Discover Computing

Review

Decoding accountability: the importance of explainability in liability frameworks for smart border systems

Uchenna Nnawuchi[1] · Carlisle George[1]

Received: 30 November 2024 / Accepted: 15 April 2025
Published online: 04 May 2025

Abstract

This paper examines the challenges posed by Automated Decision-Making systems (ADMs) in border control, focusing on the limitations of the proposed AI Liability Directive (AILD)—now withdrawn– in addressing potential harms. We identify key issues within the AILD, including the plausibility requirement, knowledge paradox, and the exclusion of human-in-the-loop, which create significant barriers for claimants seeking redress. Although now withdrawn, the commission is contemplating putting up a new proposal for the AI Liability regime; if the new proposal is anything like the AILD (now withdrawn), there is a need to address the substantial shortcomings discovered in the AILD. To address these shortcomings, we propose integrating sui generis explainability requirements into the AILD framework or mandatory compliance with Article 86 of the Artificial Intelligence Act (AIA), notwithstanding its ineffectiveness. This approach aims to bridge knowledge and liability gaps, empower claimants, and enhance transparency in AI decision-making processes. Our recommendations include expanding the disclosure requirements to incorporate a sui generis explainability requirement, implementing a tiered plausibility standard, and introducing regulatory sandboxes. These measures seek to engender accountability and fairness. With the refinement of the AILD in mind, these considerations aim to influence and make recommendations for any future proposals for an AI liability regime and to foster a regulatory environment that encourages both the development and use of AI technologies to be responsible and accountable, ensuring that AI-driven or smart border control systems enhance security and efficiency while upholding fundamental rights and human dignity.

1 Introduction: the intersection of AI, border security, and accountability

Artificial Intelligence (AI) is increasingly shaping how individuals are monitored and assessed. For example, in border control, the introduction of AI systems has led to the development of "smart borders," enhancing surveillance and operational efficiency while raising important questions about accountability, fairness, and human rights. Border control agencies now rely on various advanced technologies, including surveillance drones [1], robotic dogs [2], and large biometric databases, which can track and identify individuals with greater precision. These tools enable unprecedented tracking and analysis of migrants' journeys, utilising fingerprints, retina scans, blood and vessel pattern recognition, facial recognition, and even ear and gait analysis [3]. The integration of AI has accelerated the processing of immigration and refugee cases [3], with algorithms now being employed to predict human behaviour, determine aid delivery, and even detect deception at border crossings through "algorithmic lie detectors [4]." Concomitantly, decisions such as whether to grant a visa or detain someone, which would otherwise be made by administrative

✉ Uchenna Nnawuchi, UN055@live.mdx.ac.uk; Carlisle George, c.george@mdx.ac.uk | [1]ALERT Research Group, Department of Computer Science, Faculty of Science and Technology, Middlesex University, London, UK.

tribunals, immigration officers, border agents, legal analysts, and other officials, are increasingly supported or made entirely by AI, often through Automated Decision-Making Systems (ADMs) [4]. This shift is already occurring in certain border control agencies, such as immigration, though the extent of automation compared to human involvement can vary. According to the Working Party 29 [5], "For a decision to be considered as made by a human, the human must have meaningful involvement in the decision-making process. This means that the decision should not be the result of an automated process alone, and humans should be able to assess the situation. Human involvement should not be reduced to merely approving or ratifying an automated decision without meaningful engagement." Despite this, in many immigration systems, the opacity of these algorithms makes it challenging for human agents to engage with or fully comprehend the reasoning behind the decisions [6]. As a result, many immigration officers may find their role reduced to rubber-stamping decisions made by the algorithm, effectively serving as a formality rather than exercising meaningful judgment [7].

While these ADMs are intended to enhance efficiency and security by reducing waiting times and more effectively targeting interventions, they also raise important concerns about the loss of human judgment in critical decision-making processes. ADM systems —ranging from Emotion Recognition Systems (ERS) to advanced surveillance and data analytics [8]— aim to improve border control by detecting illicit activities such as smuggling and terrorism [9], ultimately strengthening national security [10]. However, the automation of decision-making in these contexts must be carefully balanced with adequate human oversight to prevent unintended consequences, such as errors in judgment or lack of accountability, which could undermine public trust and justice in the immigration process. For example, consider a situation where an individual arrives at the UK border and undergoes screening through the iBorderCtrl system. The system, which uses AI to assess risk based on biometrics and travel history, incorrectly flags the individual as high-risk due to a data error—her profile is mistakenly matched to that of a previously flagged person with a similar name. As a result, the individual is detained for additional questioning, and her entry is delayed. Despite having a clean record and no connections to the flagged individual, the system's error causes a false positive, leading to unnecessary distress, a violation of her right to liberty, and a delay in her business trip. More troubling, however, is the difficulty in challenging the decision, as the individual cannot comprehend or understand why he/she was flagged by the system. Such incidents could significantly erode public trust in the use of these technologies.

Furthermore, these smart systems present significant and nuanced risks. The technical autonomy of AI systems can generate unexpected outputs that even their creators cannot fully anticipate or comprehend. Deep learning models, characterised by their complex and opaque decision-making processes, create substantial challenges in understanding how specific conclusions are reached. The absence of transparency makes it extremely difficult to determine liability or trace causal relationships when AI systems produce problematic, biased or erroneous outputs [11]. This undermines transparency and exacerbates power asymmetries between state authorities and individuals. In the context of migrant control, such AI systems with obscured decision-making processes potentially perpetuate systemic human biases and diminish the individuals' (migrants) ability to understand and appeal administrative decisions that directly affect their legal status, mobility, and fundamental rights [12]. Additionally, these concerns about perpetuating or exacerbating illegal discrimination through biased training data or incorrect target variables necessitate a comprehensive regulatory approach that mandates explainability features, expands disclosure requirements, and implements a tiered plausibility standard to address knowledge gaps and empowers claimants in AI-driven border control systems [12]. Undoubtedly, these issues without a comprehensive regulatory framework erode trust and potentially compromise fundamental rights, including liberty, privacy and due process, raising substantial questions about accountability, responsibility, and liability in designing, deploying and operating AI-driven border technologies.

Consider, for instance, the use of ADMs such as ERS like iBorderCtrl in our example above and risk assessment tools ostensibly designed to streamline border checks and expedite migration processes. They raise critical questions such as who is held accountable if these smart systems misinterpret a migrant's emotional state or linguistic background, leading to unjust detention or denial of entry; who bears responsibility when a smart system generates a decision that unjustly impacts a migrant's life and under what condition were such decisions made [13]. Also, how can we ensure that the black box nature of these technologies does not become a shield against liability for border agencies (users) or technology providers, and how can legal recourse be established, particularly when algorithmic opacity in decision-making obscures the precise mechanisms of harm and potentially fragments responsibility across several actors including system developers, data scientists, administrative authorities, and system users. These questions cut to the heart of migrants' evolving relationship with AI in sensitive domains like border control.

