Home Office tool, IPIC (Identify and Prioritise Immigration Cases), which applies automated rules to recommend migrants for detention, bail conditions or removal, indicating the continued use of opaque enforcement algorithms.

United States: Virtual Borders, CBP One and the ICE Risk Classification Assessment

The United States employs smart sensors, automatic licence-plate readers, AI-enabled drones and predictive data analysis along its southern border. Human rights organisations contend that these systems target particular ethnic and

national groups and substitute algorithmic profiling for individualised asylum assessment.

CBP One application: asylum seekers were required to schedule appointments through the application, which was widely reported to experience difficulties with facial recognition for individuals with darker skin tones and to exclude users on account of inadequate internet access and server failures.

ICE Risk Classification Assessment (RCA): in 2018, reporting revealed that Immigration and Customs Enforcement had modified its automated tool for determining whether a detained migrant should be held or released on bond. Officials removed the option to recommend release, with the result that the tool almost invariably recommended detention. The case demonstrates that human-in-the-loop safeguards may be overridden in pursuit of political objectives.

European Union: Interoperability, Eurodac, ETIAS and Frontex

The European Union is interconnecting its large-scale databases (interoperability) and exploring the use of machine learning to pre-screen applications deemed suspicious. Legal scholars have cautioned that automated "hits" across databases shift the burden of proof onto asylum seekers, who must demonstrate an error without knowledge of how the system operates.

Eurodac: established in 2003 to record where asylum claims are lodged, Eurodac was modernised on 12 June 2026. It now records asylum seekers, resettled persons, irregular border crossers and persons staying irregularly. It stores facial images and fingerprints from the age of six, together with names, dates of birth, nationalities, travel documents and security flags. Police authorities and Europol have access to the system. Data is retained for ten years in respect of asylum seekers and for five years in respect of irregular entrants and resettled persons.

ETIAS: scheduled to commence operation in the last quarter of 2026, ETIAS will require travellers from more than 60 visa-exempt countries, including the United States, Canada, the United Kingdom, Australia and New Zealand, to apply online before travelling to 30 European countries. Authorisation costs €20 (with exemptions for persons under 18 and over 70), remains valid for up to three years and permits stays of up to 90 days within any 180-day period. Most applications are processed automatically within minutes, while complex cases are referred to

national units for manual review of up to 30 days. A twelve-month transition period will follow the launch.

Concerns: critics argue that, through the interoperability framework administered by the EU agency eu-LISA, the European Union has constructed a permanent biometric surveillance system directed exclusively at non-EU nationals, thereby undermining the data protection principle of purpose limitation, according to which data may be used only for the purpose for which it was collected.

Frontex: the European Border and Coast Guard Agency, which manages the external borders of the European Union, has been subject to scrutiny regarding the sharing of information with Libyan authorities in the course of Mediterranean rescue operations.

Greece: Surveillance in Reception Centres

From 2020, Greece constructed new "closed controlled access centres" for asylum seekers on its islands with funding from the European Union. These centres employ the surveillance systems Centaur, which uses cameras, drones and motion analysis to monitor the centres, and Hyperion, which regulates entry and exit by means of biometric verification. Human rights organisations argued that these systems transformed reception centres into carceral environments and were introduced without adequate assessment of their privacy implications. In 2024, the Hellenic Data Protection Authority fined the Greek Ministry of Migration and Asylum €175,000, having found that it had failed to conduct an adequate data protection impact assessment and to satisfy transparency requirements prior to deploying the systems.

iBorderCtrl: Automated Deception Detection at the Border

iBorderCtrl was a research project funded under the European Union's Horizon 2020 programme and tested between 2016 and 2019 at borders in Hungary, Latvia and Greece. Travellers responded to questions posed by a computer-generated border official displayed on a screen, while the system analysed micro-expressions in their faces in order to estimate whether they were being deceptive. Travellers assessed as presenting a risk were to be subjected to additional checks.

Scientists and human rights organisations strongly criticised the project on the ground that no reliable scientific evidence demonstrates that facial movements

indicate deception, particularly among persons who are under stress, traumatised or from differing cultural backgrounds. A Member of the European Parliament brought legal proceedings to obtain documents concerning the ethics and legality of the project, and the case raised broader questions regarding secrecy in publicly funded border research. The system was not adopted for general use.

