GENEVA GRADUATE INSTITUTE

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

Leveraging the Integration of Artificial Intelligence (AI) into Border Management Systems

A Best Practices Report

Graduate Institute of International and Development Studies (IHEID)

in partnership with

the International Organization for Migration (IOM)

Francesca Diaz, Georgia Ross, Tamiliniyaa Rangarajan, Wael Frikha

May 16, 2025

TABLE OF CONTENTS

TABLE OF ACRONYMS

Acronym	Term	Definition
CBSA	Canada Border Services Agency	Facilitates the flow of legitimate travellers and trade. The agency also enforces more than 100 acts and regulations for Canada.[1]
EES	Entry/Exit System	Scheduled to be implemented in October 2025, the European Union's EES aims to modernize border control, improve security within the Schengen area and increase the efficiency of border checks by automating numerous border control procedures, in order to cope with the increasing number of travellers.[2]
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice	Manages the European Union's large-scale IT systems used for border management, migration, and law enforcement to ensure seamless data sharing and interoperability.[3]
FRONTEX	European Border and Coast Guard Agency	Agency which coordinates border management efforts across the European Union, ensuring the security of external borders while supporting Member States during crises.[4]
ITU	International Telecommunication Union	A specialized agency of the United Nations responsible for issues related to information and communication technologies, including setting global standards.[5]
SIS	Schengen Information System	Centralized database used by Schengen Area countries and European Union agencies. Aims to enhance security and facilitate the movement of people by enabling information sharing among national border control, law enforcement, and judicial authorities.[6]
GDPR	General Data Protection Regulation	The European Union's data privacy and security law adopted in 2016. The legislation includes an explainability clause which outlines an individual's right to an explanation of how a decision was rendered from automated processes. [7]

Table 1: List of acronyms. Adapted from sources in footnotes.

[1] Canada Border Services Agency, 2025.
[2] European Commission, 2024a.
[3] eu-LISA, 2024.
[4] European Union, 2024.
[5] International Telecommunication Union, 2025.
[6] European Commission, 2024b.
[7] GDPR, Regulation (EU) 2016/679.

GLOSSARY

Term	Definition
Advanced Passenger Information Systems (API)	Refers to the infrastructure used by governments or transport operators to collect and manage passenger data before their arrival or departure.[8]
Algorithms	Sets of machine instructions designed to process information and solve problems. AI algorithms are capable of analysing data, identifying patterns, drawing inferences and predicting behaviour with speed and accuracy far beyond human ability.[9]
Artificial Intelligence	Technology that allows machines and computers to mimic human abilities such as learning, understanding, solving problems, making decisions, being creative, and functioning independently.[10]
Automated Border Control system (eGates)	Automated systems used at border control points to process travellers more efficiently. They utilize biometric verification – typically facial recognition or fingerprinting – alongside data from passports or travel documents to authenticate a person's identity.[11]
Big Data	Refers to massive complex datasets that traditional data systems cannot handle. This involves the rapid influx of a large volume of information from diverse sources. Big data is integral to AI training and effectiveness.[12]
Black Box AI	This refers to AI trained with techniques such as deep learning that involve massive datasets and relies on complex statistical patterns rather than explicitly stated conditions. They are called black boxes because their decision making logic is not interpretable for humans without tools. The user can see the system's input and output, but not the decision making process in between.[13]
Convolutional Neural Networks (CNN)	A type of deep learning algorithm specifically designed to process data with a grid-like structure, like images. Specifically used in deep learning methods for facial recognition technologies.[14]
Datafication	Datafication refers to the quantification of human life through digital information, often for extracting economic value. Information is put into a quantified form for tabulation and analysis.[15]
Deep Learning	An extension of machine learning which stimulates human-like decision making. Deep learning systems are able to effectively carry out procedures involving image and facial recognition by using multi-layered algorithms.[16] These systems, in turn, are able to learn from the data and make independent judgments, rendering the outcomes more flexible than machine learning. Although this learning mechanism offers significant capabilities, it poses transparency issues, as its decision making process is not always readily explainable.[17]
Explainable AI (XAI)	Explainable AI is a set of processes and methods that allow humans to better interpret an AI's outcomes and logic, making the decision making process more transparent. It can refer to (a)

[8] Dumbrava, 2021.
[9] Beduschi and McAuliffe, 2021.
[10] IBM, 2024.
[11] European Commission, 2020.
[12] Badman., Kosinski, 2024.
[13] Kosinski, 2024.
[14] IBM, 2025.
[15] Mayer-Schönberger and Cukier, 2013; Mejias and Couldry, 2019.
[16] Beduschi and McAuliffe, 2021.
[17] Ibid.

	AI models trained with techniques that operate using predefined, human readable logic that follows explicitly stated conditions (for instance, *if a passenger is travelling with expired documentation, flag to a border official)*, or (b) a set of methods that allow one to interpret black box AI decisions after the system has been trained. The user can see the input, output and the decision making process in between.[18]
Human-in-the-Loop (HITL)	Human-in-the-loop is a human oversight mechanism that requires a human actor to guide and validate every decision cycle that an AI-integrated system goes through, before it can be implemented.[19] Human feedback directly flows into the optimization of the AI model making it particularly effective.[20]
Human Oversight	Human oversight has emerged as a critical AI governance mechanism tasked with enhancing system accuracy and safety, upholding human values and fostering trust in the technology, through channels of human-AI collaboration.[21]
Information Communication Technology (ICT)	Covers all technical means used to handle information and aid communication. This includes both computer and network hardware, as well as their software.[22]
Machine Learning	A branch of AI which focuses on enabling computers and machines to imitate the way humans learn, to perform tasks autonomously and improve performance and accuracy through exposure to more data. Involves training algorithms to recognize patterns and make data-driven decisions. As a result, they are able to learn from and make inferences based on data, without needing to be programmed for specific tasks.[23]
Operational Data	Operational data reflects the current state of an organization, company or any other entity, and is used to manage and support day-to-day operations.[24]
Pause Scenario	A built-in failsafe procedure that allows an AI system to be temporarily halted without interrupting broader operations. THis mechanism is particularly critical in environments like airports, where systems may need regular maintenance or could experience failure.[25]
Shapley Additive Explanation (SHAP)	An explainable AI method that allows a human to interpret the decision of an AI-powered facial recognition technology trained with deep learning methods. SHAP provides a heatmap over the photo of an individual and highlights areas argued for the prediction, versus areas that argued against the prediction.[26]
Sociotechnical	Refers to the practice of incorporating both technical and social elements in systems design, keeping into consideration the system's capacity to not only be shaped by society, but also to impact it.[27]
Training Data	Refers to a set of labelled information that is used to build a machine learning model. This data can include annotated text, images, audio, or video. Through training data, AI systems are able to perform tasks at a high level of accuracy.[28]

Table 2: Definitions of key concepts. Adapted from sources in footnotes.

[18] Dwivedi et al.,, 2023; Holzinger et al., 2020.
[19] Fink, 2025.
[20] Holzinger et al., 2025.
[21] Ibid.
[22] Eurostat, 2023.
[23] IBM, 2021.
[24] Hobbs et al., 2005
[25] Adapted from an interview with CBSA.
[26] Malik et al., 2021.
[27] Mumford, 2000.
[28] TELUS Digital, 2025.

EXECUTIVE SUMMARY

According to the International Organization for Migration's (IOM) 2024 World Migration Report, there are approximately 281 million international migrants worldwide.[29] Meanwhile in the space of tourism, the United Nations recorded an approximated 1.4 billion international tourists in 2024 alone.[30] This massive scale of cross-border movement – driven by migration, tourism, commerce and crisis response alike – presents both immense opportunities and challenges for border management systems worldwide. As states strive to balance mobility, security and the protection of human rights, border agencies are increasingly turning to advanced technologies, particularly artificial intelligence (AI), to manage increasing flows with greater efficiency and accuracy.

The integration of AI into border systems offers many opportunities to enhance operational procedures such as travel document and identity verification, decision-making support and risk profiling. However, the deployment of AI must be approached with caution, by ensuring that it aligns with international legal standards, ethical norms and operational realities. Existing literature raises concerns in the sphere of algorithmic biases, data quality and privacy.[31] With this duality in mind, this report outlines best practices for the responsible use of AI in border management.

Drawing on expert insights in the fields of border management, human rights law, digital governance and AI, these recommendations aim to guide IOM Member States and stakeholders on essential operational and ethical considerations as they leverage the implementation of AI into their border management systems. Moreover, it aims to highlight the importance of ensuring that these systems are designed not only efficiently, but also transparently with respect to human rights frameworks.

[29] McAuliffe and Oucho, 2024.

[30] UN Tourism, 2024.

[31] Burrell, 2016; Ntoutsi et al., 2021.

1. General Applications of AI in Migration and Border Management

1.1. Functions and Capabilities

Artificial Intelligence (AI) refers to technologies that allow machines to perform tasks that typically require human intelligence – such as pattern recognition, data analysis and decision-making.[32] The origins of AI can be traced back to the ambitions to simulate human reasoning, all the way back in the 1950s. Today, the term general AI broadly refers to technology that allows machines to simulate human reasoning, comprehension, problem solving, decision making, creativity and autonomy. Narrow AI systems, on the other hand, are specifically designed to handle defined tasks such as facial recognition and content generation.[33] The International Telecommunication Union (ITU) recognizes the technology's ability to efficiently analyse vast amounts of data, identify trends, automate routine tasks and offer real-time analytical insights.[34] These abilities render AI an invaluable tool in incorporating cognitive automation into and enhance various sectors such as finance, healthcare and policing.[35] It has been particularly effective at handling repetitive and time consuming tasks by processing large datasets at speeds far beyond human capacity.[36]

With the IOM estimating that mobility patterns have increased over the last five decades – prompting the need for service adaptation – AI integration emerges as a powerful tool.[37] As a result, stakeholders are considering the integration of the technology into various stages of the migration cycle, including pre-departure, entry, stay and return.[38] In the pre-departure phase for instance, e-visa systems utilize machine learning techniques to automate routine applications and reduce processing times. For instance, AI-driven chatbots have been noted for their capacity to provide legal advice and psychological support to new migrants.[39] Automated border control systems (e-gates) at points of entry, on the other hand, can utilize AI with biometric data to streamline identity verification and security checks at land, air and sea crossings.[40]

The analytical capabilities of machine and deep learning allows AI systems to predict labels for new and unseen data; As a result, several countries are investing in AI technologies to predict migratory movements, optimize resource allocation and manage challenges.[41] Although AI is capable of mitigating human errors, the technology is also prone to its own

[32] Beduschi and McAuliffe, 2021.
[33] Ibid.
[34] International Telecommunication Union, 2024.
[35] Beduschi and McAuliffe, 2021; United Nations System 2024b.
[36] Beduschi and McAuliffe, 2021.
[37] IOM, 2024.
[38] Beduschi and McAuliffe, 2021.
[39] Ibid.
[40] Ibid.
[41] Ibid.

set of shortcomings. Biased system designs and the subsequent algorithmic discrimination they facilitate, for instance, pose concerns about integrating AI into existing systems.[42]

Keeping these challenges in mind, this report will explore the opportunities for leveraging the implementation of AI in border management systems.