As AI increasingly interferes with decision-making processes in border management, traditional liability frameworks appear ill-equipped to address potential harms in a way that is unique to this technology. While AI may reduce overall processing times and enhance security measures [9], it may also eliminate the ability of those wronged by these systems to seek recourse or compensation [14]. This tension underscores the need for new approaches to accountability, potentially including interpretability and transparency requirements for AI technologies used in border control. To address the challenges posed by AI technologies, the European Union (EU) Commission adopted the Artificial Intelligence Act (AIA) in 2021 [15], which came into force on August 1st, 2024 [16]. The Commission acknowledges that although the AIA aims to mitigate risks to safety and fundamental rights, it does not prevent AI systems that pose residual risks from being marketed [17]. The AIA offers a comprehensive regulatory framework and oversight mechanisms to prevent AI-related risks but remains silent on what happens when harm occurs [18][1] save for the bare establishment of an explicit legal right to explanation concerning high-risk systems in Art 86. Additionally, it is fitting to state that Article 86 has been criticised for being inadequate and non-operative. It has been argued that this right is in name only and does not serve any utilitarian purpose because it does not provide any mechanism, procedure, or blueprint for activating and enforcing the right [19]. Thus, Art 86 AIA is regarded as toothless [19].

In response to this gap in the AIA, the Commission proposed a two-pronged liability regime: the now-withdrawn AI Liability Directive (AILD) [20], designed to assist potential claimants in making non-contractual, fault-based claims, alongside a revised version of the existing Product Liability Directive (PLD) [21], which modernized the EU's non-contractual strict liability claims to compensate for damages caused by AI systems [15]. The former AILD is still in its draft form and yet to be considered by the European Parliament and Council of EU, whereas the latter PLD has been adopted by the EU and came into force on December 9th, 2024 [22].

Notably, the AILD and PLD frameworks establish rules requiring those in possession of relevant evidence of a defective product to disclose it, which not only facilitates establishing liability but also encourages compliance with the AIA's documentation and recording requirements.[2]

This paper focuses primarily on the AILD and its fault-based liability regime, as it offers a more relevant framework for addressing harms caused by the application of ADMs, *id est* post-algorithmic harm. Unlike the PLD, which is limited to economic operators [23], the AILD applies to manufacturers and professional and non-professional users, including public agencies and the state. Additionally, the AILD recognises violations of fundamental rights as compensable harms [24], making it a more comprehensive tool for addressing the unique challenges posed by ADMs in sensitive contexts like border control.

This paper delves into the complex relationship between explainability and liability within the realm of smart border systems. It begins by exploring the current landscape and application of AI-driven technologies, specifically ADMs, in border control, followed by a critical assessment of the AILD to identify gaps in providing adequate redress for migrants impacted by algorithmic decisions. The discussion then explores the integration of a sui generis explainability requirement in liability frameworks to bridge the gap identified in the AILD and the AIA, with a focus on fostering transparent and equitable border management practices. This paper also explores the impact of explainability requirements on IP rights and security and how these priorities can be balanced. This explainability requirement is unique to the AILD, especially because we consider Article 86 to be inoperative. In the alternative, we argue for mandatory compliance with Article 86 to be included in the AILD alongside an enforcement and procedural mechanism to make it operational within the context of AILD. This integration is crucial for safeguarding the rights and dignity of migrants while ensuring that both AI developers and users are held accountable. The paper concludes with advocating for balancing accountability and innovation in this rapidly evolving field. Thus, with the potential refinement of the AILD in mind, these recommendations aim to influence and make recommendations for any future proposals for an AI liability regime and to foster a regulatory environment that encourages both the development and use of AI technologies to be responsible and accountable, ensuring that AI-driven or smart border control systems enhance security and efficiency while upholding fundamental rights and human dignity.

[1] Art 1 and 2 AIA.

[2] Art 18 and 19 AIA.

2 Understanding smart border systems: technologies and applications

The opacity of ADMs such as risk assessment tools and ERS raises significant ethical and legal concerns about their impact on migrants [25]. Risk assessment tools like the Visa Information System (VIS) and the European Travel Information and Authorisation System (ETIAS) analyse risk profiles for migrants to the Schengen area [25]. VIS despite its capacity for automated processing of information, does the same manually, whereas ETIAS issues travel authorisations automatically unless flagged [26]. Despite their advanced capabilities, these systems struggle with transparency. Understanding why an individual is flagged by any of these systems can be elusive to the migrant and is therefore a major issue [8]. Another issue which is even more worrisome, is the difficulty in identifying who is liable when these systems inaccurately flag an individual. The cumulative effect of opacity and the concept of "many hands" greatly puts the migrant at a disadvantage and undermines fairness and due process [27]. Thus, this creates a major challenge for migrants, who often cannot challenge or understand the criteria behind these decisions, potentially leading to significant violations of their rights [12] and the inability to identify who is responsible for these violations.

The reliance on ADMs with the risk of perpetuating biases and systemic discrimination necessitates rigorous ethical oversight in the deployment of AI at the borders. The black-box nature of these AI systems means that once a system flags a person, the specific factors influencing this decision are often opaque, making it difficult to address errors or biases [8] or identify the agency liable for the harm occasioned. The General Data Protection Regulation 2016 (GDPR) [28] and the AIA both mandate human involvement in automated decision-making processes. However, this requirement is rendered ineffective if the human reviewer cannot grasp the reasoning behind the algorithm's decision [29]. Additionally, the threshold for demonstrating adequate human involvement, as outlined by the European Data Protection Board (EDPB, formerly WP29 [30]), presents an additional risk. In situations where a human is required to override an algorithmic decision, the reviewer may be unable to fully comprehend the decision-making process, rendering their intervention not only ineffective but potentially misguided. More so, the AILD requires potential claimants to establish plausibility before the court can order the disclosure of evidence.[3] Like the GDPR and the AIA provision on human involvement, this requirement of the AILD is an uphill task; it is nearly impossible for a potential claimant to provide facts and evidence sufficient to support the plausibility of a claim for damages if they cannot understand the decision of the algorithm, let alone identify the agency responsible. Thus, in the context of border control, migrants face the difficulty of not being able to contest the algorithmic outputs that they cannot comprehend and the difficulty in identifying those responsible. If the cause of harm or violation of a right is too complex to understand, then it will also be difficult to determine who is responsible for the violation or harm. This ethical and legal quandary means that migrants are at risk of being detained or deported, discriminated against, mobility infringed or denied entry without a fair hearing or procedural rights [26]. Depending on the circumstance, this could lead to grave emotional stress, financial loss or violation of other civil liberties. Additionally, this issue is even more troubling, given that the AILD has been withdrawn [20]. As a result, when an individual's rights are violated or harm is caused by an ADM, there is no recourse available for them. This forces individuals to rely on their national laws, which would affect technology companies due to the lack of uniformity in the law, as they would have to navigate and comply with multiple, potentially conflicting regulations, creating significant challenges for cross-border governance.