Rohingya Refugees: Data Shared with Myanmar (2021)

In 2021, Human Rights Watch reported that UNHCR had collected biometric data, including iris scans and fingerprints, from Rohingya refugees in Bangladesh for the purpose of issuing the identity cards required for access to assistance. The data was shared with the Government of Bangladesh, which transmitted it to Myanmar for the verification of eligibility for potential repatriation, reportedly without the informed consent of the refugees concerned.

Afghanistan: Seizure of Biometric Devices by the Taliban (2021)

Following the withdrawal of Western forces in August 2021, the Taliban seized United States military HIIDE devices (Handheld Interagency Identity Detection Equipment). These devices contained the fingerprints, iris scans and personal details of Afghan nationals who had worked with allied forces. The case illustrates the capacity of biometric databases constructed for security purposes to be turned against vulnerable persons by hostile authorities.

Germany: Mobile Telephone Data Extraction and Dialect Recognition

Since 2017, the Federal Office for Migration and Refugees (BAMF) of Germany has employed dialect recognition software and the extraction of data from mobile telephones to verify the identity of undocumented asylum seekers. In February 2023, the Federal Administrative Court held that the routine extraction of telephone data by BAMF was unlawful, thereby confirming that the right to privacy extends to non-citizens and that digital searches must be proportionate.

Netherlands: Discriminatory Visa Profiling (2023)

In 2023, investigations disclosed that the Ministry of Foreign Affairs of the Netherlands had employed an algorithm that profiled short-stay visa applicants on

the basis of nationality, age and gender, assigning applicants from certain countries of the Global South to high-risk processing tracks. The Dutch Data Protection Authority and subsequent reviews found that the use of factors such as nationality or origin constituted unlawful discrimination.

Canada: The Chinook System

Immigration, Refugees and Citizenship Canada (IRCC) introduced automated triage tools, most notably Chinook, to expedite the processing of study permits, visitor visas and temporary residence applications. The Citizen Lab report *Bots at the Gate* (2018) had previously drawn attention to the risks of automated decision-making within the Canadian immigration system. Critics contend that Chinook introduces an unscrutinised layer of risk profiling, limits judicial review and may contribute to high refusal rates, without adequate reasons, for applicants from certain developing countries.

UNHCR Biometric Matching

UNHCR and its humanitarian partners employ AI-assisted biometric matching for the registration and management of displaced populations. Although this practice accelerates the delivery of assistance and the verification of identity, centralised databases create risks of disclosure to repressive governments, and refugees may be excluded entirely where the system fails to match their biometric data.

Private Vendors and Procurement

Governments rely upon private companies, including Palantir, IDEMIA and Thales, for the development of border algorithms and biometric systems. Because these systems are commercial products, governments frequently invoke trade secrecy to withhold source code and training data from courts, auditors and the public. This arrangement permits companies to profit from border surveillance while avoiding responsibility for resulting human rights harms.

QUESTIONS A RESOLUTION MUST ANSWER (QARMA)

1. How can international frameworks require transparency and human-in-the-loop oversight for automated decision-making and risk assessment at borders?

2. What mechanisms should be established to audit and correct bias in training data so as to prevent discrimination against particular nationalities, ethnic groups or vulnerable persons?
3. In what ways do AI systems create, reproduce or amplify discrimination in immigration and asylum procedures, and what measures may governments and international organisations adopt to prevent it?
4. How can states ensure that predictive border technologies respect the principle of non-refoulement and the right to seek asylum?
5. What rights of appeal and remedies should migrants possess to challenge automated decisions and to understand the basis of opaque outcomes?
6. Should experimental technologies, such as emotion recognition, deception detection and dialect recognition, be subject to a global moratorium until their compliance with human rights standards has been demonstrated?
7. How should states regulate the sharing of migrants' data with countries of origin and third states?
8. What obligations should apply to the private companies that design and supply these systems?
9. How can developing states be assisted in assessing and auditing imported border technology?
10. For what period may migrants' biometric data be retained, and what should become of it once protection or status has been granted?
11. How can states ensure that persons without smartphones, internet access or digital literacy are not excluded from asylum procedures?
12. What specific safeguards are required for children, LGBTQI+ applicants, persons with disabilities and stateless persons?
13. How can national security exemptions be circumscribed so as to prevent their use as a means of circumventing human rights protections?
14. What role should UNHCR, OHCHR and other United Nations bodies play in monitoring the use of border technology?