1.2 AI in Border Security and Management

AI's ability to analyse large-scale datasets, detect patterns and draw inferences from a variety of sources, including travel records, biometric data and documentation, shows potential for its integration in border management. Experts have increasingly commented on AI systems' capacity to detect potential security threats and assist in decision processes at official points of entry with greater precision and speed. Additionally, AI not only enhances security but can also help manage migration flows, allowing authorities to make data-driven decisions that balance efficiency with safety. Meanwhile on the management end, AI tools provide risk assessment support to authorities, which some have argued can decrease burden on individual border guards during the decision making process.[43]

From an economic standpoint, incorporation of AI in border checks can also result in more effective resource allocation at borders by balancing staffing needs among authorities and reducing inconsistencies associated with under or overstaffing.[44] Furthermore, AI's integration into border management systems offers the opportunity to improve situational awareness, allowing border officials to continuously monitor real-time data and respond proactively to emerging threats or changes in the operational environment.[45]

For instance, AI is becoming increasingly integrated into Advanced Passenger Information (API) systems to improve efficiency of passenger processing and aid in risk assessment. API systems refer to the infrastructure used by governments or transport operators to collect and manage passenger data before their arrival or departure.[46] Integral to the work of border and migration authorities, these systems identify potential risks by cross-checking passenger information – such as biographical data, travel documents and flight details – with security databases before arrival.[47] Traditional API systems that predate the integration of AI rely on predefined rules and criteria for risk assessment that often necessitates manual document checking and limits the system's ability to analyze data in real-time. Integrating AI into API systems introduces machine learning capabilities, enabling continuous updates to risk models to handle new and evolving threats. This advancement reduces reliance on manual processes, which can in turn enhance the overall efficiency of border management systems.[48]

---

[42] Molnar and Gill., 2018.

[43] European Commission: Directorate-General for Migration and Home Affairs, 2020; Frontex, 2021.

[44] Ibid.

[45] International Telecommunication Union, 2024.

[46] Dumbrava, 2021.

[47] Beduschi and McAuliffe, 2021; Vavoula and Mitsilegas, 2022.

[48] Beduschi and McAuliffe, 2021.

The leveraging of AI to enhance efficiency of information systems like API have immense opportunity in the context of interoperability between distinct databases related to border management and migration processes. Broadly, interoperability refers to the ability of different databases, technologies or organizations to communicate and exchange data securely and seamlessly, ensuring that data from diverse sources can be shared, integrated and processed without compatibility issues.[49] In the border management context, interoperability often involves the integration of transport, security and criminal databases either at a national or regional level. At the national level, this might include systems at airports communicating with security or criminal databases, enabling customs officials to crosscheck traveller information against criminal records and national watchlists (see figure 2).[50] Meanwhile at the regional level, as in the European Union, interoperability takes the form of integrating national border management and security databases with those of EU agencies. This creates centralized, large-scale IT systems accessible to all member states, allowing for unified data sharing and coordinated decision-making across the region (see figure 3).[51]

Example of Interoperability in a national context: Australia's 'SmartGates'

Australia's 'Smart Gates' system is an automated border control point at airports that uses AI-powered facial recognition technology (FRT) to verify a traveller's identity against the information in their and biometric passport (passports with a microchip that contains an individual's personal details including photograph and fingerprints). The eGate scanner reads all the information contained in the chip inside the passport and runs the data against numerous databases to determine if the traveller is a security risk and must be flagged to a border official. In this case, interoperability is present in the communication of Australian airport, security and criminal databases. The seamless communication between each of these databases ensures that traveller information can be effectively cross-checked with national watchlists or criminal records before entry.

Figure 2: Example of interoperability in a national context. Adapted from Australian Border Force (n.d.). *SmartGates,* 2025; Australian Department of Home Affairs, 2024.

[49] Andreou, 2023; Dumbrava, 2021.

[50] Papademitiou and Collette, 2011.

[51] Andreou, 2023; Dumbrava, 2021; Frontex, 2021.

Example of Interoperability in a regional context: The Schengen Information System (SIS)

In the European Union context, interoperability is carried out by eu-LISA (see table 1 for full name), the EU agency responsible for building necessary technical infrastructure in the domain of security and border management. Eu-LISA manages large-scale IT systems like the Schengen Information System (SIS), a centralized database utilized by EU member-states and Frontex to enhance security and facilitate the movement of people in the Schengen Area. By enabling information sharing among national border control, law enforcement and judicial authorities, the SIS issues alerts to border authorities on persons of interest, missing persons and entry-bans for non European-nationals. Eu-LISA is currently exploring the incorporation of advanced AI technologies (i.e. knowledge management tools and risk assessment algorithms) into the SIS that aim to process real-time data and alerts more efficiently and at higher volumes, thus accelerating response times and operational accuracy.

For instance: if a border official receives an alert about a person flagged in the SIS for using forged identity documents, the officer would manually have to cross-check the alert details with other databases, and verify biometric data manually against stored records. However, an AI-integrated SIS system would instead automate the act of cross-referencing across connected databases in real-time and consolidate relevant information, thus creating a quicker and more efficient decision-making process for the officer.

Figure 3: Example of interoperability at the regional level, adapted from Dumbrava 2021; European Commission: Directorate-General for Migration and Home Affairs, 2020; eu-LISA, 2020.

Additionally, AI harnesses the potential to play an important role in improving biometric identification technologies which verify traveller identity at official points of entry. While biometric technologies like facial recognition and fingerprinting predate the advent of AI, deep learning techniques augment the functionality of biometric capturing devices by facilitating more adaptive decision-making with reduced risk of errors (see table 2).[52]

Facial Recognition without AI (manual methods)	Facial Recognition with AI (deep learning methods)
Relied on manual feature extraction and simple image processing techniques.	Utilizes convolutional neural networks (CNNs) to learn and identify complex patterns automatically across massive datasets.
Identified an individual by using predefined landmarks (i.e. distance between eyes or jawline shape) that were programmed by a human into the technology.	Identifies an individual through a multilayered algorithm (CNNs) that can detect patterns of the face without following programmed, predefined conditions.
Struggled with variations in facial expressions, aging, makeup, camera angles, or lighting.	Offers high precision and flexibility in detection and matching across conditions and demographics (i.e. low lighting, crowded areas, facial movement).
Functional in controlled environments (consistent lighting, frontal angles). Accuracy dropped significantly in real-world settings.	Can identify a face in real-time. Enables widespread use in real-world settings, such as border management, surveillance, and smartphone authentication.
Could not learn from new data, leading to rigidity and difficulty to improve over time.	Continuously improves performance overtime with more training data.

Table 2: Adapted from Balaban, 2015 and Fuad et al., 2021.

[52] Awad, et al., 2024; Balaban, 2015.

Due to the flexibility of deep learning techniques, AI-powered technologies can cross-check travellers' identities against existing records with greater speed.[53] Consequently, this can streamline border processing on both the traveller and receiving end. For border officials, this can reduce burden on border personnel at checkpoints and allow quicker processing of high volumes of travellers. Meanwhile for travellers, this can reduce waiting and response times at checkpoints, thus improving traveller experience (see example in figure 4).[54]

Example of AI-integrated Biometric Technologies at National Points of Entry: Australia's 'Smart Gates'

Australia's 'Smart Gates' system is an automated border control point at airport arrivals that uses AI-powered facial recognition technology (FRT) and biometric passports (passports with a microchip that contains an individual's personal details including photograph and fingerprints) to confirm a traveller's identity. If the FRT successfully matches the traveller to their biometric passport, they can proceed through the gate without a check from a customs officer. Though if the FRT fails to confirm the traveller's identity, they must then go to manual passport control to be further checked by an officer. 'Smart Gates' are currently implemented at all of Australia's eight major international airports inlcuding Melbourne and Sydney.

Figure 4: Example of AI-powered biometric technologies at official points of entry, adapted from Australian Border Force (n.d.). *SmartGates,* 2025; Australian Department of Home Affairs, 2024.

Despite the potential for AI systems to enhance management processes at official points of entry, it is essential to recognize that technologies must work in tandem with human oversight. AI should not replace the border official's agency to admit an individual, it simply ought to make their work easier. Governments need to remain fully responsible for the outcomes of automated processes, and human oversight is critical to ensure that decisions remain transparent, equitable and free from algorithmic bias. Ethical and effective implementation requires that AI be treated as a tool to support – not replace – human judgement in high-stakes border decisions.[55]

2. Ethical Considerations and Regulatory Challenges

2.1. Black Boxes and Biases

It is important to keep in mind that the integration of AI into border management can be accompanied by the creation of 'black boxes.' [56] Broadly, these black boxes refer to the fact that although an observer may have access to the inputs and outputs of an AI-powered system, there is no way of explaining how the transformation has occurred – that is, the functioning of the algorithm.[57] This is often, as discussed earlier, an uncontrolled

[53] Andreou, 2023; Beduschi and McAuliffe, 2021.
[54] Ibid.
[55] Ibid.
[56] Nalbandian, 2022; Kosinski, 2024.
[57] Nalbandian, 2022.

consequence of exponential growth associated with deep learning models. In the context of border management, black boxes and deep learning models most commonly arise in facial recognition technology.[58] However, the opacity of the algorithm can also be intentionally created through a combination of commercial motives and intellectual property rights.[59] As a result, its components like the training data set or the source code, can be inadvertently or deliberately obscured. This complicates the matter of reviewing AI-integrated systems for any biases they may internalize.

Drawing from Safia Umoja Noble's argument that 'algorithms of oppression' manipulate search engine results, similarly if left unchecked, covertly or overtly discriminatory AI systems can unfairly influence key migration decisions like risk assessments or entry permits.[60]

Understanding how an algorithm is created

The first step to creating any algorithm is to create a 'training set.' The training set refers to the entirety of the data from which the model is expected to learn. To determine whether an algorithm has been successful or not, it is considered important to define and establish the 'target variable.' The target variable refers to the things that the algorithm will actually predict. The process of defining such variables requires programmers to take part in 'feature selection', a process through which they decide what criteria will be prioritized to rank, sort and score.

For instance: In the example of facial recognition technology, the 'target variable' for the technology is to match a person's face to their passport photo. The 'feature selection' refers to the selection of facial features that will determine the technology's prediction

Figure 5: Understanding how algorithms are built, adapted from Noble, 2018.

The Citizen Lab at the Munk School of Global Affairs and Public Policy notes that the biases of an individual designing the system or the shortcomings of the training data itself, can be compounded to produce exclusionary outputs.[61] Discrimination can be produced covertly too. The Centre for Democracy and Technology, for instance, indicates that the most harmful algorithms are the ones that rely on statistically significant ways to sort people, often unintentionally, to deny or target historically marginalized groups.[62] The fallibility of commercially available training datasets is reflected in the study analysing the gender classification products of three different companies, IBM, Google and Face++.[63] Although the study concluded that these products managed to assign the correct gender to a face with a high overall accuracy, the error rate varied greatly between different social groups. All three companies performed better on light-skinned individuals.

[58] Garcia et al., 2019; Wehrli et al., 2022.
[59] Burrell, 2016.
[60] Noble, 2018.
[61] Molnar and Gill., 2018.
[62] Centre for Democracy and Technology, 2019.
[63] Buolamwani and Gebru, 2018.