Concomitantly, ERS tools such as iBorderCtrl and AVATAR, which purport to assess truthfulness by analysing micro-gestures and physiological responses, have come under intense scrutiny [31]. While ostensibly designed to bolster border security, these systems face mounting criticism due to their dubious scientific foundations and potential for human rights infringements [31]. The opaque decision-making processes inherent in these tools raise alarming concerns about violations of privacy and non-discrimination rights, effectively undermining the presumption of innocence and the right to a fair hearing [32]. A recent incident involving iBorderCtrl's algorithm erroneously flagging an honest journalist as deceptive has laid bare the system's shortcomings [32]. This mishap not only exposes the flaws in the technology but also ignites a contentious debate about liability. In the wake of such errors, which can profoundly impact individuals' fundamental rights, the question of accountability looms large. Who bears the responsibility when AI-driven systems falter? The nebulous nature of liability in algorithmic decision-making further muddles an already complex legal and ethical terrain [31].

Moreover, the reductionist approaches these systems employ in judging truthfulness—relying on questionable interpretations of micro-expressions and physiological cues—is not merely scientifically unsound but ethically

[3] Article 3(1).

problematic [32]. This simplistic methodology engenders a labyrinthine web of potential liabilities, compounding concerns about the systems' validity and their propensity for human rights violations in migration contexts. The challenge of establishing clear lines of accountability when errors occur adds yet another layer of complexity to this multifaceted issue [31, 32].

Furthermore, while the AIA's risk regulation framework aims to mitigate the dangers (human rights violations, system validity) posed by AI technologies, it could exacerbate these issues by creating significant loopholes. For example, while Article 6 of the AIA explicitly prohibits the use of biometric and emotion recognition technologies by law, this restriction does not apply to immigration and border control management. As a result, these technologies remain in use within these contexts, leaving a critical gap where biases and ethical concerns inherent to AI systems continue to persist. The application of AI in these sensitive areas not only raises significant human rights concerns but also amplifies them, prompting some scholars to advocate for a six-month moratorium on AI development to better assess and address these risks [33]. Similarly, the UN High Commissioner for Human Rights has called for an outright ban on untested AI tools and "black box" systems that operate without transparency and accountability [34]. In a similar vein, European Digital Rights (EDRi) has urged a complete ban on AI-based risk assessments in migration, emphasising the inherent biases and human rights violations these tools bring. Furthermore, EDRi calls for a ban on remote biometric identification to ensure the protection of privacy and uphold fundamental rights [35]. While such measures aim to protect rights indirectly, ex-ante algorithmic harm, by focusing on risk regulation, may impede AI's benefits in security and efficiency and stifle innovation [36]. Hence, the EU turned to liability (PLD and AILD) regimes to protect the fundamental rights of individuals, including migrants, affected by algorithmic harm. This research will now focus on highlighting the ethical implications of these smart border systems before critically assessing one of the proposed liability regimes, AILD, to analyse and explore the individual rights contained in this law.

2.1 Ethical implication of smart border systems

The deployment of AI systems, such as iBorderCtrl and other risk assessment tools, raises profound ethical concerns beyond mere technological failures. At the heart of these issues is opacity: the inability of individuals to understand why decisions are made about them. For migrants subjected to automated border control systems, this lack of transparency is not just an inconvenience; it is a serious barrier to justice. When a system flags a person as "high-risk" without explanation, the individual is left in the dark, unable to contest the decision or even comprehend the criteria behind it. This opacity exacerbates the vulnerability of migrants, who may be detained, denied entry, or deported without a fair understanding of the reasons behind these life-altering decisions [37]. Moreover, the increasing reliance on AI to make these critical decisions strips away the human element—the nuance and context that a machine simply cannot account for [37]. However, it is also important to recognise that there may be legitimate reasons for classifying an individual as "high-risk," particularly in cases related to national security or intelligence gathering. For example, if the decision is informed by human intelligence, disclosing the reasoning behind the classification could jeopardise vital sources or methods of intelligence collection. In such instances, withholding information might be necessary to protect broader security interests [37]. That said, this must be balanced with efforts to ensure accountability and transparency in how such decisions are made, as AI systems used in border control are prone to biased outputs, especially if the algorithms have not been trained to recognise the socio-political and cultural complexities of migration. The risk of reinforcing existing discriminatory patterns is high, as AI systems may disproportionately flag certain nationalities, ethnicities, or individuals based on faulty or incomplete data [37].

Compounding this ethical dilemma is the issue of accountability. When errors occur—such as the iBorderCtrl system flagging an innocent person as deceptive—it is often unclear who is responsible for the harm caused. Is it the algorithm developers who created a flawed system? The authorities who chose to implement it? Or the government for failing to ensure sufficient safeguards? This ambiguity in liability creates a legal and moral vacuum, where individuals are left without a clear avenue for redress, despite potentially suffering significant emotional, financial, and legal consequences [38]. Furthermore, the lack of recourse for those who are wrongly flagged or mistreated by AI systems infringes upon fundamental human rights, including the right to a fair hearing, due process, and freedom from discrimination [37, 38].

Another ethical concern arises from the dehumanisation of individuals subjected to algorithmic decision-making. When border authorities rely on AI to assess an individual's truthfulness based on physiological cues or micro-expressions, they reduce the complexity of human behaviour to cold, mechanical readings that do not account for the full context. This reductionist approach can lead to misjudgements—where a person is flagged as deceptive due to a nervous gesture, cultural differences in body language, or simple misunderstandings of the system's parameters. By treating human beings as data points in a risk algorithm [38], AI systems in border control undermine the presumption of innocence and foster an environment where individuals' rights are treated as secondary to security concerns.

Considering these issues, the ethical framework governing AI in border control systems, such as AIA, GDPR, and AILD, must evolve. It is insufficient to merely regulate the technology's use; the wider social and legal implications must also be meticulously considered. The current lack of transparency, accountability, and human oversight in AI-driven border control systems signifies an urgent need for reforms. Comprehensive measures, such as stronger rights to contest algorithmic decisions and clearer accountability structures, are vital to ensure that these tools are employed ethically and justly. The equilibrium between security and individual rights in these contexts demands ongoing scrutiny and ethical reflection, especially as migration remains a global challenge.

3 AI liability directive in smart border security operations

Before delving into the AILD, it is important to highlight why the foremost AI regulation, AIA, does not adequately protect the needs of individuals when an AI system causes harm. As noted, PLD will not be under investigation in this paper because it does not apply to a state's application of AI systems, especially in border control.

3.1 Limitation of the AIA

AI governance globally is increasingly adopting risk regulation approaches [39]. The EU, at the forefront of this trend [40], is the cornerstone of European AI regulation—the AI Act (AIA)— which came into force in August 2024. This umbrella framework implements a risk-based approach to AI regulation across the Union, aiming to ensure embedded safety and security in products and services while promoting human-centric and trustworthy AI [24].

