



# Responsible artificial intelligence in international migration management: Legal and practical considerations

Ana Beduschi<sup>1</sup>

## Introduction

Artificial intelligence (AI) technologies, including generative AI, have become increasingly prevalent in the daily lives of millions of individuals worldwide. Therefore, it is not surprising that governments use AI technologies, including generative AI, to streamline workloads and increase efficiency in migration processing.<sup>2</sup>

AI is understood here as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.<sup>3</sup> Generative AI is a subset of AI technologies which “create[s] new content ... based on their training data and in response to prompts”.<sup>4</sup> Generative AI enables the creation of various forms of content, including text, images, videos, music and software code.

Some States have disclosed the use of AI, including generative AI, in international migration management. For example, Australia has acknowledged using AI to identify potential fraud in visa applications and support staff productivity and generative AI to synthesize and analyse large volumes of documentation.<sup>5</sup> Canada has also been using AI to triage visa applications.<sup>6</sup> Germany has utilized AI for identity management, including face, speech and dialect recognition; name transliteration (i.e. the conversion from one alphabet to another, such as from Arabic to Roman alphabet); and mobile phone data analysis.<sup>7</sup> The European Union Pact on Migration and Asylum recognizes the use of facial recognition technologies in the context of the Eurodac regulation.<sup>8</sup>

However, not all States have publicly acknowledged *whether* and, if so, *how* they use AI in international migration management. Regarding the first point – whether States are

<sup>1</sup> Ana Beduschi is Professor of Law at the University of Exeter, Law School.

<sup>2</sup> See, for example, Marie McAuliffe, “AI in migration is fuelling global inequality: How can we bridge the gap?” World Economic Forum (2023).

<sup>3</sup> European Parliament and European Council, Regulation 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Articles 3–1 (13 June 2024).

<sup>4</sup> Philippe Lorenz, Karine Perset and Jamie Berryhill, “Initial policy considerations for generative artificial intelligence”, OECD Artificial Intelligence Papers No. 1 (2023).

<sup>5</sup> Australia Department of Home Affairs, “Freedom of information request - FA 24/05/01409” (2024).

<sup>6</sup> Immigration, Refugees and Citizenship Canada, “CIMM – question period note – use of AI in decision-making at IRCC” (2022).

<sup>7</sup> Germany Federal Office for Migration and Refugees, “Identity management” (n.d.).

<sup>8</sup> European Parliament and European Council, Regulation (EU) 2024/1358 of 14 May 2024 on the establishment of ‘Eurodac’ for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1351 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council (14 May 2024).



using AI in this area – this paper argues that States should be more transparent, as this would help increase trust in their systems and processes and, ultimately, strengthen the rule of law. Regarding the second issue – how States use AI in this field – the paper reflects on the current advances in AI regulation worldwide and highlights the importance of adhering to international human rights law. Finally, it introduces a framework to support States with the responsible implementation of AI in international migration management.

### **Transparency and trust in artificial intelligence in international migration management**

States should be more transparent about whether they use AI, including generative AI, in international migration management. Transparency is widely recognized as a cornerstone of trust, and this applies equally to the use of AI in international migration management. The connection between transparency and trust is reflected in the work of Schnackenberg and Tomlinson, who define transparency as the “perceived quality of intentionally shared information” and break it down into three core dimensions: disclosure, clarity and accuracy.<sup>9</sup>

Disclosure involves sharing relevant information as much as possible, considering the constraints of the matter at hand, and doing so promptly. It does not necessarily mean sharing all available information – analysing which type of information is relevant to the public involves a degree of

subjectivity. This may include considerations related to public interests and the protection of the rights and freedoms of others. In the context of international migration management, States should publicly acknowledge their use of AI without necessarily revealing sensitive details that could compromise national security or the personal information of migrants.

