International and Comparative Law Quarterly (2025), 1–29
doi:10.1017/S0020589325000090

British Institute of International and Comparative Law

ARTICLE

The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights

Alberto Rinaldi[1] and Sue Anne Teo[2]

[1]Lund University, Lund, Sweden and [2]Raoul Wallenberg Institute of Human Rights and Humanitarian Law, Lund, Sweden
Corresponding author: Alberto Rinaldi; Email: alberto.rinaldi@jur.lu.se

Abstract
The widespread use of artificial intelligence technologies in border management throughout the European Union has significant human rights implications that extend beyond the commonly examined issues of privacy, non-discrimination and data protection. This article explores these overlooked impacts through three critical frameworks: the erosion of freedom of thought, the disempowerment of individuals and the politicization of human dignity. In uncovering these dynamics, the article argues for a broader conception of human rights to prevent their gradual erosion and safeguard the core principle of protecting human dignity.

Keywords: human rights; artificial intelligence; border control; border management technologies; migration; freedom of thought; disempowerment; human dignity

1. Introduction

The use of border management technologies driven by artificial intelligence (AI) is proliferating in the European Union (EU).[1] Underpinned by the recent turn to security, AI systems such as algorithmic decision-making and decision support[2] and surveillance and forecasting tools such as drones,[3] facial recognition and

[1] MA Martínez, 'EU Borders and Potential Conflicts between New Technologies and Human Rights' (2023) Paix&SecurIntl 7; N Vavoula, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' (2021) 23 EJML 457; P Molnar, 'Technology on the Margins: AI and Global Migration Management from a Human Rights Perspective' (2019) 8 CILJ 305; F Val Garijo, 'Drones, Border Surveillance and the Protection of Human Rights in the European Union' (2020) 25 VSVT 136; D Van Den Meerssche, 'Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association' (2022) 33 EJIL 171.

[2] AM Eklund, 'Rule of Law Challenges of "Algorithmic Discretion" & Automation in EU Border Control: A Case Study of ETIAS through the Lens of Legality' (2023) 25 EJML 249.

[3] Val Garijo (n 1); ÖE Topak, 'Drones: Robot Eyes on Racialized Migrant Bodies' (2023) 61 IntlMigration 313.

emotion recognition systems[4] are being tested and deployed in all aspects of border and migration management. While the digitalization of migration and border management is not in itself a new phenomenon,[5] being seen for example in tools to assist with the identification of travellers, the increasing use of AI shows a move away from mere automation and digitalization to the development of 'smart' digital border control, where the management of border control is determined by data-driven systems.[6]

There is a sizeable body of scholarship that examines the use of AI within border and migration contexts and its impact upon human rights.[7] This scholarship typically focuses on the threat that AI systems represent for the rights to privacy, non-discrimination and data protection.[8] This article goes further than noting tangible infringements of these discrete rights, examining the unseen impacts on human rights and the potential for the subtle erosion not only of other key rights—such as the freedom of thought—but also the unravelling of the conceptual and normative logic of the human rights framework.

The article examines three distinct, but related, questions concerning the use of AI in border management. First, it examines the potential impact of the use of AI on the freedom of thought. While technological interventions that pertain to the body (e.g. body scanners, surveillance cameras) are already commonplace, the continued push towards security seeks to introduce AI technology which has the potential to impact the human mind. Such technologies can attribute intentionality and criminality to individuals and have the potential to blur the boundaries between *mens rea* and *actus reus*, i.e. from criminal intent to criminal behaviour. This potential undermines individuals' autonomy and freedom to think without undue scrutiny or external judgment, thus impacting the right to freedom of thought. Whilst there is literature examining the human rights and rule of law impacts of

[4] European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement'; S Weinberger, 'Airport Security: Intent to Deceive?' (2010) 465 Nature 412; European Digital Rights, 'Facial Recognition & Biometric Mass Surveillance: Document Pool' (25 March 2020) <https://edri.org/our-work/facial-recognition-document-pool/>.

[5] C Dumbrava, 'Artificial Intelligence at EU Borders: Overview of Applications and Key Issues' (European Parliamentary Research Service, July 2021) section 1.1 <https://op.europa.eu/en/publication-detail/-/publication/a4c1940f-ef4a-11eb-a71c-01aa75ed71a1>.

[6] P Molnar, 'Territorial and Digital Borders and Migrant Vulnerability under a Pandemic Crisis' in A Triandafyllidou (ed), *Migration and Pandemics: Spaces of Solidarity and Spaces of Exception* (Springer International Publishing 2022); Van Den Meerssche (n 1).

[7] Access Now et al, 'Uses of AI in Migration and Border Control: A Fundamental Rights Approach to the Artificial Intelligence Act' (November 2021) <https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf>; Martínez (n 1); Molnar (n 1); C Blasi Casagran, 'Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU' (2021) 21 HRLRev 433; Vavoula (n 1); P Molnar, 'Robots and Refugees: The Human Rights Impacts of Artificial Intelligence and Automated Decision-Making in Migration' in M McAuliffe (ed), *Research Handbook on International Migration and Digital Technology* (Edward Elgar Publishing 2021); A Papachristodoulou, 'The Exercise of State Power over Migrants at Sea through Technologies of Remote Control: Reconceptualizing Human Rights Jurisdiction' (2024) 73 ICLQ 931.

[8] L Jacques, 'Facial Recognition Technology and Privacy: Race and Gender – How to Ensure the Right to Privacy is Protected' (2021) 23 SanDiegoIntlLJ 111.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

specific AI technologies used within border and migration management[9] as well as highlighting the problematic human rights impacts of border management technologies in general,[10] the potential impact of AI on the freedom of thought has yet to be analysed in detail, nor has the ability of the turn to securitization to facilitate the deployment of such systems in the border context, a gap which this article seeks to fill.

Second, beyond the risk to discrete rights, the use of AI in the context of borders and migration also presents a conceptual challenge, namely the disempowerment of the individual. Border and migration control is a sector that is defined by the vulnerability of individuals, thus increasing the potential of such technology to impact fundamental rights detrimentally.[11] As the individual is the focus of human rights protection, the disempowerment of individuals in this sector risks hollowing the protection of the human rights framework from within.

Third, the increased deployment of AI-driven border management technologies risks exacerbating the inequality already present in human rights protection, in effect supporting a two-tier model of rights protection offering a lesser degree of protection to refugees and migrants than to (EU) citizens, thus challenging the very foundational principle of human rights, namely human dignity.

In examining questions of freedom of thought, individual disempowerment and human dignity, the article aims to broaden the discourse surrounding the impact of AI, recommending a more holistic understanding that transcends conventional forms of analysis. The article thus expands the usual scope of human rights analysis in relation to technology in border control, reasoning that it is not only discrete rights that are being undermined but that the very foundational purpose of human rights protection is being unravelled and undermined.

This article approaches the analysis from the standpoint of the impact of AI border and migration management technologies and the inadequacy of existing human rights critiques. As such, even though specific AI technologies will be analysed as examples in the forthcoming sections, the technologies themselves are not the central locus of examination.

[9] Vavoula (n 1); Eklund (n 2).

[10] P Molnar, 'Digital Border Technologies, Techno-Racism and Logics of Exclusion' (2023) 61 IntlMigr 307; Martínez (n 1); D Ozkul, 'Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe' (Refugee Studies Centre, University of Oxford, 2023) <https://www.rsc.ox.ac.uk/publications/automating-immigration-and-asylum-the-uses-of-new-technologies-in-migration-and-asylum-governance-in-europe>.

[11] See Recital 60 of 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 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) [2024] OJ L series (AI Act). This recital acknowledges the human rights impacts of such technologies, stating that: 'AI systems used in migration, asylum and border control management affect persons who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee respect for the fundamental rights of the affected persons, in particular their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration.'

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

Some further caveats are necessary. First, not all AI-driven systems analysed in the article are currently in deployment; some are only at the testing stage. This includes controversial technologies such as emotion recognition systems, which, at the time of writing, have yet to be deployed.[12] Nonetheless, the article observes that the general trajectory of AI systems in border and migration management is one of placing increasing trust on the objectivity, speed and scale of AI in managing the increasingly complex nature of human migration, juxtaposed against the securitized lens of reinforcing and protecting borders. Second, although border and migration management technologies are in widespread use across different jurisdictions,[13] this article focuses primarily on the EU, although other examples are given for comparison purposes. Third, a holistic human rights analysis goes beyond jurisdiction-specific human rights frameworks and provisions. Although the European Convention on Human Rights (ECHR) is used as a point of departure, the analysis extends beyond the European context and questions the broader normative aims of human rights as a concept.

The article is structured as follows. Section 2 provides an introductory overview of AI systems and their increasing use within the border and migration context in the EU. Section 3 identifies and clarifies the conceptual and normative challenges for human rights presented by the use of AI within border and migration management, examining questions of freedom of thought, individual disempowerment and human dignity. The final section concludes, with a call for policymakers to take a more expansive view of the human rights impacts of the use of AI within the border and migration context in order to respect and protect human dignity.

2. AI systems in the EU securitized border and migration context

The promise of AI as a general-purpose technology that is able to discern patterns from large datasets to aid in decision-making, recommendations and predictions has permeated the public and private sectors alike.[14] Similarly, AI is also seeing increased uptake and deployment in the border and migration context.[15] Before unpacking how AI systems in border and migration management challenge human

[12] Van Den Meerssche (n 1); J Sánchez-Monedero and L Dencik, 'The Politics of Deceptive Borders: "Biomarkers of Deceit" and the Case of iBorderCtrl' (2022) 25 InfoComm&Soc 413.

[13] L Nalbandian, 'An Eye for an "I:" A Critical Assessment of Artificial Intelligence Tools in Migration and Asylum Management' (2022) 10 CompMigrStud 32; Molnar (n 1); A Beduschi, 'International Migration Management in the Age of Artificial Intelligence' (2021) 9 MigrStud 576; R Akhmetova and E Harris, 'Politics of Technology: The Use of Artificial Intelligence by US and Canadian Immigration Agencies and Their Impacts on Human Rights' in EE Korkmaz (ed), *Digital Identity, Virtual Borders and Social Media: A Panacea for Migration Governance?* (Edward Elgar Publishing 2021) 52.