The AIA introduces requirements intended to reduce risks to safety and fundamental rights, prevent societal concerns, and foster innovation. It employs instruments such as standards, prohibitions, and risk and impact assessments to regulate behaviour ex-ante, that is, independently or before potential harm occurs. This approach reflects a growing recognition of AI's potential impact on health, safety, fundamental rights, democracy, the rule of law, and the environment [41]. Nonetheless, although the AIA proposes a comprehensive regulatory framework and an oversight structure to prevent harm from AI-related risks, it does not provide an adequate mechanism for what happens when harm occurs. For instance, while the AIA audaciously provides in Article 86 a right to explanation as one of the remedies when there is post-algorithmic harm, it does not specify mechanisms for enforcing or ensuring compliance with its provision [15]. This is the reality in cases where algorithmic decision-making leads to discriminatory outcomes, such as a visa streaming algorithm that systematically disadvantages applicants from certain ethnic backgrounds, thereby perpetuating racial biases in migration and border control [41]. Thus, while it appears that a right to explanation may arm decisional subjects with the necessary information to appeal an algorithmic decision and get compensation, the said provision has been suggested to be ineffective and non-operative, lacking the necessary tools to achieve this right, which can, in turn, support claims under the AILD, especially when Article 3(1) AILD is activated. Thus, the effect of the absence of operational effectiveness in the AIA means that harm can still occur even under the AIA, which does not provide for liability claims or compensation for victims [19]. This is so because victims or decisional subjects are left at the mercy of deployers or users of ADMs, particularly concerning Article 86 AIA [19].

Additionally, the adoption of a risk-based approach in the AIA has faced criticism from various quarters. While some think tanks and companies worry about overburdening innovative AI developers, human and digital rights activists argue that the Act does not go far enough in protecting individuals from AI harm [42]. Critiques highlight that the Act seems particularly lenient in sensitive realms such as national security, especially migration control, where a blank exception was adopted. Additionally, it allows the use of facial recognition and other biometric categorisation systems by law enforcement and migration authorities while prohibiting them in education and the workplace [26]. Thus, this tiered-risk approach inevitably leaves out certain applications that may be risky, highlighting a crucial limitation of the AIA.

Additionally, the leniency displayed by the AIA in permitting migration authorities to use advanced technologies such as emotion recognition and risk assessment constitutes a significant erosion of the protection envisioned under Article 22(1) GDPR. Consider the iBorderCtrl case above, where the system erroneously determines that an honest journalist is lying based on emotion recognition and behavioural profiling [31]. As noted, systems like iBorderCtrl rely heavily on biometric and behavioural data analysis to assess the credibility or risk level of individuals at the border [31]. Decisions rendered by such systems, such as denying entry, subjecting individuals to intrusive secondary screenings, or detaining them, have profound consequences for the data subjects. These decisions often lack meaningful human intervention, making them quintessential examples of automated decision-making that triggers Article 22 GDPR protections.

Article 22 prohibits decisions based solely on automated processing, including profiling, where such decisions produce legal effects or similarly significant consequences for individuals. This prohibition is fundamental to the GDPR's objective of safeguarding individual autonomy and ensuring fairness in the face of increasingly advanced technologies. However, the GDPR allows exceptions in specific circumstances, including where the decision is authorised by Union or Member State law that includes appropriate safeguards for individuals' rights and freedoms. In the context of immigration and border control, this exception is often invoked under Article 22(2b), as consent from migrants or asylum seekers is rarely practical given the inherent power imbalances and vulnerabilities of these groups.

The AIA's approach to regulating the use of such systems complicates this framework further. While the AIA seeks to classify systems like iBorderCtrl or AI-based risk assessment tools such as ETIAS and VIS as high-risk [see Annex III to Article 6(2)], it does not outright prohibit their use. Instead, the AIA focuses on implementing procedural safeguards such as transparency requirements, risk management, and human oversight, which, while important, fall short of the comprehensive protections envisioned by the GDPR. This permissive stance is particularly concerning considering the broad justifications allowed under the AIA for deploying these systems, such as national security and public interest. These justifications align with Recital 71 of the GDPR, which permits exceptions to Article 22 where decisions are based on substantial public interest and accompanied by safeguards.

However, the EDPB's 2018 guidelines on automated decision-making emphasise that exceptions based on public interest must be narrowly interpreted and underpinned by clear legal bases, along with strict transparency and accountability mechanisms [5]. The EDPB specifically warned against treating public interest or national security as blanket justifications [5], as this risks undermining the fundamental rights protected under the GDPR. The AIA, by allowing the deployment of high-risk AI systems in migration contexts without aligning these practices with the stringent requirements of Article 22, inadvertently facilitates the very practices the GDPR was designed to prevent.

This regulatory gap is further exacerbated by the divergence in objectives between the two frameworks. While the GDPR prioritises individual rights and autonomy, the AIA's approach to migration systems appears to prioritise operational and security concerns, potentially at the expense of robust data protection. For instance, while the GDPR prohibits decisions based solely on automated processing, the AIA implicitly permits such practices if procedural safeguards are observed. This divergence enables systems like iBorderCtrl to operate under the AIA's framework, circumventing GDPR's stricter prohibitions by relying on broadly framed justifications of public interest or national security. Such practices undermine the GDPR's foundational principles and erode the rights of data subjects.

Therefore, while the GDPR seeks to ensure robust protections against automated decision-making, its practical enforcement is significantly undermined by the flexibility introduced under the AIA. The AIA's permissive stance toward high-risk AI systems in migration contexts highlights a regulatory misalignment that risks enabling the very practices the GDPR seeks to prohibit.

Furthermore, the AIA regulates some aspects of human–machine interactions, such as human-in-the-loop and provides for a right to explanation for high-risk AI systems in Article 86, it offers limited avenues for those impacted by AI systems to seek redress [27]. As argued, Article 86 is ineffective and does not guarantee the protection it claims [43]. This gap in the AIA underscores the need for a complementary liability regime for harms caused by or with AI systems, especially in migration control. Consequently, risk regulation alone is rarely optimal [27].

From a corrective justice perspective, risk regulation must be supplemented by liability law to ensure that harmed individuals can be compensated when harm does occur. Moreover, from a risk-prevention standpoint, risk regulation may fall short of creating optimal incentives for all parties to take necessary precautions. Therefore, in this context, liability law becomes an important vehicle to ensure that the vast and fast adoption of AI systems in all facets of life, particularly in and around the border is done in a way that guarantees the protection of migrant's rights and interests, but also provides legal certainty for AI developers and deployers [44–46].

The situations highlighted above all point to the necessity of a robust liability regime for AI systems. This brings us to the consideration of the AILD, which aims to address these gaps in the AIA and provide a framework for accountability in AI-related harms.