Clarity demands that the shared information be easily understandable and accessible. In the context of international migration management, this involves sharing information in plain language about whether AI systems are used throughout the different phases of the migration process. This includes information about which AI systems are used, for what purpose, and whether – and the extent to which – they involve human input and assistance. It also entails providing general information on systems interoperability.

Accuracy requires correct and consistent information. When it comes to international migration management and AI, information about the AI systems being used should be kept up to date and in line with the rapid development of the technologies. This information does not necessarily need to be comprehensive or technical, but it should be accurate to inform migrants and the general public about the uses of AI in this context.

Increased transparency is closely connected to increased citizens’ acceptance of AI uses in public

<sup>9</sup> Andrew K. Schnackenberg and Edward C. Tomlinson, “Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships”, *Journal of Management*, 42(7):1784, 1788 (2016).



services.<sup>10</sup> Transparency can also lead to better accountability, ensuring that decisions are justified and in line with the rule of law. Even in sensitive areas, such as migration, where matters may be closely related to national security imperatives, public authorities should be accountable for their decisions and actions. Accordingly, States should prioritize transparency in AI implementation not only to enhance public trust and acceptance of AI in migration but also to strengthen accountability and the rule of law in their jurisdictions.

### **Current advances in artificial intelligence regulation and their implications for international migration management**

Specific laws and regulations regarding AI have already been implemented or are being increasingly discussed worldwide. For example, the European Union has passed legislation on AI, and the Council of Europe (CoE) adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (hereinafter the Framework Convention).<sup>11</sup> China's regulatory regime is also rapidly evolving, including the adoption of measures for the administration of generative AI.<sup>12</sup> Countries such as Brazil, Canada and the United Kingdom have also introduced plans for regulating AI, although their scope and stage of implementation vary

significantly.<sup>13</sup> At the United Nations level, there is a growing consensus that international human rights law must be respected, protected and promoted throughout the life cycle of digital technologies, including AI.<sup>14</sup>

European organizations share a similar view. The CoE Framework Convention establishes that activities within the AI life cycle – from designing to developing and deploying AI systems – must be entirely consistent with human rights.<sup>15</sup> It draws from key principles such as human dignity, transparency, accountability, equality, privacy, and safe innovation to establish specific rules and obligations for public authorities or private actors acting on their behalf. These include promoting equality and preventing discrimination, safeguarding individual privacy and personal data, and providing access to remedies in case of issues with AI systems and harm to individuals.

Admittedly, the Framework Convention allows for an exception in matters related to a State Party's national security interests. Even so, their practice should still be "consistent with applicable international law, including international human rights law obligations".<sup>16</sup> This exception could apply to matters relating to international migration management if these fall within

<sup>10</sup> Laszlo Horvath, Oliver James, Susan Banducci and Ana Beduschi, "Citizens' acceptance of artificial intelligence in public services: Evidence from a conjoint experiment about processing permit applications", *Government Information Quarterly*, 40(4):1–18 (2023).

<sup>11</sup> European Parliament and European Council, 2024; Council of Europe (CoE), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024).

<sup>12</sup> Cyberspace Administration of China, *Interim Measures for the Administration of Generative Artificial Intelligence Services* (13 July 2023).

<sup>13</sup> Brazil Senado Federal, *Bill No. 2338* (2023); Parliament of Canada, *C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act, 2022)* (2022); United Kingdom Prime Minister's Office, 10 Downing Street and His Majesty King Charles III, "The King's speech 2024", oral statement to Parliament (17 July 2024).

<sup>14</sup> United Nations General Assembly, "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development" (11 March 2024); United Nations General Assembly, "The Pact for the Future", draft resolution submitted by the President of the General Assembly, Annex I: Global Digital Compact (20 September 2024).

<sup>15</sup> CoE, 2024, Article 1 (1).