[14] A Zuiderwijk, Y-C Chen and F Salem, 'Implications of the Use of Artificial Intelligence in Public Governance: A Systematic Literature Review and a Research Agenda' (2021) 38 GovInfoQ 101577; K Yeung, 'The New Public Analytics as an Emerging Paradigm in Public Sector Administration' (2023) 27 TilburgLRev 1; 'Artificial Intelligence Summit Focuses on Fighting Hunger, Climate Crisis and Transition to "Smart Sustainable Cities"' (*UN News*, 28 May 2019) <https://news.un.org/en/story/2019/05/1039311>; M Minevich, 'How To Fight Climate Change Using AI' (*Forbes*, 8 July 2022) <https://www.forbes.com/sites/markminevich/2022/07/08/how-to-fight-climate-change-using-ai/>.

[15] Vavoula (n 1).

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

rights, it is necessary to understand what is meant by AI. However, defining the concept of AI is complex and unclear, often seemingly acting as a 'shorthand for what are deemed to be "new" or "emerging"'[16] technologies.

This article adopts the conception of AI systems as computational technologies that, for a given set of objectives, are able to produce decisions, recommendations, content and predictions that interact with or affect physical or virtual environments. This definition is close to those adopted by the Organisation for Economic Co-operation and Development (OECD)[17] and the EU, as it appears in its Artificial Intelligence Act of 2024 (AI Act).[18] AI systems, unlike their human counterparts, are able to treat 'like cases alike', at a scale and speed that far exceeds even earlier automated technologies.[19] However, the promise of AI has been tempered by the fact that such systems have been demonstrated to be biased, especially towards minority and vulnerable groups.[20] This can be caused by a variety of factors, including the lack of diverse data representation, a lack of testing and lack of diversity within the design process or organization itself.[21] In turn, AI systems based on machine learning have been criticized as being 'black boxes',[22] meaning there is a lack of transparency in the decision-making as a result of the inability to look beneath the surface to reveal the processes and rationale of a particular recommendation or decision. In this way, the outputs of an AI system can be incomprehensible to the affected person as they lack a clear statement of reasoning which is a necessary precondition upon which to contest results or decisions.[23] Thus it is clear that AI systems can potentially be discriminatory, affect access to social and economic rights and infringe the right to an effective remedy among other potentially detrimental human rights impacts.[24]

[16] C Aradau, 'Borders Have Always Been Artificial: Migration, Data and AI' (2023) 61 IntlMigr 303, 304.

[17] The updated OECD definition defines an AI system as: 'a machine-based system 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. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.' For clarification on this definition, see S Russell, K Perset and M Grobelnik, 'Updates to the OECD's Definition of an AI System Explained' (*OECD.AI Policy Observatory*, 29 November 2023) <https://oecd.ai/en/wonk/ai-system-definition-update>.

[18] Art 3(1) of the AI Act (n 11) defines artificial intelligence systems 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'.

[19] D Kahneman, O Sibony and CR Sunstein, *Noise: A Flaw in Human Judgment* (Little, Brown Spark 2021).

[20] J Buolamwini and T Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) 81 ProcMachineLearningRes 1; V Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Press 2017).

[21] Eubanks ibid.

[22] F Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015).

[23] E Bayamlıoğlu and R Leenes, 'The "Rule of Law" Implications of Data-Driven Decision-Making: A Techno-Regulatory Perspective' (2018) 10 LIT 295; S Kempeneer, 'A Big Data State of Mind: Epistemological Challenges to Accountability and Transparency in Data-Driven Regulation' (2021) 38 GovInfoQ 101578.

[24] FJ Zuiderveen Borgesius, 'Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence' (2020) 24 IJHR 1572; O Bakiner, 'The Promises and Challenges of Addressing

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

The deployment of AI within the border and migration context raises similar issues, namely the invasion of privacy through surveillance, and concerns of bias and disproportionate impacts on vulnerable and marginalized groups. However, as the rest of this article will argue, the potential harm to human rights extends beyond these well-traversed concerns.

Within the EU border and migration context, various AI systems are already being used, have been tested or will be deployed in the future. Forecasting tools have long been used in border control, and involve an array of different technologies, some of which rely (increasingly) on AI, to enable the 'forecasting and assessing the direction and intensity of irregular migratory flows' to enable short-term or medium-term planning in managing migration flows.[25] Risk assessment predictive tools use AI to aggregate and detect patterns in data to identify and flag persons of interest to the border and migration authorities.[26] Facial recognition systems identify or verify people based upon facial biometrics which are a 'numerical representation of a biographic feature of an individual' gleaned through the face, fingerprints or voice.[27] Facial recognition systems have long been commonplace, having been possible before the advent of AI using simple image processing techniques for pattern matching, but their effectiveness and scalability has dramatically increased since incorporating AI. Their more sophisticated relation, emotion recognition, has only been possible with the development of AI. Emotion recognition systems use different methods such as 'the analysis of facial expressions, physiological measuring, analyzing voice, monitoring body movements, and eye tracking' to detect and infer emotions and intentions,[28] and have, in the EU, only been tested.[29]

Border and migration management within the EU can be contextualized within the framework of the Single Market. The freedom of movement within internal EU borders is a key principle and one of the four freedoms that drives the European Single Market. However, a lack of internal borders within the EU necessitates the strengthening of its external borders.[30]

Artificial Intelligence with Human Rights' (2023) 10 BigData&Soc 1; SA Teo, 'How Artificial Intelligence Systems Challenge the Conceptual Foundations of the Human Rights Legal Framework' (2022) 40 NordJHumRts 216.

[25] Ecorys, 'Feasibility Study on a Forecasting and Early Warning Tool for Migration Based on Artificial Intelligence Technology' (November 2020) <https://op.europa.eu/en/publication-detail/-/publication/5afa29f0-700a-11eb-9ac9-01aa75ed71a1>.

[26] Dumbrava (n 5) 18.

[27] T Israel, 'Facial Recognition at a Crossroads: Transformation at our Borders & Beyond' (Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, 2020) Key Terms & Abbreviations <https://archived.cippic.ca/uploads/FR_Transforming_Borders.pdf>.

[28] P Valcke, D Clifford and VK Dessers, 'Constitutional Challenges in the Emotional AI Era' in H-W Micklitz et al (eds), *Constitutional Challenges in the Algorithmic Society* (CUP 2021) 58.

[29] The EU-funded iBorderCtrl project tested emotional recognition systems in Hungary, Latvia and Greece in 2018, and the project was concluded in 2019. The iBorderCtrl project never went beyond the pilot phase. A case was brought before the Court of Justice of the European Union (CJEU) in 2018 by European Member of Parliament Patrick Breyer to gain transparency into the project, including on its legal and ethical aspects. In 2023, the CJEU ruled that the public could partially access documentation on the iBorderCtrl project, particularly concerning the reliability, ethics and legality of the technology, but full transparency was denied to protect the commercial interests of the consortium involved, see Case C-135/22 P *Patrick Breyer v European Research Executive Agency* ECLI:EU:C:2023:640.

[30] Martínez (n 1).

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

The earliest framework was the Schengen Information System (SIS) which was introduced in 1995, facilitating the alert of the authorities to suspect travellers such as wanted persons or those with prior visa refusals.[31] An extended and updated SIS framework was put in place in 2013 and 2018, respectively. The latter significantly expanded its remit to address counter-terrorism and irregular migration better, including through the use of biometric data and expanding the categories triggering alerts.[32] While it is beyond the scope of this article to examine in detail the intricacies of every border and migration management system, other key 'large-scale IT systems', as SIS is known, should be mentioned. Eurodac is another large-scale information technology (IT) system tasked with managing the storage and processing of digitalized fingerprints of those seeking asylum in the EU. Intended to begin operation in 2025, the European Travel Information and Authorization System (ETIAS) is a system authorizing entry for visa-exempt third-country nationals to 30 European countries.[33] Although primarily aimed at enabling visa-free short-term travel to the EU, the same system will also be used prior to a traveller's arrival to assess whether they 'pose a security, irregular migration or high epidemic risk'[34] to the EU. Other key systems within the European border and security architecture include the Visa Information System (VIS), a consolidated system that enables the exchange of visa data by linking the central system to national systems;[35] the Entry/Exit System (EES), to

[31] The Schengen acquis—agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. See also EU, 'A Strengthened Schengen Information System' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4376504>.

[32] See Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14; and Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56. While SIS does not yet deploy facial recognition systems, some authors have noted the dangers of function creep in large-scale IT systems. See e.g. G Mobilio, 'Facial Recognition Technologies and the Next Frontiers of Interoperability' (MediaLaws, 13 September 2023) <https://www.medialaws.eu/facial-recognition-technologies-and-the-next-frontiers-of-interoperability/>.

[33] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L236/1.

[34] Eklund (n 2). See also ETIAS Regulation ibid arts 1(1), 2, 4.

[35] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ L218/60. The legislation has been amended several times, including to take interoperability into account. See European Commission, 'Key Documents and Legislation on VIS' <https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system/key-documents-and-legislation-vis_en>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

register third-country travellers when crossing external EU borders;[36] and, finally, the European Criminal Record Information System for Third-Country Nationals (ECRIS-TCN), a centralized system that enables Member State authorities to check the criminal records of third-country nationals or Stateless persons.[37] In other words, successive measures have expanded the legal framework for border management and ever-more complex technologies have been implemented to increase the sophistication of border management systems.

Beyond its widened application, AI is also seeing a deepened reach through the interoperability of these systems, enabling information flows across systems to manage EU borders effectively. In June 2019, Regulations (EU) 2019/817 and (EU) 2019/818 entered into force and established the interoperability of all six of the systems noted above, both those already in operation (SIS, VIS and Eurodac) and those yet to be implemented (EES, ETIAS and ECRIS-TCN). This merges these previously separate systems into 'one single, overarching EU information system',[38] creating an unprecedented information behemoth at the service of the border and migration authorities. This was highlighted in the 2021 Schengen Strategy, in which the European Commission envisioned 'one of the world's most technologically advanced border management systems', facilitated through increasing use of AI for the purposes of law enforcement.[39] It has been argued, however, that such interoperability poses human rights concerns, as it challenges the principles of necessity and proportionality.[40] The deepened reach enabled through AI also extends to distance. When data from AI systems is combined, the 'visualising, registering, mapping, monitoring and profiling [of] mobile (sub)populations' is facilitated.[41] This ecology of technological tools, processes and systems in turn constitutes the increasingly digitalized or 'virtual' border, in which border control can take place away from physical borders,[42] meaning that individuals may be treated as subjects of interest even while far from the physical borders of the destination country. Eklund argues that border controls increasingly rely on 'automated, anticipatory and intelligence-based risk management tools which work more like a technological data-driven filter'.[43]

[36] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 [2017] OJ L327/20.