The limitations of similar products must not only be attributed to conscious biases compounded by developers, but also to a lack of diversity in the data available to constitute the training set, hindering testing against parameters like gender, race or ethnicity. When the algorithms powering them learn and evolve at an exponential rate, it becomes too expensive to recall and correct their errors. Using biometric recognition software, whether or not fraught with such characteristics, to govern borders can inadvertently provide the opportunity to flag certain features as high risk and perpetuate discriminatory attitudes.[64] Such circumstances consciously influence the process of feature selection.

In the context of migration, this could mean overestimating the link between inputs like unstable credit scores and overstaying visits to the destination country. This would potentially function as a proxy to deny entry to applicants from low-income countries who might have valid reasons to visit. Using data that is one-dimensional and not representative of the factors that inform migration to streamline contemporary decision making will only intensify historical vulnerabilities.

2.2 Discussing Oppressive Consequences

If algorithms of oppression are not dealt with adequately, their impact can manifest in the form of violations on freedom of movement, right to privacy and adverse economic consequences. In theory, the Universal Declaration of Human Rights stipulates that everyone has the right to leave any country, including their own and to return to their country.[65] This right, however, is not absolute and works in tandem with national sovereignty. Several pieces of legislation worldwide guarantee different degrees of free movement for specific groups of people. All European Union citizens and their family members, for instance, are guaranteed the right to move and reside freely within the European Union as per the fundamental rights established in the Treaty on the Functioning of the European Union and Article 45 of the European Union Charter of Fundamental Rights.[66]

Apart from concerns of bias, the astronomical amounts of data that AI requires to train itself, raises questions about privacy. Integrating AI into the border management system necessitates the 'datafication' – or the systematization and analysis of data – of the entire migration cycle.[67] In the absence of an effective data collection strategy, storing large quantities of data to extract specific variables to identify a small subpopulation for later use, to run AI-integrated systems must comply with cybersecurity and personal data protection concerns.

Turning to the possibility of adverse economic consequences, there is widespread recognition that migration and development are interdependent processes. Diaspora migration strengthens their communities of origin through skills transfer, economic investment and development assistance. Migrants, notes the Global Forum on Migration and

[64] Molnar and Gill., 2018.

[65] Universal Declaration of Human Rights, Article 13, 1948.

[66] Treaty on the Functioning of the European Union, Article 21, 2008; Charter of Fundamental Rights of the European Union, Article 45, 2000.

[67] United Nations University, 2023; Beduschi, 2020.

Development, also support labour markets and fill skill gaps in their destination countries.[68] If safeguards are not developed to prevent AI-integrated systems from unfairly discriminating against aspiring migrants, it will create barriers to transnational job opportunities and hinder overall development.

2.3 Mutually Agreed Transparency and Good Practices

Achieving 'algorithmic transparency' to overcome these challenges is a complex matter. AI regulations, which are located at the intersection of legal-political concepts and computer science foundations, require the combined cooperation of national governments and private sector innovators, for their successful implementation.[69] For instance, some solutions proposed by policymakers, such as transparency, do not necessarily align with the functioning of deep learning models.[70] Some technologists, however, see regulations as stifling innovation.[71] For example, the European Union's General Data Protection Regulation includes an explainability clause that outlines an individual's right to an explanation from any algorithm driven, automated decision.[72] In this regard, it is important to consider explainable AI tools that ensure that technological innovation abides by legislations mandating transparency. This report will expand on this solution further in its best practices section. Apart from this disconnect, the relatively slow enactment of regulatory standards in comparison to rapid technological change, presents another puzzle.

It is evident that the process of integrating AI into governance systems, with all its challenges of transparency, bias and accountability, is no simple task. Its execution involves negotiating trade-offs between human rights, national security objectives and procedural efficiency to produce an ideal system. It is critical to review and account for these considerations as countries begin to integrate AI into their border management systems.

Desai and Kroll propose a 'trust but verify' approach to AI regulation, which requires the technology to be built in a way that allows for analysability and technical verification.[73] One way to realize this would be through the use of human oversight mechanisms. This will be discussed in the report's best practices section. On the path to legitimizing technology-powered governance, it is important to anchor human rights as a referential normative principle. Drawing from these, this report adopts an anthropocentric approach in discussing best practices to integrate AI in border management, where people must always be given the power to supervise machines, ensuring their dignity and autonomy.[74]

[68] Global Forum on Migration and Development, 2016.
[69] Kossow et al., 2021.
[70] Desai and Kroll, 2017.
[71] Ibid.
[72] GDPR, Regulation (EU) 2016/679.
[73] Desai and Kroll, 2017.
[74] European Commission; Directorate-General for Communications Network, 2018.

3. AI Governance and Regulation

3.1. Foundations of AI Governance

The 'AI governance paradox' describes how regulatory frameworks often lag behind technological advancements in AI.[75] Effective governance mechanisms are necessary before the deployment of AI systems, however the ability to govern only emerges after these systems exist and demonstrate their impact, posing challenges in regulating AI at national, regional and international levels.[76] On an international scale, issues of state autonomy, unaligned national interests, lack of legal enforceability, and state competition on technological innovation create a fragmented regulatory landscape for AI governance.[77] Such fragmentation poses questions on whether AI governance is most effective on a national level, or whether there is room for effective centralized governance at the global level.[78] Despite these challenges, notable advancements in global cooperation on AI governance have evolved in recent years, informed by robust international normative frameworks that include the United Nations Charter, International Human Rights Law, and the 2030 Agenda for Sustainable Development among others (see table 3 for a full list).

Acronym	International or Regional Framework	Purpose in AI Governance
UDHR	Universal Declaration of Human Rights	The UDHR offers a universally accepted set of principles that can guide AI governance, providing a common language to frame harms and establish clear parameters for what is permissible under international human rights law.[79]
ICCPR	International Covenant on Civil and Political Rights	The ICCPR obligates states to protect rights such as privacy (Article 17), freedom of expression (Article 19), and freedom of assembly (Article 21). These obligations extend to the deployment of AI systems, requiring governments to ensure that AI applications do not infringe upon these rights.[80]
GDPR	General Data Protection Regulation of the European Union	GDPR requires Data Protection Impact Assessments (DPIAs) for high-risk AI systems, restricts automated decision-making under Article 22, and emphasizes transparency, including the right to explanation.[81]
HLAB-AI	High-Level Advisory Body on Artificial	The HLAB-AI aims to align AI governance with

[75] ITU - AI Governance Day Report, 2024.
[76] Ibid.
[77] Cihon et al., 2020; Roberts et al., 2024
[78] Ibid.
[79] Shaheed et al.,2018.
[80] ICCPR, 1961.
[81] GDPR, Regulation (EU) 2016/679.

	Intelligence	the UN's overall goals. It provides global guidance on AI governance by recommending frameworks rooted in international cooperation and human rights. In its 2023 report Governing AI for Humanity, it proposed inclusive, multi-stakeholder structures – such as a global scientific panel and AI fund – to ensure equitable and safe AI development worldwide.[82]
EU AI ACT	European Union Artificial Intelligence Act	The EU AI ACT categorizes AI systems into four levels of risk—unacceptable, high, limited, and minimal—and imposes strict obligations on high-risk systems, including transparency, human oversight, and data quality requirements. The corresponding European AI office coordinates AI policy across the EU and enforces the AI act.[83]
MERCOSUR Declaration on AI	MERCOSUR Declaration on AI	The declaration establishes a regional framework for AI governance rooted in human rights, democratic values, and social inclusion. It emphasizes transparency, accountability, and human-centric design in AI systems, particularly concerning algorithmic decision-making in areas like employment, education, and public services.[84]
ICESCR	International Covenant on Economic, Social and Cultural Rights	The ICESCR emphasizes states' obligations to ensure that AI technologies support, rather than hinder, access to rights such as education, health, work, and social security. It calls for equitable access to the benefits of scientific progress, requiring that AI systems be developed and deployed in ways that reduce inequalities and enhance social inclusion, especially for marginalized groups.[85]

Table 3: International and Regional Frameworks on AI Governance, adapted from sources in the footnotes.

These frameworks provide critical legal and ethical foundations for the development, deployment and oversight of AI technologies. Moreover, these instruments safeguard rights like freedom of expression, privacy and non-discrimination, which are increasingly relevant in the context of algorithmic decision making and surveillance technologies.

Similarly, the 2030 Agenda for Sustainable Development provides a comprehensive framework to integrate AI governance with global developmental priorities. The agenda highlights the potential of AI to accelerate progress toward achieving the Sustainable

[82] United Nations, 2024.
[83] European Commission, 2021.
[84] Global AI Law and Policy Tracker, 2024.
[85] United Nations, 1966.

Development Goals (SDGs) while emphasizing the importance of mitigating risks such as digital divides and structural inequalities (see figure 6). AI governance under the 2030 Agenda emphasizes bridging digital divides both within and between nations, promoting the equitable use of AI technologies to advance economic, social and environmental development, as well as addressing biases in AI systems to prevent the perpetuation of discrimination and inequality.[86]

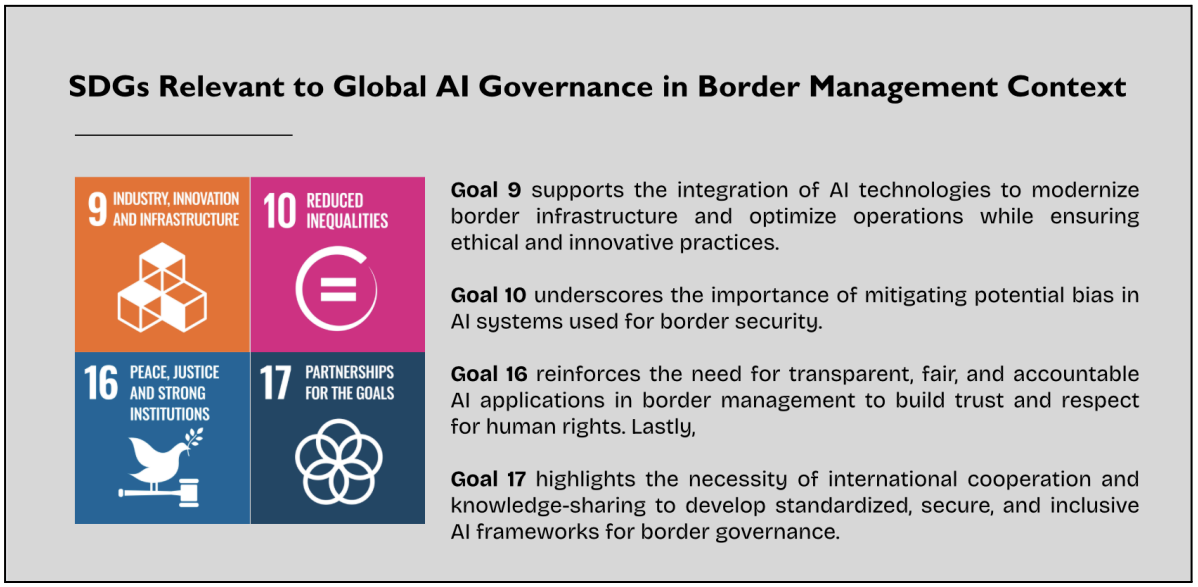

Figure 6: SDGs relevant to Global AI governance in the border management context, adapted from United Nations Sustainable Development Goals.