<sup>16</sup> *Ibid.*, Article 3 (2).



national security interests. Nonetheless, States would still need to comply with international human rights law, including the rules laid down by the European Convention on Human Rights regarding the right to privacy and the guarantee of non-discrimination.<sup>17</sup>

In the European Union, the Artificial Intelligence Act classifies AI systems used in migration, asylum and border control management as high-risk.<sup>18</sup> These are understood as AI systems used by public authorities or on their behalf for the analysis of evidence, determination of risk, examination of asylum and immigration processes, and identification and identity verification regarding asylum and immigration processing.<sup>19</sup> Providers and deployers of high-risk AI systems must adhere to various legal obligations under the Artificial Intelligence Act, including ensuring compliance with data quality standards, producing impact assessments, and establishing and implementing a risk management framework.

However, the Artificial Intelligence Act allows for some exceptions, which has been criticized by human rights organizations.<sup>20</sup> An AI system may not be classified as high-risk in the context of international migration management if it is considered not to pose a significant risk of harm.<sup>21</sup> For example, generative AI used for a specific procedural task or for preparatory tasks will likely not be classified as high-risk AI.

Accordingly, even in cases where national security exceptions apply, States should still uphold international human rights law standards and rules when designing, developing and deploying AI for international migration management. Doing so would reinforce the rule of law and ensure that States fulfil their obligations under international law. States should also ensure that AI is used responsibly and in a manner that respects the rights and dignity of migrants throughout the different phases of the migration process, as discussed in the following section.

### **A framework for the responsible use of artificial intelligence in international migration management**

This framework draws primarily on the imperative of “do no harm”, a well-developed principle in the humanitarian context that is commonly referred to in the field of technology and AI ethics.<sup>22</sup> This principle requires consideration of how one’s actions may inadvertently cause harm or create new risks for the populations concerned. This principle should thus be paramount in matters relating to international migration in order to avoid exacerbating or creating new risks for migrants who may already be in a vulnerable situation. This framework also builds on a risk

<sup>17</sup> CoE, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Articles 8 and 14 (1950).

<sup>18</sup> European Parliament and European Council, 2024, Article 6 (2).

<sup>19</sup> Ibid., Annex III (7).

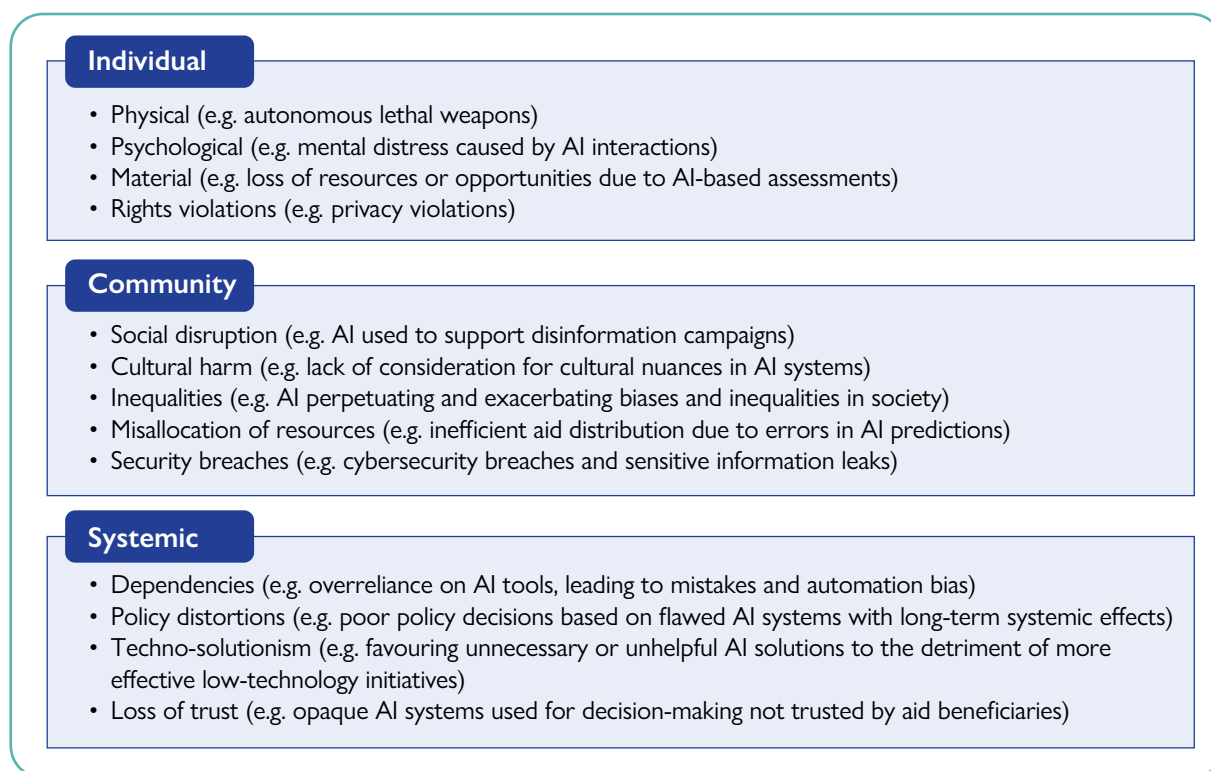
<sup>20</sup> See, for example, the #ProtectNotSurveil coalition [statement](#) on the Artificial Intelligence Act.