[37] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 [2019] OJ L135/1.

[38] Blasi Casagran (n 7) 433.

[39] Communication from the Commission to the European Parliament and the Council 'A strategy towards a fully functioning and resilient Schengen area' (2 June 2021) COM/2021/277 final.

[40] Blasi Casagran (n 7).

[41] D Broeders and H Dijstelbloem, 'The Datafication of Mobility and Migration Management: The Mediating State and Its Consequences' in I van der Ploeg and J Pridmore (eds), *Digitizing Identities: Doing Identity in a Networked World* (Routledge 2015) 243.

[42] Van Den Meerssche (n 1).

[43] Eklund (n 2) 250.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

The expansion of these various systems can be contextualized through the turn to securitization which has become the main paradigm for addressing major problems in society, to the point that 'migration, asylum, terrorism and drug traffic [have all] been handled through the exclusive lens of security'.[44] In this vein, crime prevention has undergone a significant transformation since the attacks of 11 September 2001 (9/11), as terrorism legislation has shifted focus onto preparatory activities.[45] Anti-terrorist pre-crime measures (ATPCMs) have also become the norm in many democratic States such as France, Canada and the United Kingdom (UK).[46] This turn to prevention has occurred hand in hand with advances in technology. Passenger Pre-Screening Systems, closed-circuit television (CCTV), sensors and Global Positioning System (GPS), facial recognition devices and other technologies have all become part of the new apparatus used to screen and detect potential ill-intentioned individuals.[47]

This turn has similarly gained traction within EU border and migration management, as forecasting tools are increasingly deployed for interdiction and pushbacks. AI-driven decision-making tools are used to gauge and profile suspicious persons and detect undesirable characteristics in the guise of 'risk assessment'. Facial and emotion recognition is being used ostensibly to 'read' behaviour and in the most-concerning instances, impute qualities of distrust and criminality upon persons.[48] The EU Parliamentary Research report on the use of AI in border and migration has noted the increasing '"securitisation of identity" and surveillance culture of the last two decades'.[49] Thus, management of security risks, now enabled through the measurability afforded by datafication and AI, can be read as the continuation of a securitization trajectory that began with 9/11.[50]

[44] T Balzacq, S Léonard and J Ruzicka, '"Securitization" Revisited: Theory and Cases' (2016) 30 IntlRel 505. Others have also adopted the militarization lens (examining how military technology increasingly extends to non-military use) to unpack and analyse the increasing use of different technologies such as drones within the content of border and migration management. See e.g. Topak (n 3).

[45] 'Many new terrorism offences enacted after 9/11 pushed the envelope of inchoate liability and came dangerously close to creating status offenses, thought crimes, and guilt by association', K Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (CUP 2011) 449.

[46] AJ Carrillo, 'The Price of Prevention: Anti-Terrorism Pre-Crime Measures and International Human Rights Law' (2020) 60 VaJIntlL 571. See also V Mitsilegas, 'The Preventive Turn in European Security Policy' in F Bignami (ed), *EU Law in Populist Times: Crisis and Prospects* (CUP 2019) 301.

[47] S Selter and R Kölbel, 'Hostile Intent – the Terrorist's Achilles Heel? Observations on Pre-Crime Surveillance by Means of Thought Recognition' (2010) 18 EurJCrimeCrLCrJ 237. On the utilization of facial recognition technologies in counter-terrorism, see S Robbins, 'Facial Recognition for Counter-Terrorism: Neither a Ban nor a Free-for-All' in A Henschke et al (eds), *Counter-Terrorism, Ethics and Technology. Emerging Challenges at the Frontiers of Counter-Terrorism* (Springer 2021).

[48] Ozkul (n 10); Sánchez-Monedero and Dencik (n 12). On the concept of crimmigration and biometric data, see N Amelung, '"Crimmigration Control" across Borders: The Convergence of Migration and Crime Control through Transnational Biometric Databases' (2021) 43 HistSocRes 151. However, not all EU AI-driven border and migration technologies are equally problematic. For example, the EUMigraTool, which provides both short-term and mid-term predictions of asylum seekers arriving in the EU, has requisite data protection standards in place. See Blasi Casagran (n 7); and C Blasi Casagran and G Stavropoulos, 'Developing AI Predictive Migration Tools to Enhance Humanitarian Support: The Case of EUMigraTool' (2024) 6 DataPol e64.

[49] Dumbrava (n 5) 32.

[50] ibid.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

Further, the securitization lens means that the definition of a security threat varies, as it largely depends on the subjective judgments of States regarding what they consider a threat, thereby allowing the promotion of 'highly securitised agendas'.[51]

The next section examines how the deployment and testing of AI in the border and migration context poses novel challenges for human rights within the three critical frameworks outlined above.

3. The impacts of AI on human rights

3.1. The impact of AI on freedom of thought

To date the mind remains largely *terra incognita* for the law. Although freedom of thought is a fundamental right enshrined in all major human rights texts, when it comes to defining what is actually meant by 'thought', much confusion persists.[52] As a direct corollary, the jurisprudence on the protection of the so-called *forum internum*, that is, the inner part of one's intellect, remains vague.[53] With the advance of medical technologies, specifically those used in the field of neuroscience, there has been a renewed interest in the meaning and scope of this right.[54] The use of new AI technologies that can detect facial expressions, biometric measurements and even human emotions directly calls into question the relevance of the mind. This is because such technologies are increasingly able to capture the mental processes that occur before the formulation and expression into words of an emotion.[55] Put differently, they can detect all those granular and

[51] Vavoula (n 1) 472.

[52] Specifically, International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 18 (1); Universal Declaration of Human Rights, UN General Assembly Res 217 A(III) (UDHR) (10 December 1948) UN Doc A/RES/217 (III), art 18; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 9 (1950) <https://www.echr.coe.int/documents/d/echr/convention_ENG>; Charter of Fundamental Rights of the European Union [2012] OJ C326/391 (CFR) art 10.

[53] The meaning of thought is still unclear, and little has been said about it in European human rights law. 'The absolute, unimpugnable and fundamental nature of the *forum internum* has been undermined by European institutions through persistent avoidance of principles that permit the *forum internum* rights to be asserted by applicants.' PM Taylor, *Freedom of Religion: UN and European Human Rights Law and Practice* (CUP 2005) 202.

[54] On this point, see specifically S Ligthart, 'Freedom of Thought in Europe: Do Advances in "Brain-Reading" Technology Call for Revision?' (2020) 7 JLB 1, 15–16. See also MJ Blitz and JC Bublitz (eds), *The Law and Ethics of Freedom of Thought, Volume 1: Neuroscience, Autonomy, and Individual Rights* (Palgrave Macmillan 2021). This has also translated into efforts to develop novel understandings of free will, mental autonomy and mental self-determination. For some important contributions, see S Alegre, *Freedom to Think: The Long Struggle to Liberate Our Minds* (Atlantic Books 2022); NA Farahany, *The Battle for your Brain. Defending the Right to Think Freely in the Age of Neurotechnology* (St Martin's Press 2023); S McCarthy-Jones, 'The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century' (2019) 2 FrontArtifIntell 19, 7–8. On mental self-determination, see JC Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination' in A von Arnauld, K von der Decken and M Susi (eds), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (CUP 2020) 387.

[55] I Neroni Rezende, 'Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces' in L Bachmaier Winter and S Ruggeri (eds), *Investigating and Preventing Crime in the Digital Era* (Springer 2022) 74–5; T Gremsl and E Hödl, 'Emotional AI: Legal and Ethical Challenges' (2022) 27 InfoPolity 163.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

erratic activities of the mind below the level of consciousness which have a direct effect on our behaviour.[56] Going beyond the usual concerns about privacy and data protection, these AI systems now pose a direct threat to the freedom of our inner existence.[57] In the words of the United Nations (UN) Special Rapporteur on Freedom of Religion and Belief:

> surveillance technologies deployed in 'counter-terrorism' and national security apparatuses threaten freedom of thought, among other rights, where they purport to reveal one's thought through inference … rooted in the idea that one can identify 'extremist thinking' and intervene before it manifests … authorities prosecute individuals without proving their correspondingly grave and guilty act (actus reus) shifting seamlessly from the criminalization of acts of terrorism to the criminalization of extremist thoughts and beliefs.[58]

On the one hand, the turn to security has led to a gradual blurring of the traditional *mens rea*/*actus reus* paradigm. Increasingly, (alleged) criminal intentions are flagged, leading to a culture of suspicion that closely resembles the concept of pre-crime.[59] On the other hand, new AI technologies deployed in border management are pushing that paradigm a step forward. By analysing our mental processes, they impute culpability, inferring it from a subtle movement of the face, a trembling in the tone of voice, a line of sweat, or a heartbeat.[60] The transition from criminal intention to criminal behaviour originates in the realm of our conscious and unconscious mental activities. Beyond traditional methods of profiling based on racial characteristics, the mind has become the last bastion to be conquered. But how is the mind protected within the European framework, and what is meant by 'thought' from a legal standpoint? The ECHR enshrines the protection of thought, conscience and religion in Article 9:

1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change her/his religion or belief and freedom, either alone or in community

[56] On the cognitive structure of emotions and their relevance for decision-making and human behaviour, see specifically A Damasio, *Descartes' Error: Emotion, Reason, and the Human Brain* (Harper Perennial 1995); A Ortony, G Clore and A Collins (eds), *The Cognitive Structure of Emotions* (CUP 1990); MC Nussbaum, *Upheavals of Thought: The Intelligence of Emotions* (CUP 2001); LF Barrett, *How Emotions Are Made: The Secret Life of the Brain* (Mariner Books 2017); and J. Debiec et al (eds), *The Emotional Brain Revisited* (Copernicus Center Press 2014).

[57] Recently the use of biometrics data has been sanctioned as a breach of art 10 and art 8 by the European Court of Human Rights (ECtHR) in *Glukhin v Russia* App No 11519/20 (ECtHR, 4 July 2023).

[58] 'Interim Report of the Special Rapporteur on Freedom of Religion or Belief, Ahmed Shaheed: Freedom of Thought' (5 October 2021) UN Doc A/76/380, 15–16.