3.2 An overview and analysis of AILD

The AILD, albeit withdrawn by the Commission [20], aimed to reform national fault-based liability regimes, complementing the existing PLD, which addresses defective products causing physical injury, property damage, or data loss [41]. Introduced alongside the AIA and the revised PLD [47], the AILD sought to ensure that victims of AI-related harm benefit from a legal presumption applicable to all claims involving malfunctioning AI systems. This targeted reform would have introduced a new liability framework designed to provide legal certainty and facilitate consumer claims for damages caused by AI-enabled products and services. While now withdrawn, the AILD would have applied to all AI systems available or operating within the EU market, covering claims involving violations of fundamental human rights and freedoms [48]. It extended liability beyond physical injury, offering a pathway for compensation in cases where AI systems infringe on personal rights. Furthermore, Article 2, paragraphs 6 and 7 of the AILD specified that both natural and legal persons suffering harm would have the right to pursue legal action, which could also be exercised by a successor or third party authorised to act on their behalf. Importantly, liability claims could be brought against any responsible party, including developers, suppliers, and users of AI systems. Although withdrawn, the proposed regime would have empowered applicants to challenge AI decisions impacting their fundamental and civil rights, including at the border. Given this withdrawal, it is clear that the AI liability framework still has much ground to cover.

The complexity of ADMs, in conjunction with the provisions of the AILD, pose significant challenges in claiming damages and assigning responsibility. This issue is explored through various elements outlined in the AILD, including the plausibility requirement and knowledge of harm in Article 3(1), the exclusion of human oversight, and the opacity of AI algorithms, all of which contribute to the creation of a liability gap.

A. Plausibility requirement

The AILD stipulates that claimants must "present facts and evidence sufficient to support the plausibility of a claim for damages" before a court can order the disclosure of relevant evidence (Article 3(1)). This applies in cases where a provider, under Articles 16 or 26 (1) of the AIA or a user of an AI system, refuses to disclose crucial information. However, this requirement places potential claimants in a paradoxical situation reminiscent of Joseph Heller's *Catch-22* [49].[4] Potential claimants are expected to prove plausibility without having access to the evidence needed to support their case. This dilemma is especially pronounced in the context of ADMs, which often operate as opaque "black boxes" with inscrutable decision-making processes [50]. Without transparency, it becomes nearly impossible for claimants to articulate a plausible claim.

This evidentiary conundrum raises significant concerns about fairness, particularly when viewed through the lens of the right to a fair trial. Article 6 of the European Convention on Human Rights [51] enshrines the principle of equality of arms, which requires that both parties in a legal dispute have an equal opportunity to present their case without being placed at a substantial disadvantage. This principle ensures that no party is unduly burdened in legal proceedings. Thusly, AILD's evidentiary requirements may create such a burden by disproportionately disadvantaging potential claimants, particularly in disputes against AI developers or users with far greater access to information, as is the case with migrants against the state and border agents in migration control.

Additionally, AILD's potential clash with fundamental EU legal principles cannot be ignored. The right to an effective remedy, guaranteed by Art 47 of the Charter of Fundamental Rights of the European Union [52], may be undermined by this evidentiary barrier. By making it exceedingly difficult for claimants to pursue legitimate claims, the AILD risks creating an insurmountable obstacle to justice. This concern is reinforced by the principle of effectiveness, which requires that national procedural rules must not make it practically impossible or excessively difficult to exercise rights conferred by EU law [53]. The evidentiary requirements in the AILD could easily violate this principle, particularly in border control cases where complex ADMs are deployed, making it excessively difficult to meet the plausibility standard without access to key information.

Undoubtedly, the AILD falls short in ensuring equal treatment for individuals seeking redress for AI-related harms. This lack of procedural fairness is particularly concerning when contrasted with the transparency provisions laid out in Article 15(h) of the GDPR. The GDPR's emphasis on transparency in algorithmic decision-making underscores the need for

[4] catch 22, Hellers work is used to describe a no-win situation or a paradoxical rule that creates a dilemma where one cannot escape a problem due to contradictory constraints.

claimants to have access to crucial information that could support their claims. Denying such access creates a significant barrier to justice. However, this access to information might conflict with IP rights, depending on the scope of information requested. In this context, the AILD's requirement for a potential claimant to establish plausibility without access to any supporting evidence mandated by the directive is antithetical to the very issue it attempts to address by its adoption.

This evidentiary paradox intersects with deeper theoretical and philosophical concerns about justice and fairness. The principle of procedural justice, which emphasises the importance of fair and equitable legal processes, is at risk. By placing an excessive burden on potential claimants [53], especially in the context of migration, migrants threaten those who are at the mercy of the state where they are either seeking asylum or wanting to travel for one purpose or another to violate core tenets of procedural fairness [54]. Thus, without a mechanism to reconcile the need for plausibility with the claimant's lack of access to information, the AILD risks undermining the very principles of fairness, transparency, and accountability that it aims to uphold.

B. Knowledge paradox

Although Article 3(1) of the AILD allows for the disclosure of evidence once a claimant establishes plausibility, it imposes a significant caveat that must be addressed before proving plausibility. Specifically, Article 3(2) requires that courts shall only order the defendant to disclose evidence if the claimant has undertaken all proportionate efforts to obtain it from the defendant. This includes requesting relevant evidence under Article 3(1) AILD from the provider or user of the AI system under obligations set out in Articles 16 or 26 AIA. Thus, the preconditions for court-ordered disclosure are threefold: the claimant must first request access to relevant evidence concerning the specific high-risk AI system suspected of causing damage, which evidence is currently in the possession of the defendant and has been withheld or denied; secondly, they have exhausted all reasonable avenues to obtain the evidence from the defendant, and thirdly, they must establish the plausibility of their claim.

These tripartite requirements, while aimed at preventing an overload of frivolous claims, create a paradox. It presupposes that potential victims are aware of the harm caused to them by these ADMs —a presumption that may not hold in many cases. Without such awareness, the procedural safeguards designed to limit reckless litigation could, in effect, hinder the benefits of evidence disclosure and the reversal of the burden of proof [41].This creates a delicate balance, as AILD allows defendants to withhold information under broad confidentiality claims, particularly in migrant cases involving complex AI systems. Establishing a necessary and proportionate threshold for evidence of harm, especially when the harm pertains to a violation of fundamental and civil rights by opaque ADMs, is extraordinarily difficult before any concrete proof is available. This creates a knowledge gap that leaves room for abuse and, in turn, places an undue burden on potential claimants—a burden of ignorance [55].

Furthermore, for potential claimants to submit a claim, they must be aware of or suspect harm and present sufficient facts and evidence to substantiate the likelihood of a damages claim. However, acquiring such knowledge is no simple task, especially in AI-driven border control. In many cases, the claimant may not know or suspect that the algorithm's decision was the result of bias or unlawful discrimination, particularly since they do not typically have access to the system's output logs or internal decision-making processes, nor does the AILD grant them access to the same until they have established plausibility of their claim [41]. Consider the case of the journalist that iBorderCtrl identified as lying or where a migrant was flagged or denied entry by ETIAS [32]: while this may not prompt a migrant to inquire further, even then, the information they access may not reveal the algorithmic reasoning behind the decision. Again, consider an instance where a migrant belonging to a particular racial group is systematically denied access by ETIAS. In such a circumstance, discrimination lies in the absence of access rather than an explicit refusal based on legitimate criteria. This knowledge gap is fundamental, as awareness of harm is necessary for claimants to hold those responsible to account and to close the broader accountability gap [56]. However, the AILD is silent on this matter and places an onerous burden on the claimant to establish plausibility. Considering this challenge, it is difficult for potential claimants to realistically become aware of and seek redress for such hidden discrimination.