<sup>21</sup> European Parliament and European Council, 2024, Article 6 (3).

<sup>22</sup> See Mary B. Anderson, *Do No Harm: How Aid Can Support Peace or War* (Boulder, Colorado, Lynne Rienner Publishers, 1999); Massimo Marelli (ed.), *Handbook on Data Protection in Humanitarian Action*, third edition (Cambridge, United Kingdom, Cambridge University Press, 2024); Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, “Do no harm: A taxonomy of the challenges of humanitarian experimentation”, *International Review of the Red Cross*, 99(1):319–344 (2017); Luciano Floridi, *The Ethics of Information* (Oxford, Oxford University Press, 2013).



Figure 1. Harm typology



Source: Author's visualization.

assessment matrix<sup>23</sup> and takes into account the different legal principles and obligations discussed previously.

Harm can be individual, collective and systemic.<sup>24</sup> For example, individual migrants may have their right to privacy violated, their personal data exposed or their faces discriminated due

to the use of AI systems in decision-making processes. Collectively, they could also become victims of violence and social disruption when AI is used to support disinformation campaigns that harm migrant communities. This was the case in the United Kingdom in the summer of 2024 when riots and violent outbursts targeting migrants erupted following disinformation shared online.<sup>25</sup> More broadly, on a systemic level, any overuse of AI in migration may have various negative consequences. These include creating dependencies, perpetuating biases and errors, promoting excessive reliance on technological solutions, and undermining trust in decision-making processes.