3.2. Governance and Regulation of AI in Migration and Border Management

Given AI's potential to play a pivotal role in migration and border management systems, it is important to highlight policy frameworks that centre accountability, transparency and the protection of fundamental human rights in this critical area.[87]

The European Union's AI Act, for instance, can be applied to discuss migration issues such as border surveillance and biometric identification, which are classified as 'high risk.'[88] This classification underscores the significant potential of such technologies to impact fundamental rights. These rights include privacy and data protection, non-discrimination, asylum, human dignity, freedom of movement, family life and the right to an effective remedy and fair trial. While the Act introduces oversight mechanisms – which will be later discussed as a best practice – the "Regulation of AI-Based Migration Technologies under the EU AI Act" Report critiques its inability to adequately address biases and discriminatory outcomes embedded in AI systems. These shortcomings raise concerns about fairness and equity in AI deployment. Moreover, the Act's alignment and coordination with existing legal frameworks remains ambiguous, highlighting a critical gap in ensuring cohesive and comprehensive governance.[89]

[86] UNGA Resolution on AI, 2024.
[87] Stewart, 2024.
[88] European Commission, 2021.
[89] Ibid.

International human rights norms, such as the United Nations Guiding Principles on Business and Human Rights, stress the responsibility of States and corporations to prevent the misuse of AI in migration contexts. Despite these principles, some recognize their lack of enforceability, particularly concerning accountability for private contractors managing AI systems at borders.[90] This limitation underscores the challenges of regulating cross-sectoral collaboration in migration governance. Furthermore, the World Migration Report 2024 highlights the absence of a globally harmonized framework for AI regulation, recognizing gaps in legal protections for migrants and leaving critical vulnerabilities unaddressed.[91]

Despite existing frameworks, significant gaps persist in the governance of AI in migration. The absence of a universal standard for regulating AI applications has resulted in fragmented approaches across national and regional levels, undermining the effectiveness of governance efforts.[92] Additionally, transparency deficits are a critical issue. The opaque design and deployment of AI algorithms, particularly by private contractors, raises concerns about accountability.[93] Consequently, current governance models offer limited mechanisms for redress, leaving migrants with few options to contest decisions made by AI systems.[94] These are some of the regulatory gaps that the report aims to address moving forward.

---

4. Findings

4.1. Research Methodology and Limitations

The following section outlines identified best practices for integration of AI into border management systems.

These best practices were informed by a series of semi-structured interviews conducted between February and April 2025 with professionals working in relevant fields such as border management, IT and artificial intelligence, digital governance and human rights law. In order to ensure that technical concepts of AI, ethical and regulatory considerations were reflected in the following recommendations, this report adopts an interdisciplinary approach informing the selection of contacted participants. Our sample size aimed to encompass 15 participants that included private sector stakeholders, border personnel, government border agencies, regulators, AI specialists and human rights experts.

However, due to the sensitive nature of the topic, many of the initially contacted participants declined their invitation which is reflected in (a) the sample size and (b) the lack of private sector representatives. Moreover, some governments denied the exploration of AI in their border management systems despite existing literature pointing to pilot projects conducted in these contacted countries. In this regard, our sample size includes only one government border agency. Given that this agency comes from a perspective of applied practice, their reflections will be highlighted often throughout the report.

---

[90] Tyshchukm, 2024.
[91] IOM, 2024.
[92] Ibid.
[93] Burell, 2016.
[94] Tyshchukm, 2024.

From the conducted interviews, this report distills common themes, recommendations and discussed examples, which have been compiled into fifteen IOM Member State recommendations. In order to align with the operational context of the IOM's Border Management, Returns and Readmission Division (BMRR), each recommendation has been organized according to the five pillars proposed through consultations with the IOM's Border and Identity Solutions Unit (BIS): capacity development, ICT development, security infrastructure, legal and regulation, and cooperation and collaboration. This section will proceed as follows: first, it will provide a list of the IOM Member State recommendations organized by pillar. It will then provide an analysis of the conversations which informed each recommendation.

4.2. List of Interview Participants

Interview participants included the following:

Name	Title	Affiliation	Area of Expertise
Chathura De Silva	IT consultant	IOM Sri Lanka	AI and IT systems
Anonymous	Manager of "The Centre for Responsible Data and AI" within the Chief Data Officer	Canada Border Services Agency (CBSA)	Data and analytics Responsible data Data privacy Ethical considerations of AI
Javier Galbally	Senior Officer of Research and Innovation	European Union eu-LISA	Biometric technologies AI and IT systems
Kulani Abendroth-Dias	Doctoral Candidate in International Relations and Political Science	Graduate Institute of International and Development Studies (IHEID)	AI systems Digital transformation Regulation for emerging technologies
Melanie Fink	Assistant Professor of Law	Leiden University	Human rights law EU law European migration Human rights protections in AI at borders
Colleen Thouez	Former Research Adviser for the UN Secretary-General's Representative for Migration	Formerly: UN Current: NASH	Migration law Human rights
Shantha Kulasekara	Senior Programme Manager / Head of Immigration and Border Governance Unit	IOM Sri Lanka	Border governance Border management
Madushani Warnasooriya	National IT Programme Officer	IOM Sri Lanka	AI and IT systems
Alexander Smith	Consultant and Researcher	Naif Arab University for Security Sciences (NAUSS)	Implementation of AI in border management in the MENA region
Anonymous	AI Specialist	IOM Washington D.C.	AI and IT systems
Anonymous	Border official	Anonymous	Border management

4.3. Recommendations for IOM Member States

From these expert interviews, this report identified fifteen best practices that should be considered by IOM Member States as they implement AI technologies in their border management systems:

	I. CAPACITY DEVELOPMENT
1)	Member States should build public trust through digital literacy campaigns to ensure familiarity with the workings and limitations of the technology.
2)	Member States should facilitate transparency and accountability by educating and familiarising their border personnel with the relevant technologies.

	II. ICT DEVELOPMENT
3)	To maximise the benefits of AI-Integration in border management, Member States should align their system design process with the necessity to balance facilitation and control (i.e., tourism, national security, trade) with due respect to international frameworks and human rights obligations.
4)	Member States should strive to incorporate 'explainable AI' methods over 'black box AI.' Doing so will ensure a transparent decision-making process; that the logic of a decision is readable by a human officer; and that if a decision is contested in a court of law, it is possible to return to the logic of the AI.
5)	Adopting a 'socio-technical' framework can provide Member States with an auditing system to guide their ICT development.
6)	Member States should also make sufficient arrangements to measure and evaluate potential system biases.

	III. SECURITY INFRASTRUCTURE
7)	Member States should ensure operational resilience through 'secondary processes' and 'pause scenarios' in the event of system failures or interruptions.
8)	Member States should maintain an anthropocentric approach by always ensuring human oversight over AI systems through mechanisms such as 'human in the loop.'

	IV. REGULATORY AND LEGAL
9)	Member States should work towards a common accountability forum, to collaborate on legal redressal mechanisms for individuals harmed by AI-assisted decisions in the border management context.
10)	Member States should work towards establishing preventative regulatory measures that outline permissible and non permissible uses of AI, as well as clear, enforceable standards for human oversight.
11)	Member States should establish clear guidelines on the use of sensitive data and ensure strong safeguards for how such data is stored, used and shared across borders.These measures are essential to ensure that AI systems support fairness and do not reinforce systemic bias.

	V. COOPERATION AND COLLABORATION
12)	Member States developing or using AI should consider co-design strategies that bring affected communities and internal stakeholders into the process from the start. Designing with diverse groups, rather than for them, is essential to ensuring AI systems are human centered and inclusive.

5. Best Practices to Leverage AI

5.1. Capacity Development

5.1a. Building Digital Literacy for Operational Functioning and Public Trust

Introducing an artificial tool into a fundamentally human process like migration – in which people stand at the core and directly experience its consequences – naturally breeds hesitation. AI can evoke fear and opposition, not only from the public, but also within the institutions and governments seeking its integration into their border management systems. A border official speaking to us on the condition of anonymity, admitted to not having much idea about how AI worked and fearing its use, despite the technology not yet being deployed in the airport she works at. To prevent such incomprehensibility-driven fears, it is essential that AI-driven solutions are implemented alongside comprehensive digital education and awareness strategies from the entities that adopt them. In this regard, this section highlights the reflections of the Centre for Responsible Data and AI at Canada's Border Services Agency (CBSA).[95]

[95]CBSA's recommendations will be consistently referenced throughout this report. Given their status as our team's only national government interviewee, we found their insights particularly insightful as they came from a place of applied practice.

The CBSA team, in their operational context, emphasized the importance of digital literacy not only among border management officials, but among all employees of the Canadian government :

> "If organizations or governments expect individuals to make decisions with the help of AI, it is essential to also clearly present the limitations of these technologies, how to work with them, and how to identify when there is a problem with the technology. Education is the best way to ensure proper, efficient and equitable use of AI systems." (CBSA Representative)

Part of digital literacy is 'socio-technical' literacy. The term 'socio-technical' refers to the practice of incorporating both technical and social elements in systems design, keeping into consideration the system's capacity to not only be shaped by society, but also to impact it.[96] This includes familiarity with concepts discussed in previous sections – namely, the reality that data is never neutral, and the potential for AI algorithms to reproduce data biases. In this regard, the CBSA has developed an internal presentation on data and algorithmic biases to increase digital and socio-technical literacy within the agency.

Like CBSA, Member States should consider adopting similar awareness practices into their integration strategies. Such practices can augment the capacity for human oversight as a best practice which will be discussed later in this report. Moreover, such training could facilitate conversations between border personnel and policymakers, leading to implementable and ethical capacity building for AI-integration at national borders.

However, CBSA emphasized that internal efforts to increase digital literacy within the government must work in tandem with public AI education. Similar perspectives were shared by an AI Specialist from the IOM offices in Washington D.C., who emphasized that fear surrounding AI arises from a lack of understanding. He reflected that this lack of understanding poses significant risks from three key perspectives: (a) for border personnel, who must learn to effectively work alongside AI technologies; (b) for the public, who often remain unaware of how these tools are being deployed on them; and (c) for regulators, who cannot effectively govern technologies whose limitations they do not fully understand. The CBSA representative pointed to the Finnish model as an example of robust AI education for the general public.

Finland's 'Elements of AI' open-access online course, a project collaboration between the government and the University of Helsinki, provides basic training on the workings of AI – defining what it is, how it works, how it is built and how it may affect members of the public.[97] This multi-module course was developed to 'demystify' AI and build public trust and digital literacy. As it is already publicly available across the European Union (EU), IOM Member States within the EU should consider adopting this course – or a nationally developed one – as part of required training for border personnel. For Member States outside of the EU, one may consider using this course as a blueprint for developing their own public AI education efforts.

---

[96] Mumford, 2000.

[97] "Elements of AI," 2018.

Taking these accounts into consideration, all IOM Member States seeking to integrate AI into their border management systems should consider a two-fold approach to capacity development through AI-focused education.

> **5.1a.** Building **public trust through digital literacy campaigns** – including open access courses like Finland's Elements of AI course – to ensure familiarity with the limitations and workings of the technology, allowing for greater ease of AI integration.
>
> **5.1b.** Facilitating **transparency and accountability by educating and familiarizing their staff** with the technology through means of modules such as the internal presentation used by CBSA.