[59] For recent contributions on the notion of pre-crime, see BA Arrigo and BC Sellers (eds), *The Prime Crime Society: Crime, Culture and Control in the Ultramodern Age* (Bristol University Press 2021); and J McCulloch and D Wilson (eds), *Pre-Crime: Pre-emption, Precaution and the Future* (Routledge 2016). In the context of the war on terror, see J McCulloch and S Pickering, 'Pre-Crime and Counter-Terrorism: Imagining Future Crime in the "War on Terror"' (2009) 49 BritJCriminol 628.

[60] On the relationship between emotions and facial gestures, see P Ekman and E Rosenberg (eds), *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression using the Facial Action Coding System (FACS)* (2nd edn, OUP 2005).

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

with others and in public or private, to manifest her/his religion or belief, in worship, teaching, practice and observance.

2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others.[61]

The European Court of Human Rights (ECtHR) has long held that this right constitutes one of the foundations of a democratic society.[62] The restrictions outlined in the second paragraph of Article 9 refer to the 'freedom to manifest one's religion or belief'. In other words, the freedom of thought, conscience and religion are absolute, and limits can only be imposed on the external manifestations of such thoughts and beliefs.[63] This has been described as the protection of the so-called *forum internum*.[64]

Significantly, the case law of the ECtHR on freedom of thought has mostly been confined to issues relating to the religious sphere.[65] Although Article 9 seems to distinguish between thought, conscience and religion, in practice case law has dealt mainly with the latter two, leaving the concept of 'thought' in an odd limbo.[66] Conscience has been interpreted almost exclusively in religious terms, with the terms freedom of conscience and individual conscience also being used to describe religious creed.[67] The danger posed by AI to this right is clear: AI technologies

[61] ECHR (n 52) art 9.

[62] *Kokkinakis v Greece* App No 14307/88 (ECtHR, 5 May 1993) para 31.

[63] On this point see BP Vermeulen and M van Roosmalen, 'Freedom of Thought, Conscience and Religion' in P van Dijk et al (eds), *Theory and Practice of the European Convention of Human Rights. Fifth Edition* (Intersentia 2018) 735. Art 9 can still be subjected to derogation in times of emergency under art 15(1). On this point, see WA Schabas, *The European Convention on Human Rights. A Commentary* (OUP 2015) 420.

[64] The distinction existing between *forum internum* and *externum* is supported by a vast amount of literature and scholarly work. For an opposing view, see CK Roberts, 'Reconceptualising the Place of the *Forum Internum* in Article 9 of the European Convention on Human Rights', PhD Thesis, University of Bristol (2020) <https://research-information.bris.ac.uk/en/studentTheses/reconceptualising-the-place-of-the-forum-internum-and-forum-exter>. Roberts argues that *forum internum* and *forum externum* should not be read as separate, but rather as a continuum.

[65] See for reference, Council of Europe, 'Guide on Article 9 of the European Convention on Human Rights: Freedom of Thought, Conscience and Religion' (31 August 2024) <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_9_eng>. On this point, see also generally, MD Evans, *Religious Liberty and International Law in Europe* (CUP 1997).

[66] LG Loucaides, 'The Right to Freedom of Thought as Protected by the European Convention on Human Rights' (2012) 1 CyprusHRLawRev 80.

[67] On this point, see generally C Evans, *Freedom of Religion under the European Convention on Human Rights* (OUP 2001). Conversely, freedom of conscience is found in cases dealing with objections to military service. See *Bayatyan v Armenia* App No 23459/03 (ECtHR, 7 July 2011); *Adyan and Others v Armenia* App No 75604/11 (ECtHR, 12 October 2017); *Dyagilev v Russia* App No 49972/16 (ECtHR, 10 March 2020). Additionally, an applicant can hold beliefs beyond the religious sphere, as in the case of assisted suicide. However, the Court has so far been reluctant in placing them under the protection of art 9. 'Not all opinions or convictions constitute beliefs in the sense protected by Article 9§1 of the Convention. Her claims do not involve a form of manifestation of a religion or belief, through worship, teaching, practice or observance as described in the second sentence of the first paragraph.' *Pretty v UK* App No 2346/02 (ECtHR, 29 April 2002) para 82.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

used in border management cannot distinguish between conscience, religion or other types of beliefs. The data collected is much less refined and yet more granular in its aggregation.[68] These technologies purport to detect a whole range of human reactions, as a direct consequence of conscious and unconscious thought processes.[69] Confining legal protection to personal beliefs and religious creeds is thus insufficient to address this scenario and represents a significant gap in the application of Article 9. What is the place of emotions and other mental processes affecting human behaviour in the scope of Article 9? Are they protected? And how can the potential impact of scrutiny by AI technology on a migrant's mental state be considered in this process? With the ECtHR's insistence on the absolute protection of the internal part of the mind, a discrepancy exists between the *forum internum* and the type of thoughts that enjoy legal protection, which will now be explored.

One of the earliest references to *forum internum* is found in the linked cases of *X* and *C* in the 1980s.[70] Both these Commission cases concerned Quakers who refused to contribute to military expenditure through taxation. Because they identified as pacifists, they considered military taxation contrary to their personal beliefs. In addressing the complaint, the Commission in *C* stated that: 'Article 9 primarily protects the sphere of personal beliefs and religious creeds, i.e. the area which is sometimes called the *forum internum*'.[71] It subsequently added that: 'in protecting this personal sphere, Article 9 of the Convention does not always guarantee the right to behave in the public sphere in a way which is dictated by such a belief'.[72] In both these cases, the obligation to pay taxes was seen as a neutral act due to the State, with no direct consequence for the inner beliefs of the applicant.

This basic formulation of *forum internum* is found throughout ECtHR jurisprudence.[73] It emphasizes that Article 9 protects people's innermost beliefs, but restrictions can be imposed the moment that such inner beliefs are translated into actions. However, the exact nature of what is meant by beliefs, other than

[68] AI technologies used in border management operate on probabilistic correlations rather than genuine understanding, meaning that they cannot accurately distinguish between conscience, religion or other types of beliefs. Instead, they rely on large-scale data collection and pattern recognition, which often lead to misleading or overly broad inferences. The data collected is simultaneously less refined—lacking context or nuance—but more granular in its aggregation, meaning that seemingly innocuous details can be pieced together to make sweeping assumptions. An example would be airline passenger data, where meal choices such as vegetarian, kosher or halal meals might be used as proxies to infer religious affiliation. Similarly, frequent travel to specific religious sites or attendance at faith-based conferences could be flagged by AI systems as indicators of religious belief, potentially leading to unwarranted scrutiny or discrimination.

[69] On this point, see JC Bublitz, 'Banning Biometric Mind Reading: The Case for Criminalising Mind Probing' (2024) LIT 1, 5–7.

[70] *X (Ross) v United Kingdom* App No 10295/82 (Commission Decision, 14 October 1983); and *C v United Kingdom* App No 10358/83 (Commission Decision, 15 December 1983).

[71] *C v United Kingdom* ibid 147.

[72] ibid.

[73] *Saniewski v Poland*, App No 40319/98 (ECtHR, 26 June 2001) para 6; *Porter v UK* App No 15814/02 (ECtHR, 8 April 2003) para 3; *Blumberg v Germany* App No 14618/03 (ECtHR, 8 March 2008) para 3; *Skugar and Others v Russia* App No 40010/04 (ECtHR, 3 December 2009) para 6; *Schilder v The Netherlands* App No 2158/12 (ECtHR, 16 October 2012) para 18.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

those related to the religious sphere, remains an open question. As noted above, answering this question has become critical now that AI technology can detect a whole range of mental states. The position of the ECtHR is somewhat contradictory. This is reflected, for instance, in the Guide to Article 9: '[o]n the one hand, the scope of [the Article] is very wide, as it protects both religious and non-religious opinions and convictions. On the other hand, not all opinions or convictions necessarily fall within the scope of the provision.'[74]

In one of its earliest formulations, the Commission adopted a restrictive approach, underlining that Article 9 'is essentially destined to protect religions, or theories on philosophical or ideological universal values'.[75] In *Salonen*, however, the Commission referred to 'the comprehensiveness of the concept of thought' in accepting the parents' wish to give their child a particular name.[76] Whilst it remains ambiguous what freedom of thought means and what it encompass, over the years the ECtHR has established a threshold for Article 9 protection. As formulated in *İzzettin Doğan*: 'the right to freedom of thought, conscience and religion denotes only those views that attain a certain level of cogency, seriousness, cohesion, and importance'.[77] This relatively high bar potentially has a negative impact when it comes to new AI technologies. If only opinions that reach a certain level of cogency find full protection, there is ample room for abuse. Furthermore, it is unclear how the importance of thoughts can be determined and through which moral framework they ought to be examined. The greater the ability of such technologies to detect internal mental processes, the stronger the protection under Article 9 should become. Here it is important to highlight once more how the securitarian paradigm whereby States seek to grasp the malicious intentions of individuals has significantly increased the interference in people's inner lives.[78]

It is therefore necessary to reconsider the core considerations underlying the original development of the freedom of thought. When introducing this right during the preparatory works of the ECHR, the French Rapporteur Pierre-Henri Teitgen stated:

[74] Council of Europe (n 65).

[75] *F.P. v Germany*, App No 19459/92 (Commission Report, 23 March 1993) 3.

[76] *Salonen v Finland*, App No 27868/95 (Commission Report, 2 July 1997) 5.

[77] *İzzettin Doğan and Others v Turkey* App No 62649/10 (ECtHR, 26 April 2016) para 68. See also in *Eweida and Others v the United Kingdom* App Nos 48420/10, 59842/10, 51671/10 and 36516/10 (ECtHR, 15 January 2013) para 81; and in *S.A.S. v France* App No 43835/11 (ECtHR, 1 July 2014) para 55. The Court has elaborated also on the meaning of conviction: 'The term "conviction", taken on its own, is not synonymous with the words "opinions" and "ideas" [It] denotes views that attain a certain level of cogency, seriousness, cohesion, and importance.' *Campbell and Cosans v the United Kingdom* App Nos 7511/76 and 7743/76 (ECtHR, 25 February 1982) para 36. See also *Valsamis v Greece* App No 21787/93 (ECtHR, 18 December 1996) para 25; and *Folgerø and Others v Norway* App No 15472/02 (ECtHR, 29 June 2007) para 84.