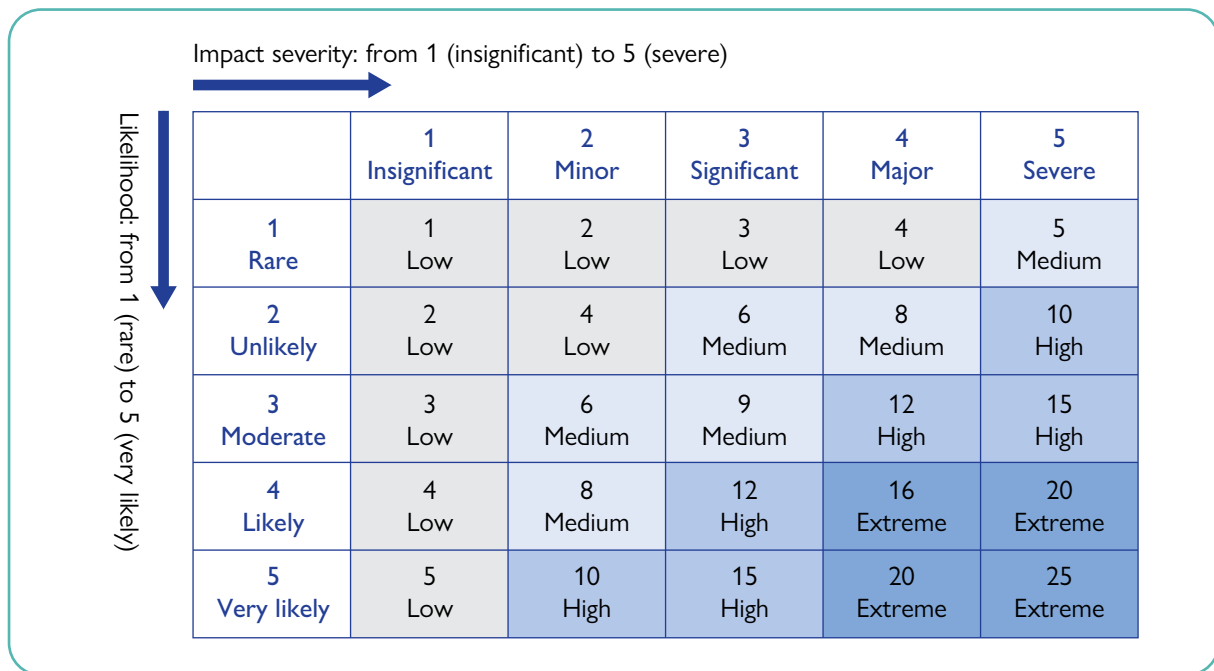
<sup>23</sup> See notably David Leslie, Christopher Burr, Mhairi Aitken, Michael Katell, Morgan Briggs and Cami Rincon, "Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence" (The Alan Turing Institute, 2021); Alessandro Mantelero, "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template", *Computer Law & Security Review*, 54:1–18 (2024); CoE, Committee on Artificial Intelligence, "Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA methodology)" (Strasbourg, France, CoE, 2024).

<sup>24</sup> See also for a discussion of harms in related fields: Daniele K. Citron and Daniel J. Solove, "Privacy harms", *Boston University Law Review*, 102:793–863 (2022); Lorna McGregor, Daragh Murray and Vivian Ng, "International human rights law as a framework for algorithmic accountability", *International and Comparative Law Quarterly*, 68(2):309–343 (2019).

<sup>25</sup> Will Downs, "Policing response to the 2024 summer riots", Insight section, House of Commons Library, UK Parliament (9 September 2024).



**Figure 2. Risk matrix**



Source: Author's visualization.

A risk matrix methodology can be particularly helpful for States undertaking risk assessments to identify, avoid and mitigate such risks of harm at the individual, community and systemic levels. The risk matrix proposed (see Figure 2) follows the risk matrix methodology<sup>26</sup> and is based on two axes, focusing on the likelihood of the risk of harm materializing and the impact it would have if it did materialize. Overall risk ranges are based on a scale of 1–25, where 1–4 is low, 5–9 is medium, 10–15 means high and 16–25 means extreme.

Consider, for example, a situation whereby a State may employ AI systems to automate tasks such as migrant identity verification, previously carried

out manually. However, using facial recognition for identity verification may lead to inaccuracies due to the limitations of AI systems in recognizing the faces of individuals with darker skin tones. That could lead to unlawful discrimination of individuals based on race and ethnic origins if no alternative ways to verify their identities were used. On a risk matrix, the likelihood that facial recognition will be inaccurate for recognizing darker skin types could be considered moderate (3) to likely (4) based on available evidence from studies in this area.<sup>27</sup> The impact of deploying such a technology, considering its inaccuracies,

<sup>26</sup> Leslie et al., 2021; Mantelero, 2024; CoE, 2024.