Assuming a migrant were to invoke their transparency rights to access relevant logs considering the opinion provided by the European Data Protection Supervisor (EDPS) [57] in their executive summary on the proposal AILD— which states that the disclosure required in Article 3 AILD pertains to the technical documentation and logs of high-risk AI systems under Article 18 of the AIA— firstly, the understandability of these logs, coupled with the opaque nature of such systems, significantly hinders transparency and understanding; and secondly, this disclosure can only happen after the claimant has established plausibility. However, if migrants were entitled to a functional and operative right to explanation and explainable AI, the rationale behind an algorithm's output can not only help them comprehend the decision and the decision-making process but also raise their awareness of the harm suffered and establish plausibility.

The AILD's emphasis on transparency as a solution is well-intentioned but fails to resolve the inherent opacity faced by potential victims. It assumes an unrealistic level of awareness and access to information, thus reinforcing the knowledge gap [56] between claimants and the developers or users of ADMs.

In addition, by reiterating that courts can only order the disclosure of evidence if claimants have undertaken proportionate efforts to gather it (Article 3(2)), the AILD further entrenches the challenge of proving plausibility without the necessary information. Such caveats, albeit designed to prevent a flood of unfounded claims, inadvertently disadvantage those who lack the awareness or means to understand the potential harm inflicted upon them by complex ADMs. In this way, the procedural protections intended to mitigate frivolous litigation could, in practice, restrict access to justice and obscure the path toward a fair and equitable resolution for victims of AI-related discrimination and harm.

C. non-human in the loop requirement

The AILD introduces complexities regarding the role of human oversight in AI systems, specifically in cases where human intervention is minimal or unclear [21]. Recital 15 of the AILD proposal states that liability claims are excluded "when the damage is caused by a human assessment followed by a human act or omission," even if the AI system provided advice that the human considered. However, this phraseology overlooks situations where human judgment is heavily influenced by the output of the ADM, raising questions about accountability and responsibility.

For example, consider the iBorderCtrl system at the border: If a border agent follows the system's recommendation to deny entry based on an incorrect assessment of risk, the agent's decision might be seen as a "human act" under the AILD. It could be suggested that liability lies with the border agent, not the system provider. Sometimes given the various stakeholders involved in the design, development, placement, and operation of these AI systems, it is more or less difficult to find an agency responsible [41]. However, owing to the complex nature of AI systems and their often-opaque decision-making processes, the agent may have relied heavily on the AI's recommendation. This reliance complicates the attribution of liability, as the line between human judgment and AI influence becomes blurred.

This issue is further complicated in scenarios where minimal human intervention occurs, such as when a border agent briefly reviews an ADM's recommendation before denying entry. In such cases, even if this handoff meets procedural requirements, the system's influence on the final decision may still play a significant role. Without further nuance in the AILD, claimants would need to demonstrate that there was meaningful human involvement. As earlier stated, the EDPB opinion on automated decision-making [30], Art 22 GDPR, is of paramount importance here. The EDPB emphasised that for a decision to be considered "solely automated," there should be no human intervention that influences or impacts the outcome of the decision. Recital 15 (AILD) echoes similar concerns raised in Article 22(1) of the GDPR, where scholars [58] have cautioned that automated decisions could be unjustly validated through superficial human intervention (rubberstamping of decisions). Recent court rulings in *Schufa holding AF* support this argument [59].[5] Thus, failure to demonstrate significant human influence over the decision establishes grounds for AI liability.

Furthermore, the European Data Protection Supervisor (EDPS) has expressed concerns over Recital 15, warning that this exclusion could lead to circumvention of accountability by allowing AI systems' decisions to be "rubberstamped" by humans [57]. Hence, the exclusion of human acts following an AI-recommended decision under the AILD presents a significant challenge. The directive must account for instances where ADMs like iBorderCtrl exert significant influence over human decisions, or it risks leaving gaps in accountability and undermining the directive's purpose.

D. The liability gap

The opacity of ADMs makes it difficult to close the liability gap in attempting to distribute liability among designers, developers, deployers, or users [41]. This challenge becomes even more pronounced in cases of algorithmic discrimination, where biases related to sex, race, or other protected categories emerge [56].For example, ERS tools like iBorderCtrl, as already noted, make sweeping judgments about an individual's truthfulness based on questionable interpretations of micro-expressions and physiological responses [60]. Such systems often disregard the complexity of human emotion

[5] CJEU in the Schufa holding case stated that solely automated decision-making in Art 22 GDPR includes a fully automated *part* of the final decision.

and the diversity of cultural expressions, raising serious concerns about their scientific validity. As a result, they could potentially discriminate based on ethnicity or nationality, flagging individuals as suspicious without a sound basis. This example highlights how the autonomy, complexity, and opacity of AI systems, particularly when operating within socio-technical environments, such as a smart border, can undermine ethical standards, weaken accountability chains, and complicate efforts to determine who is responsible for such discriminatory outcomes.

These issues are further exacerbated by the concept of "many hands." *Id est* the involvement of multiple actors at various stages in an AI system's lifecycle [27]. From the design and programming phases to deployment and ongoing supervision, numerous individuals and organisations contribute to the system's operation and outcomes [27]. In the case of iBorderCtrl, responsibility could be diffused across those who develop a component of the algorithm, the producer or manufacturer of the AI system, border agents who deploy it, and the supervisors who oversee its operation etc. This diffusion complicates the attribution of responsibility and accountability for harm, as it is difficult to narrow which actor's contribution led to the discriminatory outcome, especially considering the opaque nature of these systems and the absence of an operative and functional right to explanation [19]. The complexity of socio-technical systems like iBorderCtrl or ETIAS, combined with the lack of clear accountability structures, highlights the need for a robust liability framework to simplify and narrow the liability gap for victims and ensure that responsibility for AI outcomes is properly allocated.

AILD is designed to address both the liability gap by easing the burden of proof for claimants and the knowledge gap by granting the right to access relevant information about high-risk AI systems to demonstrate fault. However, in practice, the AILD falls short of adequately addressing these issues. It leaves critical questions about the relevance and distribution of information unresolved and fails to sufficiently reduce the asymmetry of knowledge between claimants and defendants [41]. While the AILD reduces legal fragmentation by standardising claims processes, it fails to eliminate the legal uncertainty surrounding AI-driven decisions [41]. The AILD prioritises transparency and the disclosure of high-risk AI systems Article 3(2) over providing meaningful knowledge of the harm suffered by individuals, shifting the burden onto claimants to not only establish plausibility but also to navigate and interpret the information supplied by defendants, Article 3(1). In this sense, the AILD, in its current form, may struggle to fulfil its regulatory objectives.