BIBLIOGRAPHY

Agenda A: Biocolonialism and Indigenous Data Sovereignty

United Nations and Human Rights

United Nations (2007) *United Nations Declaration on the Rights of Indigenous Peoples*. Available at: <https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html>

UN Expert Mechanism on the Rights of Indigenous Peoples (2025) *Right of Indigenous Peoples to Data, Including with Regard to Data Collection and Disaggregation*, A/HRC/60/66. Available at: <https://docs.un.org/en/A/HRC/60/66>

United Nations, Department of Economic and Social Affairs. *Indigenous Peoples, Data and Indicators*. Background resource.

Biodiversity and Benefit-Sharing

Convention on Biological Diversity (1992) *Text of the Convention*. Available at: <https://www.cbd.int/convention/text>

Convention on Biological Diversity (2010) *Nagoya Protocol on Access and Benefit-Sharing*. Available at: <https://www.cbd.int/abs>

Nagoya Protocol, Article 12: *Traditional Knowledge Associated with Genetic Resources*.

Convention on Biological Diversity (2024) *Cali Fund for the fair and equitable sharing of benefits from the use of digital sequence information*. Available at: <https://www.cbd.int/dsi-gr>

Indigenous Data Governance

Global Indigenous Data Alliance (2019) *CARE Principles for Indigenous Data Governance*. Available at: <https://www.gida-global.org/care>

First Nations Information Governance Centre. *The First Nations Principles of OCAP®*. Available at: <https://fnigc.ca/ocap-training/>

First Nations Information Governance Centre. *OCAP® Research Library*.

South African San Council (2017) *San Code of Research Ethics*.

Te Mana Raraunga, Māori Data Sovereignty Network. Available at: <https://www.temanararaunga.maori.nz>

Maiam nayri Wingara, Indigenous Data Sovereignty Collective. Available at: <https://www.maiamnayriwingara.org>

Research Ethics and Case Studies

- Mello, M.M. and Wolf, L.E. (2010) "The Havasupai Indian Tribe Case: Lessons for Research Involving Stored Biologic Samples", *New England Journal of Medicine*, 363(3), pp. 204–207.
- Garrison, N.A. (2013) "Genomic Justice for Native Americans: Impact of the Havasupai Case on Genetic Research", *Science, Technology, & Human Values*, 38(2).
- UNESCO (1997) *Universal Declaration on the Human Genome and Human Rights*. Available at: <https://www.unesco.org/en/legal-affairs/universal-declaration-human-genome-and-human-rights>
- UNESCO (2003) *International Declaration on Human Genetic Data*. Available at: <https://www.unesco.org/en/legal-affairs/international-declaration-human-genetic-data>

Health Research and Current Guidance

- World Health Organization (2026) *Participatory Framework for Respectful Engagement with Indigenous Peoples on Biodiversity, Health and Traditional Knowledge Systems* (unedited final draft).
- National Human Genome Research Institute. *Informed Consent for Genomics Research*. Available at: <https://www.genome.gov>

Agenda B: Algorithmic Discrimination in Immigration and Asylum Systems

- Abomhara, M. et al. (2022) "How to do it right: A framework for biometrics supported border control", *arXiv [cs.CY]*. Available at: <https://doi.org/10.48550/arXiv.2201.03407>
- Behrendt, H. and Loh, W. (2022) "Informed consent and algorithmic discrimination – is giving away your data the new vulnerable?", *Review of Social Economy*, 80(1), pp. 58–84. Available at: <https://doi.org/10.1080/00346764.2022.2027506>
- Buolamwini, J. and Gebru, T. (2018) "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research*, 81, pp. 77–91.
- Chatham House (2022) *Refugee Protection in the Artificial Intelligence Era: Challenges in Meeting International Legal Obligations*. Available at: <https://www.chathamhouse.org/2022/09/refugee-protection-artificial-intelligence-era/3-challenges-meeting-international-legal>
- Citizen Lab (2018) *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*. Available at: <https://citizenlab.ca/research/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/>