<sup>27</sup> See, for example, Joy Buolamwini and Timnit Gebru, “Gender shades: Intersectional accuracy disparities in commercial gender classification”, *Proceedings of Machine Learning Research*, 81:1–15 (2018); Andrew Hundt, William Agnew, Vicky Zeng, Severin Kacianka and Matthew Gombolay, “Robots enact malignant stereotypes”, proceedings of the 2022 Association for Computing Machinery (ACM) Conference on Fairness, Accountability, and Transparency (FAccT ’22) (20 June 2022).



would be severe (5), as it could lead to denial of services due to the lack of identity verification and potential discrimination. Accordingly, the overall risk would be extreme (15 or 20, depending on whether the likelihood of harm is set as 3 or 4).

In this scenario, alternative methods, such as manual identity verification, a two-step verification process or validation by a human case worker, should be made available to avoid or mitigate the risk of harm. On the risk matrix, the likelihood that facial recognition would be inaccurate for recognizing darker skin types could still be considered moderate (3) to likely (4). However, the impact of deploying such a technology could be considered insignificant (1) or minor (2) if these alternative methods were implemented in parallel. Accordingly, the overall risk of harm would decrease to low (3 or 4) or at most medium (6 or 8).

The risk assessment matrix can thus be used to identify, prioritize, avoid and mitigate risks. If relevant, it can also be used alongside SWOT (strengths, weaknesses, opportunities and threats) and PESTLE (political, economic, social, technological, legal and environmental) factors analysis methods. Yet, the “do no harm” principle should be paramount and inform these analyses.

For example, applying SWOT to the hypothetical scenario mentioned earlier, one strength (S) of using AI for migrant identity verification is the ability of AI systems to process large amounts of data quickly, reducing wait times and increasing efficiency. However, a significant weakness (W) in this situation is that AI systems would be processing sensitive data about migrants in potentially vulnerable situations, which could be at risk if cybersecurity measures were not

adequately set up from the outset. Additionally, using AI for migrant identity verification presents opportunities (O), such as freeing up human resources to focus on other critical areas in migration services if AI systems could save caseworkers’ time. However, the analysis should also consider potential threats (T), such as addressing data privacy and legal and ethical requirements for using AI in sensitive areas concerning migration management.

In the context of a PESTLE analysis of the hypothetical scenario discussed, States should consider political factors, such as the opportunity for enacting laws and policies, to support the use of AI in migration services. They should also assess the economic advantages and disadvantages of developing or procuring AI solutions compared to the potential savings in human resources. Furthermore, they should take into account societal factors, including public trust in AI used in this field, as well as technological advancements in generative AI and large language models, ensuring compliance with existing legal and regulatory obligations. Additionally, they should consider environmental factors, such as the environmental impact of energy-intensive AI systems.

Finally, the principle of “do no harm” should be considered throughout the analysis as an overarching aim to avoid causing new harm or exacerbating existing harm to migrants and migrant communities.

## **Conclusion**

As AI technologies, including generative AI, continue to advance rapidly, their use in international migration management is



becoming increasingly prevalent. This paper argues that States should be more transparent regarding whether they use these technologies in international migration management. Transparency not only enhances public trust and acceptance of AI in migration management but also strengthens accountability and the rule of law.

The paper also emphasizes the importance of improving how States use AI in this field and highlights the importance of adhering to international human rights law. This is especially relevant considering the numerous harms and challenges that migrants and migrant communities face, which can manifest at the individual, collective and systemic levels.

Accordingly, States should ensure that AI is used responsibly and in a manner that respects the rights and dignity of migrants throughout the different phases of the migration process. In this regard, the paper introduces a framework to support States in the responsible implementation of AI in international migration management. This framework adopts a principled approach centred on the “do no harm” principle. It encourages States to actively and thoroughly assess whether AI systems, including generative AI, could potentially cause harm or worsen existing situations for migrants and their communities. By integrating elements from the risk assessment matrix, SWOT analysis and PESTLE methodologies, States can be better equipped to more effectively decide how to implement AI in international migration management responsibly.