The AILD, though withdrawn by the Commission, still offers invaluable insight into the challenges of integrating liability and accountability into AI-driven systems, particularly in the context of border control and ADMs. Despite its withdrawal, the issues identified within the AILD remain pressing and continue to inform ongoing discussions about the future of AI liability in the EU. This analysis has highlighted significant gaps within the AILD framework, including the plausibility requirement, the knowledge paradox, and the exclusion of human oversight, all of which complicate efforts to ensure fairness and justice for individuals harmed by AI systems.

In response to the current regulatory gap, we propose integrating an operational right to explanation or a sui generis explainability requirement within any future AI liability framework. This would ensure that claimants can access sufficient facts and evidence to establish plausibility before seeking further disclosure, as outlined in Article 3(1 & 2) of the withdrawn AILD. Such a provision would not only strengthen the claimant's position but also assist both users and producers in addressing issues proactively, reducing the need for claimants to resort to legal action to contest harm. It is important to note that while such disclosures would enhance transparency, they may also conflict with intellectual property rights and potentially expose trade secrets, which could present significant risks to producers.

As the Commission contemplates new proposals for AI liability, these considerations must be integrated into any future legislative efforts. The need for a balanced, transparent, and accessible framework is more urgent than ever, especially given the growing deployment of ADMs in sensitive areas such as border control. Ensuring that AI-driven systems uphold human rights and fundamental freedoms requires both clear legal protections for individuals and a robust accountability mechanism for the developers and operators of these systems. Thus, to ensure that AI systems—especially those in high-risk sectors like border control—do not undermine fundamental rights, future liability regimes must adopt more robust mechanisms for transparency, explainability, and access to evidence. As such, our proposal considers integrating sui generis explainability requirements into AI liability laws alongside mandatory compliance with existing transparency provisions in the AIA. This would help bridge the knowledge gap, empowering claimants and ensuring that individuals harmed by AI systems can pursue effective legal recourse. This proposal aims to influence and inform the development of future AI liability regimes, fostering a regulatory environment that promotes both the responsible advancement of AI technologies and the protection of individual rights.

3.3 Effects of the commission's withdrawal of the AILD

The withdrawal of the AILD raises significant concerns, particularly when individuals are harmed by automated decision-making (ADM) systems. One of the primary consequences is the fragmentation of regulatory approaches across the EU. Without a uniform framework, individual member states are left to develop their own rules regarding AI liability or apply their respective national laws, resulting in inconsistent standards and practices. This fragmentation can lead to disparities in how victims of AI-related harm are treated in different countries. Inconsistent regulations could also make it more difficult for businesses to operate across borders, as they would need to navigate various rules and requirements in each jurisdiction. Consequently, victims might face unequal levels of protection depending on where the harm occurred, creating an imbalance in access to justice.

Furthermore, the absence of the AILD presents a challenge for innovation in the AI space. The uncertainty surrounding liability and accountability may cause developers to hesitate in releasing AI systems, particularly in high-risk sectors like border control, where the potential for harm is significant. Developers might be reluctant to create systems that could lead to legal challenges, which could either slow the advancement of AI technologies or prompt overly cautious approaches that limit their potential benefits.

Without a clear liability framework, the risk of undermining fundamental rights becomes even greater. AI systems, especially those involved in decision-making about individuals' lives, must be transparent, accountable, and subject to strict oversight to ensure they do not infringe upon basic rights and freedoms. The lack of the AILD means there is no established legal mechanism to hold those responsible for AI systems accountable when they cause harm. This absence leaves individuals exposed to rights violations without an effective means to seek redress, eroding trust in both AI technologies and the systems that deploy them.

4 Integrating sui generis explainability requirement into liability framework for smart borders

The integration of explainability into AILD or future AI liability regimes presents a compelling solution to the multifaceted above-mentioned issues—plausibility requirement, knowledge paradox, bridging the liability gap, meeting the, and unravelling the opacity that obfuscates responsibility. As ADMs increasingly permeate border control mechanisms, the need for transparency and accountability becomes paramount, not only to protect the rights of migrants but also to ensure the integrity and fairness of these systems [35]. This section will discuss the importance of explainability requirements, the trade-off with IP rights and security, and the integration of explainability requirements or rights.

4.1 Imperative for integrating explainability in AILD

Integrating a sui generis explainability requirement in Article 3(1) AILD or mandating a corresponding right to explanation directly addresses the plausibility requirement outlined in Article 3(1). By providing claimants with a clearer understanding of the decision-making process of ADMs, explainability equips them with the necessary tools to construct a plausible narrative of harm. In essence, the claimants are not disadvantaged and handicapped, as outlined in the AILD. Requesting a claimant, in the context of this paper, a migrant, to provide facts and evidence to establish the plausibility of harm claimed without understanding the grounds on which his claim is based is like asking an explorer to navigate a maze blindfolded without a map or sense of direction. This is the nature of the burden placed on claimants when activating their procedural rights as enshrined in AILD. However, a right to explanation, which ordinarily ought to occur as of right following any decision, human-made or algorithm-made, provides a clear understanding of the basis or grounds for a decision. A right to explanation or an explainability requirement not only levels the playing field between claimants and defendants but also aligns with the AILD's underlying goal of facilitating just compensation for AI-related harms Article 1. The enhanced transparency afforded by explainable AI models (XAI) and a right to explanation could potentially lower the initial threshold for plausibility, allowing for a more equitable disclosure process that does not unfairly burden claimants with an impossible evidentiary standard. Additionally, it ensures fair and just reconciliation of AI-related harms [61].

ADMs are known for being opaque, making it difficult to understand their decision-making process, let alone even know when harm has occurred [62]. The AILD requires potential claimants to know when a wrong has been done by an algorithm. As alluded to (*in paragraph 3 sub 3.2 point B*) above, in different circumstances, people may be keen to enquire and others not, how do you reconcile when a harm has been done. This conundrum is referred to as a knowledge paradox, which stems from the AILD's requirement. Potential claimants are expected to present facts and evidence supporting the plausibility of their claim before accessing crucial information to determine if they were harmed or not. This paradox can be significantly mitigated through the implementation of a sui generis explainability requirement and ensuring potential claimants, *id est* migrants in this context, are provided with an explanation, especially where high-risk AI systems are involved. By elucidating decision-making processes without compromising accuracy, these models provide claimants with the initial insights necessary to formulate a plausible claim [63]. This transparency serves as a bridge over the chasm of ignorance that often separates potential claimants from understanding the decisions that profoundly affect their lives. For instance, in the case of systems like iBorderCtrl or ETIAS, explainability could reveal the specific factors that led to a migrant being flagged or denied entry, empowering them to challenge decisions based on concrete information rather than mere suspicion [64, 65].