- Delioglu, F. (2025) *Technology at the Borders: Surveillance, Control and Resistance in EU Migration Governance*, Balsillie Papers. Available at: <https://balsilliepapers.ca/bsia-paper/technology-at-the-borders-surveillance-control-and-resistance-in-eu-migration-governance/>
- European Digital Rights (EDRi) (2026) *Your Data, Their Decision: The Hidden Surveillance Infrastructure Behind Europe's Digital Borders*. Available at: <https://edri.org/our-work/your-data-their-decision-the-hidden-surveillance-infrastructure-behind-europes-digital-borders/>
- European Parliamentary Research Service (2025) *Artificial Intelligence in Asylum Procedures in the EU*. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)775861](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775861)
- Grother, P., Ngan, M. and Hanaoka, K. (2019) *Face Recognition Vendor Test Part 3: Demographic Effects*, NISTIR 8280. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.IR.8280>
- Hertz, M.E., Byrne, W.H. and Gammeltoft-Hansen, T. (2025) "What 'real risk' means for AI-assisted Refugee Status Determination", *Verfassungsblog*. Available at: <https://doi.org/10.59704/65e66bd895af5c3b>
- Jesuit Refugee Service (2026) *Excluded by an Algorithm: Technological Discrimination in Migration Systems*. Available at: <https://www.sjesjesuits.global/2026/07/17/excluded-by-an-algorithm-technological-discrimination-in-migration-systems/>
- Joel, A. (2023) "Trusted cross-border data flows: A national security priority", *Lawfare*. Available at: <https://www.lawfaremedia.org/article/trusted-cross-border-data-flows-a-national-security-priority>
- Laupman, C., Schippers, L.-M. and Papaléo Gagliardi, M. (2022) "Biased algorithms and the discrimination upon immigration policy", in *Law and Artificial Intelligence*. The Hague: T.M.C. Asser Press, pp. 187–204.
- Meier, A. (2026) *Algorithmic Migration*. Stiftung Wissenschaft und Politik (SWP).
- Memon, A. et al. (2024) "Artificial Intelligence (AI) in the asylum system", *Medicine, Science and the Law*, 64(2), pp. 87–90. Available at: <https://doi.org/10.1177/00258024241227721>
- Mixed Migration Centre (2025) *AI, Surveillance and the Privatisation of Migration Management*. Available at: <https://mixedmigration.org/publications/mmr/2025/ai-surveillance-privatised-migration-management/>
- Nalbandian, L. (2022) "An eye for an 'I': a critical assessment of artificial intelligence tools in migration and asylum management", *Comparative Migration Studies*, 10(1), p. 32. Available at: <https://doi.org/10.1186/s40878-022-00305-0>

OHCHR. *The Right to Privacy in the Digital Age: Reports*. Available at:
<https://www.ohchr.org/en/privacy-in-the-digital-age/reports>

OHCHR (2021) *A/HRC/48/76: Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement*. Available at:
<https://www.ohchr.org/en/documents/thematic-reports/ahrc4876-racial-and-xenophobic-discrimination-and-use-digital>

United Nations Human Rights Council (2020) *A/HRC/44/57: Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis*. Available at:
<https://docs.un.org/en/A/HRC/44/57>

United Nations Office at Geneva (2021) *Special Rapporteur on Contemporary Forms of Racism Calls for a Moratorium on the Use of Surveillance Technology in the Immigration Enforcement Context*. Available at: <https://www.ungeneva.org/en/news-media/meeting-summary/2021/10/la-rapporteuse-speciale-sur-les-formes-contemporaines-de-racisme>

United Nations. *General Assembly Third Committee: Social, Humanitarian & Cultural*. Available at: <https://www.un.org/en/ga/third/index.shtml>

Refugee Survey Quarterly (Oxford Academic). Available at:
<https://academic.oup.com/rsq/article/43/4/410/7824359>

Societies (MDPI) (2023), 13(6), 149. Available at: <https://www.mdpi.com/2075-4698/13/6/149>

SIT Digital Collections. Available at:
<https://digitalcollections.sit.edu/cgi/viewcontent.cgi?article=1010&context=szg2>