[78] On the normalization of mass surveillance regimes in the Eurozone, see specifically M Klamberg, 'Big Brother's Little, More Dangerous Brother: Centrum för Rättvisa v. Sweden' (*Verfassungsblog*, 1 June 2021) <https://verfassungsblog.de/raettvisa/>; and M Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa' (*EJIL: Talk!*, 26 May 2021) <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

> in recommending a collective guarantee not only of freedom to express convictions, but also of thought, conscience, religion and opinion, the Committee wished to protect all nationals of any Member State, not only from 'confessions' imposed for reasons of State, but also from those abominable methods of police enquiry or judicial process which rob the suspect or accused person of control of his intellectual faculties and of his conscience.[79]

This need to protect individuals' thoughts is even greater in the case of border and migration control, an already heavily securitized field in which individuals' vulnerabilities are starkly exposed. Facial and emotional recognition AI systems increase the potential risk by aggregating a whole series of biometrics and biomarkers related to mental state. Multiple types of thoughts and mental processes which form an individual's inner life are today susceptible to being flagged as dangerous. Society is on the threshold of transferring analysis of a person's intellectual state from traditional, human-centred, intelligence methods to myriads of aggregate data and algorithmic processes over which there is no real control. The perils seem even greater with border management systems, where migrants and asylum seekers are subject to fear, tiredness and the constant threat of rejection. It is therefore imperative that the protection of the mind be elevated to greater prominence and importance in the years to come.[80]

A potential development of greater protection can be noted in *Sinan Işık* which established that the Turkish government could not force the applicant to disclose his faith. The ECtHR recognized that: 'what is at stake is the right *not to disclose* one's religion or beliefs, which falls within the forum internum of each individual. This right is inherent in the notion of freedom of religion and conscience.'[81] While remaining within the sphere of religious creed, this formulation of *forum internum* takes an inverse perspective, the ECtHR noting that it would examine the case: 'from the angle of the *negative aspect* of freedom of religion and conscience, namely the right of an individual not to be obliged to manifest his or her beliefs'.[82] This approach has been endorsed by several scholars who have emphasized the need to move away from an interpretation of freedom of thought in the traditional sense and rather to consider the negative aspects of the protection offered by Article 9, focusing on an individual's right to have certain thoughts or beliefs without fear of manipulation or punishment.[83]

[79] European Commission of Human Rights, 'Preparatory Work on Article 9 of the European Convention on Human Rights' (16 August 1956) Doc DH (56) 14, 3–4 <https://www.echr.coe.int/documents/d/echr/echrtravaux-art9-dh-56-14-en1338892>.

[80] On this point, see L Swaine, 'Freedom of Thought as a Basic Liberty' (2018) 46 PolTheory 405; and M Moore, 'Freedom of Thought at the Ethical Frontier of Law & Science' (2022) 32 Ethics&Behav 510.

[81] *Sinan Işık v Turkey* App No 21924/05 (ECtHR, 2 February 2010) para 42 (emphasis added).

[82] ibid para 41 (emphasis added).

[83] The negative protection offered by freedom of thought has been articulated by Susie Alegre as: (1) the right not to reveal one's thoughts; (2) the right not to have one's thoughts manipulated; and (3) the right not to be penalized for one's thoughts: S Alegre, 'Rethinking Freedom of Thought for the 21st Century' (2017) 3 EHRLR 225. See also JC Bublitz, 'Freedom of Thought in the Age of Neuroscience: A Plea and a Proposal for the Renaissance of a Forgotten Fundamental Right' (2014) 100 ARSP 1; and S Ligthart

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

Some comparative insights might be usefully drawn with Article 18 of the Universal Declaration of Human Rights (UDHR), which largely inspired the text of Article 9. The preparatory material of the UDHR shows an emphasis on the importance of the *forum internum* in Article 18. In particular the French representative René Cassin took the stance that:

> freedom of thought was the basis and the origin of all other rights. Freedom of thought differed from freedom of expression in that the latter was subject to certain restrictions for the sake of public order. It might be asked why freedom of *inner* thought should have to be protected even before it was expressed. That was because the opposite of *inner* freedom of thought was the *outward* obligation to profess a belief which was not held. Freedom of thought thus required to be formally protected in view of the fact that it was possible to attack it indirectly.[84]

Cassin stressed the substantial difference between the expression of a thought and its protection *before* it was even articulated.[85] Even though the UDHR debates do not elucidate the meaning of thought itself, they do offer an indication of the importance given to this right (and to the meaning of *forum internum*) at the time of its inception. This understanding should be revisited in this era of facial recognition and AI-based border management technologies.

Indeed, the approach in *Sinan Işık* suggests that this distinction is highly relevant in relation to AI technologies and algorithmic screening, with the ECtHR taking a step forward in protecting inner beliefs from State intervention. This case has brought new attention to the idea that thought can be attacked 'indirectly', as highlighted more than half a century ago by Cassin. It is clear that AI technologies are capable of inferring mental processes and unconscious activity with ever greater precision, which in combination with the widespread datafication and securitization of border management represents a considerable cause for concern. The time has therefore come for the ECtHR to reconsider the scope of Article 9 and adopt a more holistic approach, extending beyond religious beliefs and encompassing protection of the *forum internum*.[86] It is argued that adopting this view for future cases is crucial and would generate positive spillover effects not

et al, 'Rethinking the Right to Freedom of Thought: A Multidisciplinary Analysis' (2022) 22 HRLRev ngac028.

[84] Summary Record of the Sixtieth Meeting [of the Commission on Human Rights] (4 June 1948) UN Doc E/CN.4/SR.60, 10, preparatory to the UDHR (n 52). Art 18 of the UDHR states: 'Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.'

[85] Cassin further argued that thought had a metaphysical significance, which should not be subjected to any restrictions, and that there was a significant distinction to be drawn between freedom of thought and freedom to hold an opinion, Summary Record ibid 1768.

[86] For instance, O'Callaghan and Shiner have argued that art 9 'provides a separate right to freedom of thought that can be mobilised outside of the freedom of religious belief', P O'Callaghan and B Shiner, 'The Right to Freedom of Thought in the European Convention on Human Rights' (2021) 8 EJCL 129.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

only at the level of fundamental rights protection under the ECHR, but also in relation to migration and the status of refugees in Europe.[87]

3.2. Individual disempowerment

This section will examine a second challenge posed by border and migration technology that has yet to be addressed squarely, namely the disempowerment of the individual. It is a truism that the international human rights law framework consists primarily of individual legal rights.[88] On this basis, it can be argued that the human rights framework is premised upon empowering the individual to challenge and address violations prohibited under the framework. This section begins by demonstrating the fundamental nature of individual empowerment before examining how it is being undermined through the deployment of AI systems for border and migration management.

First, history supports the assertion that the individual is the focus of human rights protection. One key theoretical underpinning of human rights centres on natural rights, arguing that the contemporary human rights framework mirrors pre-existing moral rights.[89] The theory can be traced to scholars such as Locke, who argued that various rights exist in the 'state of nature' and are meant to be protected by the constitution of government.[90] The contemporary interpretation of natural rights is generally reflected in the concept of human dignity that underpins the human rights framework.[91] In this sense, individuals are said to have inherent worth by virtue of their existence, independent of who they are, where they are from or other status markers. Since only individuals possess moral rights, it is uncontroversial to describe the international human rights protection framework as being centred on the empowerment of the moral rights holder.

A second historical rationale for individual empowerment stems from more recent history, namely the impetus for international human rights protection created after the Holocaust and World War II.[92] Buchanan argues that 'radical collectivism',[93] meaning collectivist ideas promoted by, for example, National Socialism, negated the worth and importance of the individual and subsumed this to forms of collective identity. The individual is said to have 'no significant moral worth on his own account but rather derives whatever value he has by virtue of his usefulness to

[87] The need to develop the traditional understanding of *forum internum* has recently been stressed by the UN Special Rapporteur on Freedom of Religion or Belief: 'As technological advances increase the possibility of accurately decoding or inferring one's inner mind, clear parameters, and protections for *forum internum* rights need urgent consideration.' 'Interim Report of the Special Rapporteur' (n 58) 9. On the same lines, see also S Alegre, 'Regulating around Freedom in the "Forum Internum"' (2021) 21 ERAForum 591.

[88] See the Introduction in A Buchanan, *The Heart of Human Rights* (OUP 2013).

[89] On the 'mirroring' view, see A Buchanan, 'Why International Legal Human Rights?' in R Cruft, SM Liao and M Renzo (eds), *Philosophical Foundations of Human Rights* (OUP 2015).

[90] P Laslett (ed), *Locke: Two Treatises of Government* (CUP 1988).

[91] CR Beitz, 'Human Dignity in the Theory of Human Rights: Nothing but a Phrase?' (2013) 41 Phil&PubAff 259, 264; J Morsink, *Inherent Human Rights: Philosophical Roots of the Universal Declaration* (University of Pennsylvania Press 2009).

[92] J Morsink, 'World War Two and the Universal Declaration' (1993) 15 HumRtsQ 357.

[93] Buchanan (n 89) 247.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

or membership in the nation'.[94] The subsequent adoption of the UDHR reaffirmed the inherent worth of the individual *qua* individual by guaranteeing their fundamental rights.[95]

Third, the emphasis upon individual empowerment is also evident through the conferral of rights to the individual as a pushback against the sovereign power of the State.[96] While State excesses of power have resulted in gross rights violations, the individual is generally able to hold the State accountable through a wide array of human rights which extend protection beyond physical violations to more 'intangible' harms such as violations of the right to privacy.

Fourth, the international protection of human rights is said to enable the operationalization of equality, demonstrating a 'robust commitment to affirming and protecting the equal basic moral status of all individuals'.[97] Thus, beyond reflecting the moral rights that individuals are said to possess inherently, ensuring equal worth in practice necessitates conferring individuals with equal legal rights. As Besson notes, '(h)uman rights are rights individuals have against the political community, i.e. against themselves collectively. They generate duties on the part of public authorities not only to protect equal individual interests, but also individuals' political status qua equal political actors.'[98]

Finally, the very nature of human rights as enforceable and justiciable individual legal rights confirms that the framework was designed with the normative goal of empowering individuals.[99]

It is thus clear that human rights aim to empower individuals by granting them a set of rights and ensuring that they can seek protection for those rights. The paradigm of individual empowerment is also observed in the digital age, including through the developing space of digital rights.[100] However, the deployment of AI-driven border and migration management may be challenging the idea of individual empowerment which lies at the core of the human rights protection framework in three ways.

3.2.1. Datafication

First, it is becoming increasingly onerous or even impossible to be aware of the process and to challenge the imputation of intentionality upon the individual through the use of AI systems. The use of risk classification systems and emotion and facial recognition systems by border security arguably makes it increasingly impossible for the individual to understand why and how they have been deemed a risk factor and to challenge such classification. Risk classification systems work

[94] ibid.