In tandem with public AI education, Member States should practice public transparency – ensuring that how AI solutions are being incorporated into the border management process, what kinds of AI and how these technologies function are all public information.

5.2. ICT Development

5.2a. Aligning AI system design with national objectives

The use of AI technologies in border management is highly context-dependent, shaped by a country's primary objective at the border – whether it is security enforcement, trade and tourism facilitation, or a hybrid approach. Keeping national priorities in mind, the representatives from the Immigration and Border Governance Unit at IOM Sri Lanka outlined several best practices, grounded in the Sri Lankan experience but adaptable to a range of border governance models.

In contexts where trade and tourism facilitation are prioritized, AI can streamline passenger experiences and reduce resource burdens. Madushani Warnasooriya, an IT programme officer with the team, highlights how AI can be introduced first in non-regulatory tasks, such as e-forms, translation, or travel assistance.

In countries like the Maldives, where open border policies and tourism are economic cornerstones, AI should prioritize speed, convenience and customer service over enforcement. Warnasooriya cited that in some countries, the border is all about facilitation, not restriction. AI-powered predictive analytics and resource allocation tools can be used to optimize operations without compromising traveller experience. For countries that prioritize their tourism industry, for instance, AI-integration strategies should be aimed at reducing waiting times and safely approving as many visitors as possible. Looking at the example of Sri Lanka's Electronic Travel Authorization (ETA) system, in the pre-departure phase, it successfully reduces visa processing time from four days to three hours for low-risk travellers.

When prioritizing national security and enforcement, AI tools are most effective when deployed in hybrid models that retain strong human oversight. These tools support but do not replace human decision-making in high-stakes enforcement environments. AI is primarily used for initial filtering and risk profiling, though final entry decisions remain at the discretion of trained officers. This is evident in Sri Lanka's scenario-based targeting system, which profiles incoming passengers and flags potential risks for further human review. Continuing to draw from the Member State's experience, the 'Threat Environment Rule Engine' is of particular interest. It is an AI engine which processes incoming passenger data and compiles a shortlist of passengers who match the criteria for feature selection. This list is then presented to human officers for final evaluation before any action is taken. As a result, this two-tiered review system mitigates the risk of potential false positive or negative errors. Because there is a second level of human oversight involved, the final entry decisions are legally defensible and procedurally transparent.

AI use in border management cannot follow a one-size-fits-all approach. Whether driven by objectives such as enforcement, facilitation or tourism, Member States should deploy AI in border management systems based on aligning solutions with the necessity to balance border facilitation and control with due respect to international frameworks and human rights obligations.

5.2b. Preference for explainable AI techniques

Explainable AI (XAI) refers to a set of processes and methods that allow humans to better interpret an AI system's outcomes and logic, rendering more transparency in the decision making process.[98] It can refer to (a) AI models trained with techniques that operate using predefined, human readable logic that follows explicitly stated conditions (for instance, *if a passenger is travelling with expired documentation, flag to a border official)*, or (b) a set of methods that humans to interpret black box AI decisions after the system has been trained.[99] In either explainable AI scenario, the user can see the input, output and the decision making process in between.[100] In contrast, 'black box' AI models like deep learning-based systems, rely on complex statistical patterns rather than fixed rules in their decision-making processes, rendering them more flexible and accurate but harder to interpret (see tables 2 and 3 for differences between XAI and black box AI).[101] Users can see the input and output of the system, but not the process or logic in between. In this regard, explainable AI methods aim to unbox the opaque black boxes in the inbetween stage.

[98] Kosinski, 2024.
[99] Ibid.
[100] Ibid.
[101] Ibid.

Feature	Explainable AI methods (XAI)	Black Box AI (without XAI)
Transparency	Decision-making process is understandable	Decision-making is opaque and difficult to trace
Interpretability	Easy for humans to interpret or validate	Difficult to impossible to interpret without tools; user must have access to the data to interpret
Trustworthiness	Users can see why a decision was made	Trust is based on the accuracy rates of the AI model, but is not explainable
Complexity of Models	Machine learning models use simpler or interpretable models (decision trees, linear models, if-then rules)	Usually involves complex models and large-scale data patterns (deep learning, ensemble methods)
Typical Uses	Healthcare, Law, Finance – industries where accountability is necessary	Chatbots, image recognition, generative AI (ChatGPT)
Regulatory Compliance	Easier to meet transparency and auditability requirements	Harder to meet regulations like GDPR's 'right to explanation'

Table 2: Differences between explainable AI and black box AI. Elaborated from Dwivedi, Rudresh, et al.; 2023, and Holzinger et al., 2020; Andreou., 2023.

Feature	Explainable AI tools (XAI)	Black Box AI (without XAI)
Transparency of decisions	Border officers and oversight bodies can understand why an individual was flagged	The system flags someone, but the reasoning is unclear or hidden
Operational Trust	Increases trust among frontline personnel who can interpret the model's behavior	Reduces trust due to unpredictability and opaque decision-making
Accountability and Human Oversight	Supports legal and human rights compliance; decisions can be audited and justified	Difficult to explain or justify decisions if challenged in a court of law
Public Perception	Demonstrates responsible use of AI, improving legitimacy in the eyes of the public	Raises concerns about surveillance, discrimination, or profiling
Error Detection	Enables quicker identification and correction of bias or false positives	Makes it harder to identify why errors occur or if the system is biased
Regulatory Compliance	Helps meet transparency requirements under laws like GDPR or domestic oversight rules	May violate obligations around explainability and individual rights

Table 3: Differences between explainable AI and black box AI in the border management context. Elaborated from Dwivedi, Rudresh, et al.; 2023, and Holzinger et al., 2020; Andreou., 2023.

The Immigration and Border Governance Unit at IOM Sri Lanka highlighted the importance of utilizing explainable AI techniques in high stakes industries like border management. Utilizing such techniques ensures that decision-making is not only understandable, but verifiable and subject to human oversight. Chathura de Silva, an AI specialist and IT consultant for the team cites the following examples:

(a) If an AI system flags an individual as a national security threat at a point of entry, the border official upon examining the AI's classification should be able to refer back to its logic (for example, if the individual was flagged due to irregular travel patterns, or expired documentation) before making a final entry decision.

(b) In a situation in which any entry decision, partially informed by AI's classification, be challenged in a court of law, it is crucial that the logic behind the classification is explainable.

Example: Explainable AI for Facial Recognition Technology at Airport Customs

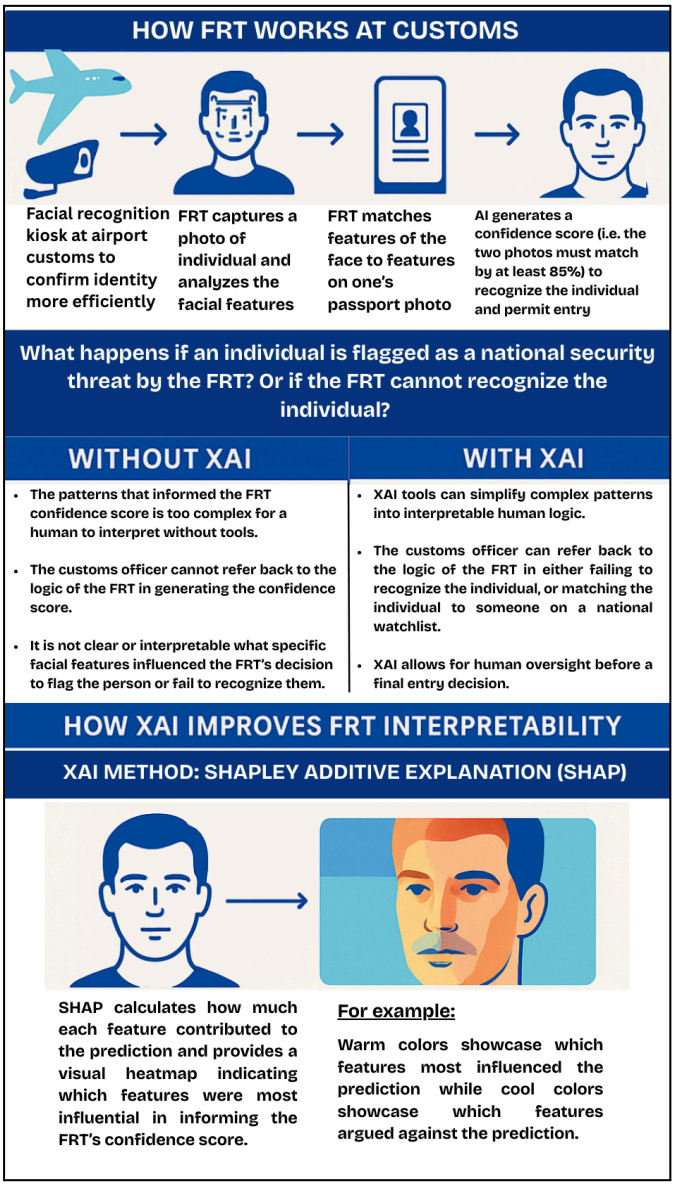

Figure 7: How XAI improves FRT. Adapted from Malik et al., 2021; Agrawal et al.,2024.

We can apply de Silva's points to the case of AI-powered facial recognition technology (FRT). As FRT is already widely used for identity verification at customs in several major international airports, it serves as a practical example of how explainable AI (XAI) can improve transparency and accountability in decision-making processes at borders.

Though FRT is an efficient tool for verifying identity of high volumes of travellers, it is classified as a 'black box' system as its decision-making relies on identifying complex patterns from large-scale image datasets.[102] Therefore, in situations that warrant further human review – for instance, if the FRT flags an individual as a security threat, or simply fails to confirm an individual's identity – the opaque design of the technology poses issues for the customs officer's ability to return to the AI's logic before making a final entry decision. While it is impossible for humans to understand these patterns, explainable AI methods pose potential to translate the AI's complex pattern recognition processes into interpretable human logic.

Figure 7 elaborates on how explainable AI methods that provide visual and feature-based explanations – like the Shapley Additive Explanation (SHAP) – can improve the interpretability and transparency of facial recognition systems.[103] Returning to the reflections of the IOM Sri Lanka Team, such techniques are especially important to create space for effective human oversight. As outlined in figure 7, if FRT is deployed at airport customs without explainable AI techniques, in the case of further review by a human officer, one cannot determine which specific features influenced the system's prediction. Contrastingly, XAI tools can not only allow the officer to analyze which specific facial

[102] Balaban, 2015.
[103] Malik et al., 2021

features informed the AI's logic, but support the official in either overriding or following through with the AI's decision.

Furthermore, in an instance where an AI-assisted entry decision is challenged in a court of law, it is vital that the rationale behind such decisions is explainable. This ensures that decisions not only withstand legal scrutiny, but also comply with laws mandating explainability and transparency in automated decision-making. For instance, the EU's General Data Protection Regulation (GDPR) explicitly includes an explainability clause, requiring that organizations deploying AI systems have the ability to provide clear and intelligible explanations for any automated decisions that may harmfully impact individuals.[104]

Article 22 of the EU General Data Protection Regulation (GDPR)

"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Figure 8: GDPR, Regulation (EU) 2016/679, Article 22

Legislation such as this one underscores not only the importance of transparent AI systems, but an individual's right to receive an explanation from an automated decision.[105] While opaque deep learning models and AI systems designs are often deemed incompatible with regulations with transparency, explainable AI tools have the potential to be a bridge between this gap.[106]

Finally, the use of explainable AI is particularly imperative in the context of inherent data biases – as discussed in the previous sections (see section 2.1 and section "Building Digital and Socio Technical Literacy") – and how they are often reproduced in AI models.[107] With this in mind, there are certain precautions that can be taken in the design and testing process to mitigate the risks of reproduced biases.

5.2b Measuring biases of AI systems and auditing demographic performance in biometric systems

Javier Galbally, Senior Officer of Research and Innovation at eu-LISA, highlights that unlike human bias, biases in AI technologies offer greater potential to be measured, traced and corrected. Using the example of an AI-powered facial recognition technology (FRT), in order

[104] GDPR, Regulation (EU) 2016/679, Article 22.
[105] Ibid.
[106] Hamon et al., 2022.
[107] Ntoutsi et al., 2021.

to assess and mitigate its potential biases, he emphasizes the importance of evaluating performance across a comprehensive range of demographic variables such as place of origin, gender, age, nationality and race. A robust evaluation should determine whether the system maintains consistent accuracy levels across these attributes. If significant discrepancies are observed *within* a demographic group – such as a FRT model achieving 99 per cent recognition accuracy for one age category (for example, persons over 70 years of age) but only 90 per cent for another (for example, persons less than two years of age) – this accuracy bias should be analysed to determine whether it is due to a systemic flaw (for example, unbalanced training data) or other factors that must be traced and corrected before implementation. In this example, the model exhibits a bias towards age, but the same can be applied to race, gender, or any demographic variable.

However, Galbally also cautions that detection of an accuracy bias across demographic groups does not necessarily imply a flaw in the system subject to correction. The accuracy variance may be due to the intrinsic difference in the amount of identity related information that can be found in one demographic group (for example, persons over 70 years of age) compared to a different demographic group (for example, persons less than two years of age). In this case, even if the system is perfectly designed and trained, it will always be better at recognizing older persons than babies. Such nuances should also be a factor in assessing the accuracy of an AI system.

However, referring back to CBSA's reflections that data is always biased – and that this will never cease to be a risk in the deployment of AI – this risk can be mitigated through bias evaluation methods that ensure measurability, traceability and correction. When developing AI technologies in the border management context, Member States should always deploy such evaluation mechanisms, especially in the deployment of AI-powered biometrics and FRT.

5.2c Adopting a 'socio-technical' assessment to audit AI systems

The Centre for Responsible Data and AI is a team within CBSA's Chief Data Office that utilises intersectional frameworks to ensure the building of a responsible data and analytics ecosystem within the agency. In a conversation with its manager, valuable insights were shared regarding the frameworks deployed by the team when auditing and assessing the responsibility of new AI systems and designs. These frameworks can serve as a model for IOM Member States looking to integrate AI into their border management systems in a responsible manner.

The team at CBSA developed a 'socio-technical assessment,' an evaluation grid centered around four pillars: transparency, accountability, explainability and human-centric design. Using these pillars, the team audits new AI systems throughout every stage of the development process. They thoroughly examine how the model is built, its key indicators and critical aspects of the data – that is, what data the system was trained on, its source, its quality, the reasoning behind its selection, and whether it was collected with appropriate consent.

This assessment framework ultimately serves a multi-pronged purpose: (a) to ensure that training data is ethically sourced and abides by data privacy laws (b) that the development of the AI technology is designed with as little harmful social impact as possible and (c) that the technology is not only inclusive for everyone, but adheres to existing Canadian anti-discrimination legislations.

For example, in the case of developing an AI-powered facial recognition system, CBSA's data responsibility team might consider several key factors in their assessment:

(a) Does this technology account for persons with physical disabilities? That is, does it function properly for a person with facial tourettes; is the recognition technology apt to recognize a face in motion; or the physical traits of an individual with down syndrome?

(b) Does this technology abide by the Canadian Accessibility Act, or national digital legislation?

(c) Is the data used to train the technology proportionally representative? Are there certain demographics that are overrepresented or underrepresented in the datasets?

Central to all of these considerations is the awareness that certain groups may be wary of providing their data for various state discrimination reasons. For instance, if a minority community in a specific country has faced a long history of traditional over policing, they will be hesitant to provide their biometrics to an associated authority for fear of further persecution. A socio-technical assessment similar to CBSA's can be useful to IOM Member States, especially if the government is working with private contractors whose data sources may not be entirely transparent.

5.3 Security Infrastructure

5.3a. Operational Resilience: Implementing 'secondary processes' and 'pause scenarios'

CBSA highlighted the importance of 'secondary processes' in border processes when AI fails or is inaccessible. A 'secondary process' refers to the manual process that predates the integration of AI technologies, which can often lead to 'undue hardship' or the point at which it is too unsafe, difficult, or expensive to remove barriers so people can participate in work or other areas of daily life.[108] This default process occurs when individuals are either unable or unwilling to engage with digital technologies, and need to be directed to less efficient manual procedures. These groups may include seniors, persons with disabilities or individuals who are cautious about engaging with surveillance technologies. The CBSA team stressed that manual alternatives must be just as efficient as digital ones, supported by dedicated staff and real-time data capture. Without this, some communities may be left out of the system's database, leading to demographic gaps and biases in upcoming AI models.

[108] British Columbia's Office of the Human Rights Commissioner., 2025.

Member States should ensure that both digital and manual options are equally efficient and accessible to mitigate situations where a group is disadvantaged. These measures are not only technical requirements, but reflect a government's commitment to fairness for all persons. When backup systems are slow or difficult to use, they place an extra burden on already marginalized groups. For CBSA, ensuring inclusive access to both digital and manual services is a fundamental part of responsible AI integration.

Furthermore, CBSA has integrated the practice of 'pause scenarios' into its AI operations. A pause scenario is a failsafe procedure which allows for an AI system to be paused without disrupting operations. This is especially important in environments like airports, where relevant systems require periodic maintenance or in some cases fail. This procedure ensures that services remain uninterrupted even if the AI-integrated system fails. The CBSA representative explained that failing to account for such scenarios can result in the complete breakdown of operations. A well-designed pause scenario works in a manner that the systemic interruption goes unnoticed by staff and travellers. Member States should consider building similar fallback mechanisms into AI systems to avoid disruptions when the technology fails.

5.3b. Human in the Loop Implementation

A shared consensus across interviews was the non-negotiable role of human oversight during the process of deploying AI tools at the border. When AI systems are treated as infallible, overreliance on these technologies suggests a danger of officials defaulting to automated decision making, even though these tools have been noted for their biased and erroneous outputs. Oversight mechanisms broadly ensure that decisions remain with trained officers equipped to challenge algorithmic output and rely on their own judgement. Member States using AI in sensitive areas, such as migration management, should consider adopting similar approaches to keep the decision making process aligned with the anthropocentric lens.

In order to complement the best practices of ensuring explainability and measuring bias discussed earlier, it is crucial to explore human oversight mechanisms.[109] Some broader regulatory discussions and frameworks such as the EU AI Act, – which aim to instrumentalise the involvement of humans to counter the unintended consequences of AI integration – already exist.

[109] Discussed by Javier Galbally, Professor Melanie Fink and the IOM Sri Lanka team.

Article 14 of the EU AI Act requires that:

"High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use."

Figure 9: European Commission, 2021, Article 14.

However, Melanie Fink, a legal scholar researching the EU's role in border control, notes that Article 14 simply discusses the effectiveness of human oversight but not the actual applicable oversight mechanisms to achieve that level of effectiveness. Conversing with the team at CBSA prompted us to explore the usefulness of 'human-in-the-loop (HITL)' as an oversight mechanism. Referring to the real-time human intervention during the operation of an AI system, a human actor is required to guide or validate its every output before it can take effect.[110] This ensures that the AI-integrated system will have a constant loop of feedback to take into account and correct any inconsistencies. In the context of border management, the mandatory clause in the HITL mechanism allows border governance officials to almost instantaneously intervene and verify automated decisions.

This allowance is particularly important as conversations with relevant experts revealed that the training data used to train algorithms to perform certain functions may not always match the operational data, leading to inaccurate outputs. Or as explained previously, it has different benchmarks for successful identification among different demographic groups. These inconsistencies can be flagged and prevented by human operators who are required to validate the AI system's output at each stage of its functioning.

This report, however, recognizes that the realisation of this best practice can be hindered by the operation of a reinforcing loop: AI-integrated is touted as a solution to counter human biases in critical areas of decision making before inconsistencies are flagged in the technology's regular operation. Next a team of human actors are assembled to review and correct biases internalized by the algorithm, bringing one back to the initial point of human bias and trapping the integration process in a cyclic loop. Nevertheless, Member States should continue to experiment and develop ethical and implementable oversight mechanisms that break the vicious cycle.

In addition to HITL, there are plenty of opportunities for human oversight outside of real-time review. One involves seeking human intervention after an AI-integrated system's output has taken effect, possibly to overturn the action in circumstances where it is required – more commonly known as an act of 'human review.'[111] On the other hand, human

[110] Fink, 2025.
[111] Fink, 2025.

oversight can also take the form of 'human design,' where humans are involved during the design, training and testing stages, but not at all during the operation of the actual system. As iterated earlier in this report, given that the act of migration concerns critical issues such as the right to free movement, non-discrimination and the protection of personal data, it is important for Member States to establish concrete human oversight mechanisms.

This report recommends prioritizing human design over human review, for the former allows developers to test and tackle issues before they can even arise, saving time, labour and capital when it comes to redressal processes. However, this does not mean that Member States should neglect human review mechanisms.

5.4 Regulatory and Legal Collaboration

5.4a. Legal Redressal Collaboration on an Accountability Forum

Drawing from the reflections of Professor Fink, technological innovation in the border governance space must be balanced with strong, accessible mechanisms for justice – especially for individuals particularly at risk of algorithmic profiling. In this regard, Fink emphasized the need for ex post and ex ante safeguards. Referring back to IOM Sri Lanka's recommendations for explainable AI, these safeguards can provide accessible and understandable mechanisms for individuals to challenge AI-assisted decisions in court.

Ex post safeguards are reactive regulatory measures designed to correct a harm that has been inflicted. A key concern identified by Fink is the diffusion of responsibility across different actors involved in the development and deployment of AI tools for migration management. Legal redress mechanisms are traditionally tied to jurisdictional boundaries – whether national, or regional level like the EU – which makes accountability in complex, cross-border AI systems especially difficult. A potential ex post safeguard to address this challenge includes the establishment of a common forum which acts as a centralized accountability mechanism. This would envision the creation of a space where individuals who have suffered harm from AI-assisted decisions in the migration context could lodge complaints without needing to first determine whether the responsible party is a national government, a regional agency or a private contractor. The establishment of an accountability forum can thus make the legal redressal process clearer and more accessible for the complainant (see figure 7).