[95] ibid.

[96] CR Beitz, *The Idea of Human Rights* (OUP 2009) 129; C van Veen, 'Artificial Intelligence: What's Human Rights Got to Do with It?' (*Medium*, 18 May 2018) <https://medium.com/datasociety-points/artificial-intelligence-whats-human-rights-got-to-do-with-it-4622ec1566d5>; Buchanan (n 88) 16.

[97] Buchanan (n 88) 28; S Besson, 'The Law in Human Rights Theory' (2013) 7 ZMR 120.

[98] Besson ibid 139.

[99] Buchanan (n 88) 38–9; Buchanan (n 89) 245.

[100] European Commission, 'European Declaration on Digital Rights and Principles for the Digital Decade' (15 December 2022) <https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

based upon a form of profiling, categorizing individuals by the risk that they potentially pose to the country of destination. Such systems are based on the data provided by the individual but also via other means such as other data-based risk profiles and data gleaned from other systems. Due to the interoperability of such systems, allowing for the cross-checking of data to find 'hits', and the imperative of security that underpins the use of AI systems, the individual is no longer the central figure in the maze of datapoints. The datapoints in turn pertain not to the individual, as historically and biologically situated,[101] but to profiles constructed for the purposes of informing decision-makers such as the border and migration authorities. Given that these systems operate in securitized settings, the individual is unlikely to be aware of the content of their profile or how intentionality has been imputed to them, let alone have access to the subsequent recommendations made by the system. Van der Sloot argues that 'control is no longer feasible because of time and resources, but also because of information and power asymmetries: data is produced by data controllers and was thus never in the hands of an individual in the first place'.[102]

While machine learning AI systems have been long criticized as being 'black boxes', i.e. their internal processes are so complex or opaque it is impossible to understand how outputs are reached, the individual's lack of knowledge is not (only) due to computational impossibility but is compounded by political impossibility in the face of endemic secrecy in securitized settings such as border and migration management. Transparency, if even available, is likely only superficial and insufficient to empower the individual, typically from an already vulnerable or marginalized group, to challenge a decision or seek accountability. Another reason that has been used to justify the lack of transparency around algorithmic systems, including those used within the field of border and migration, is that transparency could ostensibly facilitate misuse of the system by those seeking to exploit loopholes or information provided.[103]

3.2.2. Inference and construction

Second, the difficulties of finding out how a decision is made and challenging it are exacerbated by the fact that it is not personal data per se that informs algorithmic decision-making, recommendations or forecasting, but rather algorithmic constructions of the individual's profile and inferences being drawn from that data. This 'profile' is thus by nature elusive and ever-changing, incorporating new datapoints as they are encountered, rendering it much harder to challenge. In effect, the individual is being judged not by their own personal data as such, but through acts, group profiling and the inferences therein. While data protection, privacy and human rights laws are generally applicable in the border and

[101] OH Gandy, 'Engaging Rational Discrimination: Exploring Reasons for Placing Regulatory Constraints on Decision Support Systems' (2010) 12 Ethics&InfoTechnol 29.

[102] B van der Sloot, 'The Production of and Control over Data in the AI-Era: The Two Failing Approaches to Privacy Protection' in A Quintavalla and J Temperman (eds), *Artificial Intelligence and Human Rights* (OUP 2023) 176.

[103] N Diakopoulos, 'Accountability in Algorithmic Decision Making' (Communications of the ACM, 1 February 2016) <https://cacm.acm.org/practice/accountability-in-algorithmic-decision-making/>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

migration setting, the operationalization of these protections faces certain novel difficulties. The use of AI systems such as algorithmic assessments of the risk profiles of various travellers represents not only a novel way to 'read' subjects, but, as Van den Meerssche observes, it is in effect a new form of subject *creation*.[104] Subject construction means that 'data flows, bodies and scattered signatures of past passages or events are assembled as scores amenable to immediate institutional action'.[105] This ephemeral form of subject making challenges the subject's capacity to know what data is out there about them and how it is processed, and could be framed as a form of 'hermeneutic injustice', described by Milano and Prunkl as the 'depletion of epistemic resources that are needed to interpret and evaluate certain experiences'.[106] Such disempowerment of the individual in relation to their creation as an AI 'subject' also contravenes the 'emancipatory promises of collectivity, solidarity and equality'[107] of international law, including human rights law. The generation of a profile from many types and sources of data also does not fall squarely within the ambit of data protection law, which is concerned with the identifiability of existing subjects.

3.2.3. Algorithmic groupings

The third way that AI systems disempower individuals stems from the fact that algorithmic profiles pertain not to the individual at all, but rather to groups. Algorithmic predictions and recommendations, even if applied to the individual, are essentially the result of groups created by inference based upon shared algorithmic patterns. It has been argued that: 'in an era of big data where analytics are being developed to operate at as broad a scale as possible, the individual is often incidental to the analysis'.[108] Algorithmic group-based correlations enable actionability based upon the insight they afford in relation to the population as a whole.[109] This is fundamentally at odds with the interpretation of human rights as being premised upon individual empowerment. While there are attempts to broaden human rights protections to include group privacy and expand the basis of non-discrimination law, there are still unresolved issues in relation to 'group rights', such as which groups are deserving of protection, how a group can be identified when its contours are constantly shifting[110] and where the threshold for what constitutes a group should lie.[111]

There is a general counterargument that can be offered to the assertion of disempowerment of the individual by AI systems. It can be argued that the human

[104] Van Den Meerssche (n 1).

[105] ibid 173.

[106] S Milano and C Prunkl, 'Algorithmic Profiling as a Source of Hermeneutical Injustice' (27 December 2023) <https://philpapers.org/versions/MILAPA-8>.

[107] Van Den Meerssche (n 1) 171.

[108] L Taylor, L Floridi and B van der Sloot, 'Introduction: A New Perspective on Privacy' in L Taylor, L Floridi and B van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2017) 10.

[109] S Viljoen, 'A Relational Theory of Data Governance' (2021) 131 YaleLJ 82.

[110] B Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Phil&Technol 475.

[111] S Wachter, 'The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law' (2022) 97 TulLRev 149.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

rights framework is not centred upon the empowerment of the individual as such, but rather, it puts in place a protection mechanism that aims at securing a minimum standard of protection to prevent the worst human rights excesses.[112] However, as will be examined in Section 3.3, the minimum level of protection offered by human rights law serves the underlying purpose of the protection and realization of human dignity. Individual empowerment is a necessary ingredient for the realization of human dignity as individual autonomy is one of its key components.

In summary, it is clear that the use of AI systems within the border and migration context has the effect of disempowering the individual and is exacerbated by the turn to securitization. The lack of transparency is not only inherent to such systems, but is also necessary for their proper functioning. This differentiates the border and migration context from many other contexts in which AI systems are deployed, where transparency has been hailed as a key element in empowering the individual in understanding and challenging algorithmic decision-making, for example, within public administration where good governance principles are built upon transparency.

3.3. Politicising human dignity

This section delves into how human dignity, a key foundational concept within human rights, is being politicized and undermined. The 1945 United Nations Charter recognized the 'dignity and worth of the human person'[113] and this was subsequently reflected in the UDHR in 1948 which affirmed that 'all human beings are born free and equal in dignity and rights'.[114] The concept itself is open ended and its philosophical and historical provenance has seen human dignity being interpreted variously as not treating humans as a means to an end,[115] as protection of certain vulnerable classes of persons[116] and as recognizing the distinct capacities of humanity, including reasoning capacities of the human mind.[117] Human dignity has been described as the 'the foundation on which the superstructure of human rights is built',[118] and the very reason why we protect human rights.

The openness of the concept might intuitively convey its correspondingly open and evolving utility, even in light of new challenges to human rights. Thus, even putatively novel challenges such as environmental harms have been couched within the language of human dignity.[119] Human dignity has also been a relevant concern

[112] S Moyn, *Not Enough: Human Rights in an Unequal World* (Harvard University Press 2018).

[113] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) preamble.

[114] UDHR (n 52) art 1.

[115] I Kant and CM Korsgaard, *Kant: Groundwork of the Metaphysics of Morals* (M Gregor ed, CUP 1998).

[116] *Pretty v UK* (n 67).

[117] SA Teo, 'Human Dignity and AI: Mapping the Contours and Utility of Human Dignity in Addressing Challenges Presented by AI' (2023) 15 LIT 241.

[118] R Brownsword, 'Human Dignity from a Legal Perspective' in D Mieth et al (eds), *The Cambridge Handbook of Human Dignity: Interdisciplinary Perspectives* (CUP 2014) 3.

[119] E Daly and JR May, 'The Indivisibility of Human Dignity and Sustainability' in CG Gonzalez, SL Seck and SA Atapattu (eds), *The Cambridge Handbook of Environmental Justice and Sustainable Development* (CUP 2021) 23.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

when it comes to AI systems.[120] However, others have criticized the human rights discourse for being shortsighted in its response to new challenges. Rodríguez-Garavito argues that human rights responses have tended to 'register the earthquake but lose sight of the tectonic plates that are shifting beneath the surface',[121] pointing to foundational concerns that are either missed or neglected.

This section puts forward three arguments as to how the use of AI within border and migration management contexts poses a normative problem for the human rights framework by failing to address the politicization of human dignity and the inherent worth of the human being.

3.3.1. Exacerbated exclusion in the border and migration context

First, while acknowledging that migration is an inherently exclusionary context that engages with the sovereign power of the State to determine who may or may not enter their territory, the use of AI systems in such determinations may exacerbate power inequalities and result in the disproportionate exclusion of certain ethnicities, races and nationalities.[122] While sovereign States have an almost exclusive power—barring international obligations such as protections afforded under refugee law and human rights law—to determine who they want to have within their borders,[123] this discretion is not unfettered. The use of AI in border and migration management can result in both direct and indirect discrimination, and at the same time impacts not only the individual but also effectively builds discriminatory structures and leaves them in place. Thus, even though the use of AI is pervasive within different segments of society and public administration, the border and migration context bring forth unique concerns.