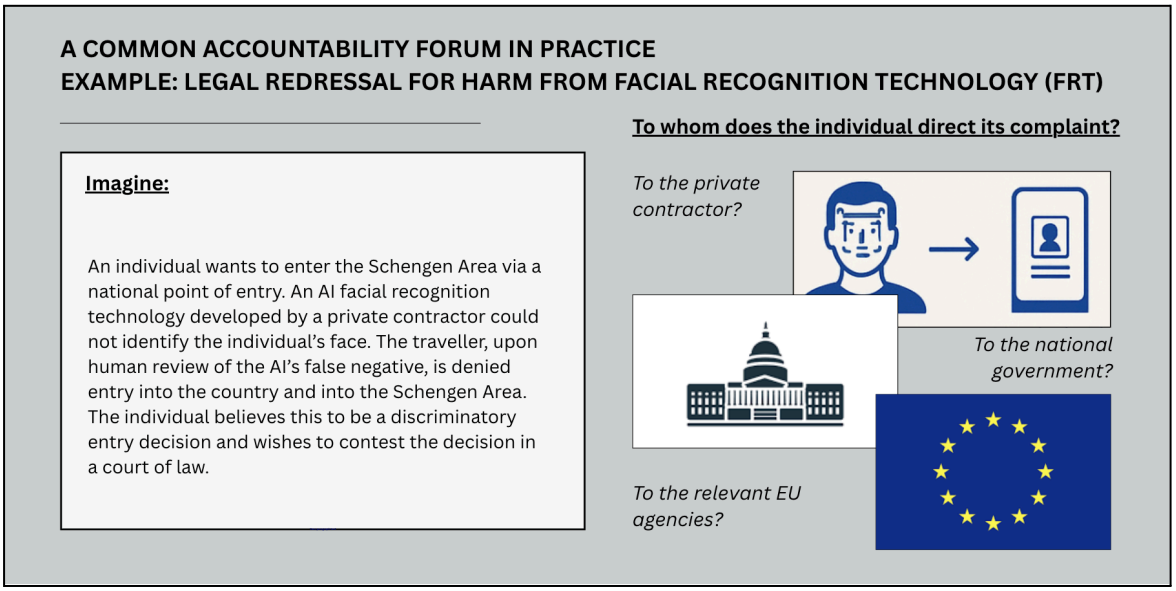

Figure 7: Common accountability forum example. Adapted from discussion with Fink.

5.4b. Regulatory Collaboration on Preventative Measures

In tandem with reactive regulatory measures, Fink highlighted the importance of ex ante safeguards – preventive regulatory measures designed to mitigate harm. This includes adopting legal structures that clarify permissible and impossible uses of AI and unambiguously delineate acceptable applications of AI in the field of migration. These frameworks must ensure that AI tools are used to uphold, rather than circumvent, human rights obligations. Legal structures should encourage the use of AI for purposes aligned with humanitarian objectives, such as improving reception preparedness or enhancing administrative efficiency.

In addition, ex ante safeguards should help establish enforceable standards for human oversight in all AI systems used in migration, especially those involving high-stakes decisions such as risk profiling or detention. To be meaningful, the role of human oversight must be precisely defined, with clear responsibilities, decision-making authority, and training to understand and intervene in automated processes. Oversight must not serve as a symbolic safeguard but as a standardised, enforceable mechanism that ensures individuals can understand and challenge the decisions affecting them.

Fink recommends that these be implemented at multiple levels including national, regional and international, in order to shape the design and permissible uses of AI systems. For this purpose, this report recommends that Member States consider:

(a) Establishing a common accountability forum.

(b) Adopting legal structures that clarify permissible and impermissible uses of AI.

(c) Establishing enforceable standards of human oversight in order to ensure interpretability of AI decisions in sensitive domains like migration.

5.4c. Regulatory Guidelines for Data Usage

Fairness and equity are central to responsible AI deployment, especially when working with sensitive data that can reflect or reinforce bias. In border management, where decisions often involve diverse populations, clear guidelines around data collection and the use of that data are essential.

Building on existing data protection frameworks like the European Union's GDPR, CBSA has developed a race-based data framework that sets strict boundaries on how race-related data can be used. As a result, CBSA's framework reinforces strict safeguards for how sensitive data is stored, accessed and potentially shared across borders. The GDPR's provisions for 'special categories of data,' including race and ethnicity, inform CBSA's approach. This approach limits the use of race-based data to three specific purposes: (a) identifying discrimination (b) eliminating discrimination and (c) measuring improvement. As a result, this data cannot be used in decisions related to enforcement or admissibility at the border.

Additionally, the CBSA team emphasized that certain data points, such as race or gender, must be handled with care due to the potential for discrimination. For example, giving too much weight to gender in a decision-making model could violate the Canadian Charter of Rights and Freedoms. Similarly to CSBA, Member States should establish explicit guidelines on the use of sensitive data and ensure the establishment of strong protections and clear safeguards for how this data is stored, used and shared across borders. These measures are essential to ensure that AI systems support fairness and do not reinforce systemic bias.

5.5 Cooperation and Collaboration

5.5.a. Co-Design with Affected Communities

Building on the earlier discussion about collaboration with affected communities, it becomes clear that effective AI governance in migration depends on collaboration across various sectors. Whether it is the design, regulation, or oversight of these systems, collaboration helps ensure that AI tools reflect diverse perspectives and are accountable to the people they affect. This includes working directly with affected communities through co-design, creating legal systems that share accountability, and coordinating efforts across regional and international institutions.

A central part of CBSA's approach is co-design. The agency works with partners such as the Indigenous Affairs Secretariat, accessibility offices, gender-based analysis groups, and racialized employee networks to shape systems from the beginning of the development process. This collaborative approach reflects CBSA's effort to design for everyone, not just the majority. The goal is not to entirely eliminate bias – something CBSA acknowledges is not possible – but to create space for ongoing conversations about identifying and addressing bias in the systems. As the team pointed out, AI systems may need to be paused, adjusted and even retracted as they are deployed in real-world applications. These

adjustments should not be perceived as failures, but as necessary steps toward building more equitable systems. Member States developing or using AI should consider co-design strategies that bring affected communities and internal stakeholders into the process from the start. As CBSA's model shows, designing with diverse groups of people, rather than for them, is a key part of creating AI systems that are truly human-centered.

Finally, in addition to co-design, Member States should consider referring to the international frameworks discussed earlier in this report – such as the UDHR, ICCPR or the Agenda for Sustainable Development – to ensure cooperative policy development across national and regional contexts. This consistency is particularly critical in the migration government. Additionally, these frameworks can be used to ethically guide partnerships between national governments and private companies as they collaborate on developing technological solutions to integrate into border management systems.

---

6. Conclusion

6.1. Best Practices

Although this report provides recommendations on operational, ethical and regulatory considerations for IOM Member States exploring the implementation of AI at their borders, several topics warrant further research. Further research into the partnerships between the public and private sector during the development of AI technologies would provide valuable insights that this report was not able to. Similarly, engagement with more government agencies across a variety of regions, and on-the-ground border personnel would expand the scope of this analysis.

Capacity Development	Build Public Trust through Digital Literacy	Facilitate Transparency & Accountability		
ICT Development	Align System Design with National Objectives & International Law	Use Explainable AI	Adopt Socio-Technical Frameworks	Measure and Evaluate System Biases
Security Infrastructure	Secondary Processes & Pause Scenarios	Human Oversight		
Regulatory and Legal	Common Accountability Forum	Define AI Use Limits & Oversight Standards	Establish Data Rules & Safeguards	
Cooperation and Collaboration	Co-Design with Diverse Groups	Common Evaluation Frameworks Aligned with International AI Governance		

6.2. Highlighting IOM's Role as a Leader and Collaborator

Returning to the report's initial recommendation on digital literacy and public AI education, the AI Specialist from the IOM offices in Washington D.C. emphasized the importance and necessity of familiarizing IOM staff with foundational AI concepts and exploring how these technologies can be leveraged to benefit migrants, travellers and border personnel.

"As the leading migration organization in the world," he noted, "it is important that we lead the conversation on how AI can be responsibly applied in the migration domain." To do so, he emphasized IOM's responsibility to engage stakeholders, donor countries and programme partners in open, informed discussions on both the opportunities and challenges of AI in migration.

With this IOM staff's reflection in mind, this set of outlined best practices, aims to aid the IOM's Border and Identity Solutions Unit in embracing this leadership role and shaping responsible AI discourse, practices and policies among Member States and within the migration space more broadly.

REFERENCES

Agrawal, A., Kaur, K. and Kaur, H. (2024). Explainable AI in Biometrics: A Novel Framework for Facial Recognition Interpretation. *2024 International Conference on Modeling, Simulation & Intelligent Computing (MoSICom)*, Dubai, United Arab Emirates, pp.524–529. Available at: https://doi.org/10.1109/MoSICom63082.2024.10881703.

Andreou, A. (2023) 'E-securing the EU borders: AI in European integrated border management', *Journal of Politics and Ethics in New Technologies and AI*, 2(1). DOI: https://doi.org/10.12681/jpentai.34287

Australian Border Force (2025) *SmartGates - Arrivals*. Available at: https://www.abf.gov.au/entering-and-leaving-australia/smartgates/arrivals

Australian Department of Home Affairs. (2024). *Freedom of Information request FA 24/05/01409 – Document released*. Available at: https://www.homeaffairs.gov.au/foi/files/2024/fa-240501409-document-released.PDF

Awad, A. I., Babu, A., Barka, E., and Shuaib, K. (2024). "AI-Powered Biometrics for Internet of Things Security: A Review and Future Vision." *Journal of Information Security and Applications* 82: 103748. https://doi.org/10.1016/j.jisa.2024.103748

Badman, A., Kosinski,M. (2025) IBM. Big Data.*IBM Think Blog*. Available at: https://www.ibm.com/think/topics/big-data

Balaban, S.,(2015). Deep learning and face recognition: the state of the art. *Biometric and Surveillance Technology for Human and Activity Identification XII*, Proceedings of SPIE, 9457, p.94570B. Available at: https://doi.org/10.1117/12.2181526.

Beduschi, A. (2020) 'International migration management in the age of artificial intelligence', *Migration Studies*, 9(3), pp. 576–596. DOI: https://doi.org/10.1093/migration/mnaa003.

Beduschi, A. and McAuliffe, M. (2021) 'Artificial Intelligence, Migration and Mobility: Implications for Policy and Practice', in McAuliffe, M. and Triandafyllidou, A. (eds.) *World Migration Report 2022*. Geneva: International Organization for Migration (IOM).

British Columbia Office of the Human Rights Commissioner. (2025). *Undue hardship*. https://bchumanrights.ca/glossary/undue-hardship/

Buolamwini, J. and Gebru, T. (2018) 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', in *Proceedings of 1st Conference on Fairness, Accountability and Transparency.* Available at: *https://proceedings.mlr.press/v81/buolamwini18a.html*

Burell, J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), pp. 1–12. Available at: https://doi.org/10.1177/2053951715622512

Canada Border Services Agency. (2025). *Canada Border Services Agency*. https://www.cbsa-asfc.gc.ca/menu-eng.html

Cataleta, M. S. (2020). *Humane Artificial Intelligence: The Fragility of Human Rights Facing AI*. East-West Center. http://www.jstor.org/stable/resrep25514

Centre for Democracy and Technology (2019) *AI and Machine Learning* https://cdt.org/ai-machine-learning/

Cihon, P., Maas, M.M. and Kemp, L. (2020). Fragmentation and the future: Investigating architectures for international AI governance. *Global Policy*, 11(5), pp.545–556. Available at: https://doi.org/10.1111/1758-5899.12890

Desai, D.R. and Kroll, J.A. (2018) 'Trust but Verify: A Guide to Algorithms and the Law', *Harvard Journal of Law and Technology.* https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech1.pdf

Dumbrava, C. (2021) *AI at EU Borders*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf

Dwivedi, R., Das, A., Roy, A., Samanta, S., Saha, S. and Saha, B., 2023. Explainable AI (XAI): Core ideas, techniques, and solutions. *ACM Computing Surveys*, 55(9), pp.1–33. Available at: https://doi.org/10.1145/3561048.

Elements of AI." Accessed April 11, 2025. https://www.elementsofai.com.

eu-LISA, (2020) Artificial Intelligence in the Operational Management of Large-scale IT Systems. DOI:10.2857/58386

eu-LISA (2024). *EURODAC.* https://www.eulisa.europa.eu/activities/large-scale-it-systems/eurodac.

European Commission. (2020). 'Automated Border Control (ABC)'. Ec.europa.eu. https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/automated-border-control-abc_en

European Commission (2024a) *Entry / Exit System (EES)*. Available at: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en

European Commission (2024b) *Schengen Information System (SIS).*https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en

European Commission: Directorate-General for Communications Network, Content and Technology (2018) *Draft Guidelines for Trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai

European Commission: Directorate-General for Migration and Home Affairs (2020). *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security. Volume 1, Main Report.* Publications Office, 2020. https://data.europa.eu/doi/10.2837/923610.

European Commission (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Union (2000). Charter of Fundamental Rights of the European Union. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union (2008). *Treaty on the Functioning of the European Union.* Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4301854

European Union (2016). *General Data Protection Regulation (GDPR) Compliance Guidelines*. Available at: https://gdpr.eu

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).* Official Journal of the European Union, L 119 (May 4, 2016): 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts (Artificial Intelligence Act).* Official Journal of the European Union, L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

European Union (2024). *Frontex.* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/frontex_en.

European Union. (2025). *How will the EES work? What is new during the border checks?*. https://travel-europe.europa.eu/ees/how-will-ees-work-what-new-during-border-checks_en

Eurostat. (2023). *Glossary: Information and communication technology (ICT)*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Information_and_communication_technology_(ICT)

Fink, M. (2025). *Human Oversight under Article 14 of the EU AI Act*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5147196

Fuad, M.T.H., Islam, M.T., Hossain, M.S. and Jang, Y.M.(2021.) Recent advances in deep learning techniques for face recognition. *IEEE Access*, 9, pp.99112-99142. : https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9478893&isnumber=9312710

FRONTEX (2021) *Artificial Intelligence Capabilities for the European Border and Coast Guard*. https://www.frontex.europa.eu/publications/artificial-intelligence-based-capabilities-for-the-european-border-and-coast-guard-final-report-CYyjoe

FRONTEX. (2022). *Frontex and France run pilot project to ease travel across borders*. https://www.frontex.europa.eu/innovation/announcements/frontex-and-france-run-pilot-project-to-ease-travel-across-borders-bb6hNt

FRONTEX. (2023). *Frontex EES Land Border Pilot Project: Bulgaria and Spain – Executive Summary*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/373d88a0-cc51-11ed-a05c-01aa75ed71a1/language-en

Garcia, R.V., Guo, G., and Valera, I. (2019). The harms of demographic bias in deep face recognition research. *2019 International Conference on Biometrics (ICB)*. IEEE, pp. 1–8. Available at: https://doi.org/10.1109/ICB45273.2019.8987373.

Global AI Law and Policy Tracker (2024) *Global AI Law and Policy Tracker*. Available at: https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf

Global Forum on Migration and Development (2016) *Economics of Migration and Development: Supporting Evidence for Thematic Area I.* Available at: https://publications.iom.int/system/files/pdf/final_report_economics_ninth_gfmd.pdf

Hobbs, L. *et al.* (2005) 'Data Warehousing,' in *Elsevier eBooks*, pp. 1–22. https://doi.org/10.1016/b978-155558322-4/50003-5.

Holzinger, A., Carrington, A. and Müller, H., (2020. Explainable AI methods: A brief overview. In *International Workshop on Extending Explainable AI Beyond Deep Models and Classifiers*, pp.13–38. Cham: Springer International Publishing.

IBM. (2021). Machine Learning.*IBM Think Blog*. Available at: https://www.ibm.com/think/topics/machine-learning.

IBM. (2025). Convolutional Neural Networks. *IBM Think Blog.* Available at: https://www.ibm.com/think/topics/convolutional-neural-networks

IBM. (2024). *What is artificial intelligence (AI)?*. https://www.ibm.com/think/topics/artificial-intelligence

International Organization for Migration (2024) *World Migration Report 2024, Chapter 11*. Available at: https://publications.iom.int/books/world-migration-report-2024

International Telecommunication Union (ITU) (2024) *AI Governance Day – From Principles to Implementation*. ITU Publications. Available at: https://www.itu.int/hub/2024/07/key- findings-on-the-state-of-global-ai-governance/

International Telecommunication Union. (2025). *About ITU*. https://www.itu.int/en/about/Pages/default.aspx

Israel T. (2020) 'Facial recognition at a crossroads: Transformation at our borders and beyond," *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3714297

Mumford, E. (2000). A socio-technical approach to systems design. *Requirements engineering*, *5*, 125-133.https://doi.org/10.1007/PL00010345

OECD and EMN (European Migration Network) (2022). *The Use of Digitalisation and Artificial Intelligence in Migration Management*. https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/migration/EMN-OECD-INFORM-FEB-2022-The-use-of-Digitalisation-and-AI-in-Migration-Management.pdf

Hamon, R., Junklewitz, H., Malgieri, G., De Hert, P. and Sanchez Martin, J.I. (2022). Bridging the gap between AI and explainability in the GDPR: Towards trustworthiness-by-design in automated decision-making. *IEEE Computational Intelligence Magazine*, 17(1), pp.72–85. Available at: https://ieeexplore.ieee.org/document/9679770

Kosinski, M. (2024) IBM. Black Box AI. IBM*Think Blog*. Available at: https://www.ibm.com/think/topics/black-box-ai

Kossow, N., Windwehr, S., & Jenkins, M. (2021).*Algorithmic transparency and accountability*. Transparency International. http://www.jstor.org/stable/resrep30838

Malik, S., Kumar, P. and Raman, B. ,(2021). Towards interpretable facial emotion recognition. In *Proceedings of the Twelfth Indian Conference on Computer Vision, Graphics and Image Processing*.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think.* John Murray.

McAuliffe, M. and L.A. Oucho (eds.), 2024. World Migration Report 2024. International Organization for Migration (IOM), Geneva.

Mejias, U.A. and Couldry, N. (2019) 'Datafication,' *Internet Policy Review*, 8(4). https://doi.org/10.14763/2019.4.1428.

Molnar, P. and Gill, L. (2018) 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System', *Citizen Lab* [Preprint]. Available at: https://tspace.library.utoronto.ca/handle/1807/94802.

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). DOI: https://doi.org/10.1186/s40878-022-00305-0.

Noble, S.U. (2018) *Algorithms of oppression*. New York University Press DOI: https://doi.org/10.2307/j.ctt1pwt9w5.

Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.E., Ruggieri, S., Turini, F., Papadopoulos, S., Krasanakis, E. and others (2020). Bias in data-driven artificial intelligence systems—An introductory survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 10(3), p.e1356. Available at: https://doi.org/10.1002/widm.1356.

OpenAI (2024) *ChatGPT (November 19 version)*. Available at: https://chat.openai.com/[112]

Papademetriou, D.G. and Collett, E. (2011).*A new architecture for border management*. Migration Policy Institute, Washington, DC. https://www.migrationpolicy.org/sites/default/files/publications/borderarchitecture.pdf

Roberts, H., Cowls, J., Morley, J. and Floridi, L. (2024). Global AI governance: barriers and pathways forward. *International Affairs*, 100(3), pp.1275–1286. Available at: https://doi.org/10.1093/ia/iiae073

Shaheed, Ahmed, and Vivian Ng. "UDHR at 70- Putting Human Rights at the Heart of Design, Development and Deployment of Artificial Intelligence." Essex Human Rights, Big Data and Technology Project, 2018. https://www.academia.edu/93702916/UDHR_at_70_Putting_Human_Rights_at_the_Heart_of_Design_Development_and_Deployment_of_Artificial_Intelligence?utm

TELUS Digital. (2025). *Training data*. https://www.telusdigital.com/glossary/training-data

[112] ChatGPT was used solely to format bibliography references and improve transitions in this document. No content generation was performed using the tool.

Tyshchuk, V. (2024) 'A Review of Legal Regulation Regarding The Use of Unmanned Aerial Vehicles for Border Security', *ICJ Journal of Border Studies*. DOI: https://doi.org/10.13165/j.icj.2024.06.005.

UNESCO (2021) *Recommendation on the Ethics of Artificial Intelligence*. Paris: United Nations Educational, Scientific and Cultural Organization, 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137.

United Nations (2024) *Governing AI for Humanity: Final Report of the High-Level Advisory Body on Artificial Intelligence.* New York: United Nations, 2024. https://digitallibrary.un.org/record/4062495.

United Nations (1966) *International Covenant on Civil and Political Rights.* Adopted December 16, 1966. Entry into force March 23, 1976. United Nations Treaty Series, vol. 999, p. 171. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

United Nations (1966) *International Covenant on Economic, Social and Cultural Rights.* Adopted December 16, 1966. Entry into force January 3, 1976. United Nations Treaty Series, vol. 993, p. 3. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights.

United Nations (1948) *Universal Declaration of Human Rights.* Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2013,to%20return%20to%20his%20country.

United Nations (2024a) *UNGA Resolution on Artificial Intelligence*. Available at: https://documents.un.org/doc/undoc/ltd/n24/065/92/pdf/n2406592.pdf

United Nations (2024b) *United Nations System White Paper on AI Governance*. https://unsceb.org/sites/default/files/2024-04/United%20Nations%20System%20White%20Paper%20on%20AI%20Governance.pdf

United Nations (n.d.) *Sustainable Development Goals*. Available at: https://sdgs.un.org/goals

UN Tourism. "World Tourism Barometer and Statistical Annex." *UNWTO*, 2024. https://www.unwto.org/un-tourism-world-tourism-barometer-data.

Vavoula, N. and Mitsilegas, V. (2022) *Advance passenger information (API) - an analysis of the European Commission's proposals to reform the API legal framework: Think tank: European parliament*, available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)745768

Vision-Box. (2021). *Vision-Box and The Finnish Border Guard deploy the first EU Entry/Exit System project inside the Schengen area.* https://www.vision-box.com/press-release/vision-box-and-finnish-border-guard-deploy-first-eu-entryexit-system-project-inside

Vision-Box. (2022). *Vision-Box and partners deliver Frontex innovative Entry/Exit System pilot at the largest EU land border in Bulgaria.* https://www.vision-box.com/press-release/vision-box-and-partners-deliver-frontex-innovative-entryexit-system-pilot-largest-eu

Wehrli, S., Braun, A., Seitz, J., and Schilling, M. (2022). Bias, awareness, and ignorance in deep-learning-based face recognition. *AI and Ethics*, 2(3), pp.509–522. Available at: https://doi.org/10.1007/s43681-021-00115-7.