To mitigate these concerns, the lens of human dignity has been deployed to cast a wider net of protection. For example, the European Data Protection Board (EDPB) Joint Opinion with the European Data Protection Supervisor (EDPS) on Artificial Intelligence called for a ban on 'any use of AI for an automated recognition of human features in publicly accessible spaces – such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals'.[124] Similarly, the Opinion also called for a ban on the inference of emotions from natural persons such as through emotion AI systems. These systems were argued to impact human dignity detrimentally as individuals are computationally read and

[120] European Data Protection Board and European Data Protection Supervisor (EDPB-EDPS), 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (EDPB, 18 June 2021) <https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en>.

[121] C Rodríguez-Garavito, 'ChatGPT: What's Left of the Human in Human Rights?' (*OpenGlobalRights*, 25 May 2023) <https://www.openglobalrights.org/chatgpt-whats-left-human-rights/>.

[122] K Weitzberg and R Pakzad, 'Primer: Defending the Rights of Refugees and Migrants in the Digital Age' (Amnesty International 2024) POL 40/7654/2024; 'Racial and Xenophobic Discrimination and the Use of Digital Technologies in Border and Immigration Enforcement: Report of the Special Rapporteur on contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, E. Tendayi Achiume' (17 December 2021) UN Doc A/HRC/48/76.

[123] Buchanan (n 89) 259. The right to asylum is also guaranteed under art 18 of the CFR (n 52).

[124] EDPB-EDPS (n 120) para 32.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

thereby may have their life opportunities 'determined or classified by a computer as to future behaviour independent of one's own free will'.[125] The calls for banning such systems, including through civil society efforts, have not been taken up in the EU's groundbreaking AI Act.[126] However, the AI Act does classify AI systems used within the border and migration context as high risk, meaning operators will be subject to obligations on ensuring robustness, cybersecurity, data governance, data quality and bias, amongst others.[127]

However, even the strong language of human dignity is unable to stop the systemic incursions of these technologies into human rights due to two evolving transformations. First, the lines between security and migration have been and continue to be increasingly blurred. The border and migration space is witnessing the combination of security-focused systems with migration-focused systems, including through the interoperability of large-scale IT systems. Blasi Casagran notes that border management systems such as EES, VIS, Eurodac and systems with distinct security logics such as ECRIS-TCN are now part of the interoperability framework. SIS, also part of the interoperable system, was the only system initially designed to straddle both border management and security. In effect, the enmeshing of these initially distinct objectives means that the EU can in effect 'treat the objective of border management and the objective of police cooperation as one single general purpose'.[128] In criticizing the expanding reach of these interlinked databases, the EDPS has argued that surveillance capture is too wide as it 'will put everyone trying to enter the EU under broad surveillance, when in fact they were designed to only catch a small minority of criminals'.[129] This leaves even the powerful language of human dignity unable to scale the high walls erected by the securitization lens.

In addition to the line between security and migration being blurred, the lines between asylum and refugee protection and migration management in general are also being blurred. Even though border and migration management falls under the high-risk designation in the AI Act, the categorization does not distinguish the distinctive elements at play, especially in relation to the heightened international legal obligations of the State when it comes to the protection needs of asylum seekers and refugees. In seeking to assess the risk of AI systems in the different use cases and sectors, the EU ended up compressing distinct State obligations relating to borders and migration into the same risk bucket. Doing so inadvertently entwined two distinct concerns with separate governing mechanisms, for example,

[125] ibid para 34.

[126] B Goodwin, 'Joint Statement: The EU AI Act Must Protect People on the Move' (European Civic Forum, 6 December 2022) <https://civic-forum.eu/statement/joint-statement-the-eu-ai-act-must-protect-people-on-the-move>.

[127] AI Act (n 11) art 6(2) and Annex III on high-risk AI systems and section 2 for requirements of high-risk AI systems.

[128] Blasi Casagran (n 7) 434.

[129] W Wiewiórowski, 'Privacy and Data Protection Too Often Suspended at EU Borders' (www.euractiv.com, 27 January 2023) <https://www.euractiv.com/section/data-privacy/opinion/it-is-time-to-tear-down-this-wall/>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

someone claiming refugee status has different needs and legal concerns to those of a third-country national attempting to visit the EU.

A key element of refugee law protection is the concept of non-refoulement which prohibits States from returning refugees to countries where they may face persecution or threats to their life or freedom.[130] The principle of non-refoulement is argued to have *jus cogens* status and cannot be overridden by a generalized (and ever-expanding) securitization imperative.[131] Refoulement can be facilitated through AI forecasting technologies where they have been used to interdict migratory flows and facilitate pushbacks, instead of enabling better planning of asylum assistance.[132] This facilitates a form of 'digital refoulement'.[133] For dignity and human rights to be respected effectively, the non-derogability of *jus cogens* norms must be reinforced to prevent the use of certain intrusive AI technologies such as emotion recognition and biometric facial recognition in migration management that threaten the principle of non-refoulement, and the detriment to human dignity that such treatment entails.[134]

3.3.2. Inherent worth and AI-determined abnormalities

The inherent worth of human dignity is also being politicized through the AI-driven determination of the boundaries of normality versus abnormality. Border crossings and airport security checks involve intrusive forms of anomaly detection, including physicality-related anomalies. Security concerns are once again pertinent, in that these checks are deployed to ensure that no one is transporting banned or illegal items and substances that could endanger the security of many. However, at sites of border control, it has also been seen that bodies which do not fit into the binary male–female mould are singled out for scrutiny and undignified forms of examination.[135] In addition, disabled bodies have also triggered AI systems to suggest the need for human intervention, demonstrating a disproportionate impact

[130] Convention Relating to the Status of Refugees (adopted 28 July 1951, entered into force 22 April 1954) 189 UNTS 137 (Refugee Convention) art 33(1); CFR (n 52) art 19(2).

[131] Exceptions to the principle of non-refoulement are found under art 33(2) of the Refugee Convention ibid. The provision states that '(t)he benefit of the present provision may not, however, be claimed by a refugee whom there are reasonable grounds for regarding as a danger to the security of the country in which he is, or who, having been convicted by a final judgement of a particularly serious crime, constitutes a danger to the community of that country'. This requires individual assessments and scholars have also called for other measures, such as prosecution in the host country, in order to respect the *jus cogens* nature of non-refoulement. See e.g. R Bruin and K Wouters, 'Terrorism and the Non-Derogability of Non-Refoulement' (2003) 15 IJRL 5.

[132] Papachristodoulou (n 7); Office of the High Commissioner for Human Rights, 'Report on Means to Address the Human Rights Impact of Pushbacks of Migrants on Land and at Sea' (12 May 2021) <https://www.ohchr.org/en/special-procedures/sr-migrants/report-means-address-human-rights-impact-pushbacks-migrants-land-and-sea>; Martínez (n 1); Euro-Med Human Rights Monitor, 'Greece: Illegal Pushbacks Are Dooming Migrants to Freeze to Death' (3 February 2022) <https://euromedmonitor.org/en/article/4887/Greece:-Illegal-pushbacks-are-dooming-migrants-to-freeze-to-death>.

[133] A Fill, 'Pushbacks, Pullbacks, Backscattering: Evolving Forms of Digital Refoulement at the EU Borders' (*Security Praxis*, 6 November 2020) <https://www.securitypraxis.eu/digital-refoulement-eu-borders/>.

[134] Although Recital 60 of the AI Act (n 11) stressed that States are to uphold their international obligations in relation to refugee law, the rest of the recital fails to distinguish the mobility of third-country nationals from the rights of refugees and asylum seekers.

[135] S Costanza-Chock, *Design Justice: Community-Led Practices to Build the Worlds We Need* (MIT Press 2020) 1–5.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

on the rights of persons with disabilities.[136] The classification of bodies as normal or abnormal signifies that there is a range of normality in terms of what is acceptable within highly securitized settings, perpetuating 'ableism, inequality, and other harms'.[137] It has been criticized that: 'biometric technologies across the matrix are used to create baselines of what constitute "normal" behaviours and bodies, which further reinforces unequal treatment of people whose bodies and behaviours do not adhere to this normative frame'.[138]

In addition to policing 'normal' ranges of external attributes, AI systems such as biometric facial and emotion recognition systems also create an algorithmically determined 'acceptable' range of emotions, micro-expressions and movements to analyse internal attributes. Those not falling within the acceptable range raise the potential of being singled out as displaying 'biomarkers of deception',[139] often without their knowledge. Thus, both bodies and intimate aspects of a person's existence such as emotions are 'informatized',[140] ostensibly revealing hidden intention.

The 'datafication' of human movements, expressions and micro-expressions poses a significant challenge for human dignity as it reduces individuals to datapoints, potentially undermining their autonomy, privacy and the presumption of innocence. An individual who possesses dignity and autonomy should fundamentally be empowered to govern themselves and make choices within their own life. For this to be possible, data concerning them has to be accessible and knowable, but instead datafication places trust in ostensibly neutral technology, whereby 'as a multiplicity of inscriptions are produced, migrants' claims can be disqualified through circumscriptions of data and ascriptions of expertise'.[141] It is the datafied individual that is judged, rather than the actual individual, whose human dignity is detrimentally impacted by the inability to know how their micro-expressions, emotions or gestures are profiled, or how these are seen as security threats or otherwise, thus rendering challenging such decisions impossible.

3.3.3. Possibility of solidarity and resistance

The final challenge for human dignity presented by AI systems used within the border and migration management setting is the impact it has on dignity as human flourishing, enabled through practices such as social solidarity or resistance (towards practices deemed as unjust).

[136] The UN Special Rapporteur on the Rights of Persons with Disabilities, Gerard Quinn, has also raised concerns regarding misinterpretation of facial expressions and recommended for a moratorium on such tools until human rights respecting measures and safeguards are in place. See 'Rights of Persons with Disabilities: Report of the Special Rapporteur on the Rights of Persons with Disabilities' (28 December 2021) UN Doc A/HRC/49/52.

[137] X Wang and S Ahmed, 'Bodily Harms: Mapping the Risks of Emerging Biometric Tech' (Access Now, 2023) 4 <https://www.accessnow.org/wp-content/uploads/2023/10/Bodily-harms-mapping-the-risks-of-emerging-biometric-tech.pdf>.

[138] ibid.

[139] Sánchez-Monedero and Dencik (n 12).

[140] I van der Ploeg, 'Genetics, Biometrics and the Informatization of the Body' (2007) 43 AnnIstSuperioreSanita 44.

[141] S Perret and C Aradau, 'Drawing Data Together: Inscriptions, Asylum, and Scripts of Security' (2023) 49 SciTechnol&HumValues 4, 739.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

First, even though the EU's AI Act sets the tone as the first comprehensive AI legislation, the large-scale IT systems[142] used in border and migration control, including their inter-operationalization, are exempted from the initial coverage of the Act. Rather than being obliged to be brought into compliance by 2 August 2027 like other AI systems already in operation, these systems have until 31 December 2030.[143] This practice indirectly introduces a two-tiered application of human rights in relation to AI in the EU, with migrants' rights apparently protected in the AI Act, but that protection being limited in practice. Civil society groups have criticized this as it 'reinforces the notion of a differential approach to fundamental rights when migration is the subject matter and people on the move are the right-holders'.[144]

While the securitization logic is one element of this two-tiered rights application, the exclusion of these large-scale IT systems reflects the fact that trust in technology within the field of border and migration is essential, and the widespread acceptance that 'AI common sense'[145] can better forecast, assist in decision-making and determine truth or falsity to facilitate the management of human mobility than the testimony of migrants themselves. This form of technological determinism does away with the notion of the primacy of the human being and their own agency in shaping their destinies, as technological insights gleaned from AI systems are seen as better indicators of trustworthiness, reliability or deceit.[146]

Solidarity and resistance can also be curtailed through the generation of 'invisibilities' by AI systems. As shown in Section 3.2, the way AI systems operate in making generalizations and drawing inferences does not necessarily correspond to socially salient concepts (such as age or gender) or fall within the protections offered by the law, such as non-discrimination law.[147] Instead, the data-driven inferences and categorizations of individuals take place outside of the individual's frame of reference and are thus 'invisible', both as a result of this data-driven nature, but also because operational details are intentionally kept confidential to deter attempts to circumvent their mechanisms.[148] Mann and Matzner agree and argue that 'emergent categories are also "invisible" from the point of view of existing anti-discrimination protection. It becomes an invisible production of invisibilities.'[149] These invisibilities can generate new vulnerabilities and vulnerable groupings, as opposed to merely falling within existing categories of vulnerable groups.[150] Beyond non-discrimination law, this creates a new challenge for

[142] AI Act (n 11). Art 111 notes that large-scale systems are those established by the legal acts listed in Annex X.

[143] ibid art 111(1).

[144] Access Now et al (n 7).

[145] Aradau (n 16).

[146] Sánchez-Monedero and Dencik (n 12).

[147] Wachter (n 111).

[148] Pasquale (n 22).

[149] M Mann and T Matzner, 'Challenging Algorithmic Profiling: The Limits of Data Protection and Anti-Discrimination in Responding to Emergent Discrimination' (2019) 6 BigData&Soc 7.

[150] J Gerards and F Zuiderveen Borgesius, 'Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence' (2022) 20 ColoradoTechnolLJ 3.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

individual autonomy that is central to human dignity. How does one resist, challenge and gather solidarity around invisibilities when these are neither made evident to the individual nor known to others also subjected to such algorithmic readings? Van der Sloot argues that the legal forms of resistance and accountability, through the right to privacy and data protection law, are ill-prepared to address the changing ways in which knowledge is now produced through AI systems. Thus, individual knowledge and control over data have now been overtaken by datafication that enables algorithmic groupings, and the individual self-narrative has been replaced by reliance upon observed data.[151]

The generation of invisibilities in this manner can make solidarity through shared experiences and challenging such experiences much more onerous. Prior forms of solidarity building in relation to human rights concerns, such as the suffragette movement, the LGBTQI+ (lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and more) movement and others, all relied upon a shared sense of injustice and mobilization against an identifiable cause. As AI systems generate invisibilities, such forms of shared solidarity and resistance can no longer be taken for granted. The data-driven groupings and inferences created by AI systems are atomized to each individual, making it difficult to form alliances. Such invisibilities benefit the party deploying the AI system as they not only have exclusive control over knowledge about how the system functions, but they can also prevent others from effectively understanding how various datapoints are used to infer certain characteristics about individuals subjected to the system. Where individuals and communities have successfully challenged the experimentation and use of technologies, these challenges were built upon effective knowledge, shared experiences and a shared sense of injustice, which are impossible in this context, thus preventing the full realization of human dignity. Scholarship has suggested various means to address the generation of such invisibilities, including calling for more transparency, proposing for protections for new 'artificial' groups[152] and for the burden of (dis)proving harms to move from the individual to the deployer.[153] Others have called for *a priori* solidarity, namely through refusal in being made algorithmically reducible and readable through AI systems.[154]

The concept of human dignity is being relied upon in re-asserting the primacy of the human being and in protecting the inherent worth of the individual person. As noted in Sections 3.3 and 3.3.1 above, the EDPB and EDPS used the language of human dignity to reassert the primacy of the individual when they called for a ban on the use of biometric facial recognition systems.[155] Human dignity can also be considered as an implicit motivation for the ban on certain types of AI systems under the EU's risk-based approach to AI regulation. In Recital 28 of the AI Act, banned AI systems such as those used for social scoring or which manipulate or exploit are said to 'contradict Union values of respect for *human dignity*, freedom,

[151] Van der Sloot (n 102).

[152] Wachter (n 111).

[153] H Weerts et al, 'Algorithmic Unfairness through the Lens of EU Non-Discrimination Law: Or Why the Law is not a Decision Tree' in *2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23)*, June 12–15, 2023, Chicago, IL, USA (Association for Computing Machinery 2023).

[154] Van Den Meerssche (n 1).

[155] EDPB-EDPS (n 120).

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

equality, democracy and the rule of law and fundamental rights'.[156] It can thus be reasoned that a red line is being drawn concerning AI systems that bring forth particular harms that threaten the foundational idea of human dignity. At the same time, however, the list of banned versus high-risk and limited-risk categories has been criticized as unsustainable and a legal fiction.[157] For example, the fact that emotion recognition systems are banned if deployed within the education and workplace settings, but not within even more consequential fields such as law enforcement and border and migration management (which fall under the category of high-risk AI), warrants examination. If power disparities and the potential for abuse are the justifications given, it is clear that there is even greater potential for these issues to arise in relation to law enforcement and borders and migration. Thus, while attempts have been made to draw a red line by banning some AI use cases, there are internal tensions and lack of clarity as to why some systems are banned or classified as high risk for certain uses whilst others are not.[158]

Although the drawing of a red line is commendable, policymaking should also be informed by the 'hidden' impacts of AI raised in Sections 3.1 to 3.3. Some successful legal developments indicate that there is hope on the horizon. The EDPS has criticized the use of forecasting technologies, including social media data, in ways that go against the purpose limitation within data protection law, whereby data gathered can only be used for specific purposes and not unknown future uses.[159] The Court of Justice of the EU, in its judgment in the *PNR* case,[160] stated that automated decision-making for risk assessment purposes had to respect the individual's right to privacy and data protection under the EU Charter of Fundamental Rights.[161] The Court argued that the transfer, processing and retention of passenger name record (PNR) information under the PNR Directive[162] must be limited to what is strictly necessary and rejected the use of self-learning systems to determine the result of the application or in the weighting of the criteria used for identification. In the UK, the use of an algorithmic system to allocate different 'streams' to visa applicants was found to be racist and discriminatory towards minority populations and was subsequently scrapped.[163]

[156] AI Act (n 11) Recital 28 (emphasis added).

[157] M Veale and F Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act—Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 ComputerLRevIntl 97.

[158] ibid.

[159] EDPS, 'Formal Consultation on EASO's Social Media Monitoring Reports (Case 2018-1083)' (14 November 2019) <https://www.edps.europa.eu/data-protection/our-work/publications/consultations/social-media-monitoring-reports_en>.

[160] Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491 (*PNR* case).

[161] J Gerards, 'Machine Learning and Profiling in the PNR System' (*Verfassungsblog*, 8 May 2023) <https://verfassungsblog.de/ml-pnr/>.

[162] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132 (PNR Directive).

[163] H McDonald, 'Home Office to Scrap "Racist Algorithm" for UK Visa Applicants' *The Guardian* (London, 4 August 2020) <https://www.theguardian.com/uk-news/2020/aug/04/home-office-to-scrap-racist-algorithm-for-uk-visa-applicants>.

https://doi.org/10.1017/S0020589325000090 Published online by Cambridge University Press

These examples demonstrate that while the deployment of AI systems is increasing throughout the border and migration setting, legal challenges can successfully be mounted to halt certain problematic uses of such systems. However, more scrutiny going beyond these discrete legal challenges is required in this field. Ongoing vigilance in relation to evolving harms and their 'hidden' impacts on human rights and human dignity can be maintained through tools such as human rights impact assessments. Also, more thorough stakeholder engagement in relation to the design and deployment of AI systems is necessary, including with particularly affected groups such as refugees, migrants and asylum seekers or civil society representatives. In turn, systems posing a disproportionate threat to human dignity should be banned. Policymaking should thus be informed not only by the familiar concept of threats to human rights, but also by the deeper implications of these concerns for the foundational elements of the human rights framework.

4. Conclusion

The deployment of AI systems in border and migration control can challenge not only the protection of specific human rights but also threaten the foundational and normative principles of the human rights framework. This article has demonstrated that the use of AI systems within the field of border and migration management is challenging human rights in novel ways, going beyond the oft-cited concerns for privacy, data protection and non-discrimination. It has shown how the freedom of thought can be compromised in new ways through AI systems that read and construct interpretations, including through biometric and emotion data, ostensibly to reveal suspicion or threat and therein impute intentionality upon the individual. The expanding use of AI within the border and migration context can also undermine the power of the individual to address disparities, and challenges even the wide concept of human dignity that is foundational to the human rights discourse. In addition, a data-based reading of an already vulnerable person can generate new threats to solidarity and mobilization and pre-empt resistance. As AI systems have transformed physical borders into digital ones, and redrawn boundaries between biometrics, intentionality and criminality, a need to reinvigorate and protect human dignity in the age of AI systems has arisen. This is essential to safeguard the foundational principles of human rights in an increasingly technologized (and mobile) world.

Acknowledgements. This paper was written within the framework of the Raoul Wallenberg Visiting Chair Project (2021–2025), *The Future of Human Rights*, a collaboration between the Faculty of Law at Lund University and the Raoul Wallenberg Institute of Human Rights and Humanitarian Law. The authors gratefully acknowledge the support provided by both institutions.

Cite this article: A Rinaldi and SA Teo, 'The Use of Artificial Intelligence Technologies in Border and Migration Control and the Subtle Erosion of Human Rights' (2025) ICLQ 1–29. https://doi.org/10.1017/S0020589325000090