Additionally, the liability gap, exacerbated by the complexity and opacity of AI systems, especially in border control, can be narrowed through the systematic implementation of explainability measures [65]. By shedding light on the internal workings of these systems, explainability helps to delineate the chain of responsibility from design to deployment. This clarity is crucial in scenarios where the concept of "many hands" obscures accountability, such as in the development and operation of complex systems like iBorderCtrl. With XAI, it becomes easier to trace decisions back to specific components or stages of the system, facilitating a more precise attribution of liability when harm occurs [66]. This makes it easier for the potential claimants to attribute their claim and damages at the earliest stage to establish a plausible claim. Certainly, for a case to be plausible, the potential claimant must be aware of who wronged them; a claimant does not file an action for the sole purpose of waiting for disclosure of the high-risk systems to determine liability. Establishing a plausible claim must include knowing who is responsible for the damages alleged. Hence, Article 3(1) is drafted to exist in isolation in the absence of any obligation to adhere to the right to explanation in Article 86 AIA or the integrating an explainability requirement that ensures individuals are not only aware that they have been wronged but know who is responsible and the wrong committed—the violation of their fundamental and civil rights.

Undoubtedly, the integration of explainability into AILD serves to mitigate the power asymmetries inherent in the use of AI systems, especially in border control. By democratising access to information about AI decision-making processes, explainability shifts power away from technocratic elites and towards a more balanced governance structure. This ensures an equal playing field and aligns with the AILD's goal of protecting individuals affected by AI systems and ensures that these technologies serve the public interest rather than reinforcing existing power structures or creating new forms of digital authoritarianism [67].

However, it has been argued that the right to explanation could potentially expose proprietary confidential information, which might lead to the system being gamed or imitated by other providers. Additionally, there is concern that providers or users could exploit this as a justification to evade disclosure altogether.

4.2 Trade-off between explanation rights and intellectual property rights

Arguments abound suggesting that the two priorities— the right to explanation and intellectual property (IP) rights— are inherently at odds due to the fundamental conflict between them. The right to explanation is designed to grant claimants access to information and reasoning behind algorithmic decisions that negatively impact their legal interests. In contrast, IP rights, particularly trade secrets, aim to protect proprietary information, ensuring that sensitive data critical to innovation remains confidential and does not provide competitors with an unfair advantage. This clash between the transparency needed for accountability and the confidentiality required for competitive advantage poses a significant challenge. Providing detailed explanations of algorithmic decisions risks inadvertently disclosing business-critical information, thus potentially undermining a company's competitive edge [68]. Given this tension, it becomes crucial to consider how the Court of Justice of the European Union (CJEU) addresses such conflicts, particularly in its decision in *Dun & Bradstreet Austria* [69]. The court stated in paragraphs 70–74 of the judgment that the right of access under Article 15(1)(h) GDPR is clear regarding meaningful information about the logic involved in automated decision-making, including profiling. This information must be concise, easily accessible, and formulated in clear and plain language to allow data subjects to understand the methodology behind the automated decisions that affect them. In paragraph 71, the Court also emphasised that such information must be sufficiently complete and contextualised, enabling the data subject to verify its accuracy and ensure that there is a causal link between the method and the resulting decision.

However, as the Court points out in paragraph 72, this right does not extend to information that is so technically complex that it would be beyond the understanding of a typical data subject, especially when this information involves the detailed workings of algorithms used for decision-making. This raises a significant conflict: algorithms and other proprietary technologies, which are often protected as trade secrets, could be considered too sensitive to disclose fully.

the court stated in its decision that while the data controller/user, *id est* border agents in the context of border control, does not have to provide technical details of algorithms, it must still ensure that the information provided to the data subject is adequate for them to challenge the decision and understand its rationale.

Particularly in paragraphs 84–86, the Court recognises that Article 15(4) GDPR and Recital 63 allow for limitations on the right of access when such access would infringe upon the rights and freedoms of others, including the protection of trade secrets. The Court unequivocally stated in paragraph 89 that a data subject's right to access information should be restricted only where this is necessary and proportionate to safeguard the protection of trade secrets or other competing rights. Importantly, the Court clarifies that the right of access is not absolute and must be balanced with the need to protect IP.

Thus, to mitigate the risk of withholding too much information, the Court emphasises in paragraph 95 that, in cases where disclosure of certain information could infringe IP rights, the competent supervisory authority or court should be called upon to conduct a proportionality assessment. This assessment would determine the extent to which information can be disclosed without breaching trade secrets or other confidential business information. The Court's approach ensures that the right of access is not undermined by blanket claims of IP protection but instead is weighed carefully considering the specific context of the case.

Furthermore, in paragraphs 92–94, the Court reinforces the idea that, even when trade secrets are involved, it is still possible to provide general information about the logic of automated decision-making, such as the criteria and methodology used, without disclosing the actual algorithms or other proprietary data. The Court stresses that the right of access is not an all-encompassing right to full disclosure but rather a right to meaningful information that helps the data subject understand and, if necessary, contest the automated decision. This means that, while trade secrets might limit the disclosure of highly sensitive data, there must still be sufficient transparency to allow the data subject to verify the fairness and accuracy of the decision-making process and to challenge the outcome of an algorithmic decision.

Hence, while users might use IP rights as an excuse to avoid providing information—it can be addressed through the proportionality principle outlined in the CJEU decision. The Court's ruling makes clear that IP concerns such as trade secrets should not provide an absolute justification for withholding all relevant information. Instead, controllers/users must ensure that the data subject's right to transparency, in this context explanation, is respected to the extent possible without compromising legitimate business interests, and when in doubt, the involvement of supervisory authorities or courts or even regulatory sandboxes under a regulated condition may be necessary to strike the right balance.

Clearly, from the decision of the court, it is about finding the balance between access to information, in the context of this paper explanation requirements and IP rights. Thus, it is important that in explaining, only the right amount of information, *id est* information or details are necessary for the affected person or claimant in the AILD to challenge and contest the decision. In this way, trade secrets are protected.

4.3 Trade-off between explanation rights and security

The increasing reliance on smart border control systems is a direct response to the growing need for enhanced security at national borders. These systems leverage advanced technologies, including biometric data, automated decision-making algorithms, and AI to help border authorities identify potential threats in real time [70]. The core goal is to prevent the entry of individuals involved in criminal activities, terrorism, or those on no-fly lists. As such, smart border systems serve as a technological safeguard designed to protect the sovereignty of nations by regulating the movement of people across borders efficiently and effectively. These systems undoubtedly contribute to the security and integrity of borders, making it harder for dangerous individuals to enter a country undetected [71].

However, this increasing reliance on ADMs raises important questions about individual rights, particularly the right to an explanation. Explaining the decisions made by these systems is crucial in maintaining transparency and ensuring that individuals are not unfairly or unknowingly punished due to errors, biases, or lack of clarity [31]. As more nations adopt systems like iBorderCtrl or the ETIAS [31], these systems increasingly flag individuals for reasons that may not always be immediately clear or understandable to the person involved. For instance, an individual may be denied entry, flagged for secondary questioning, as was the case with the journalist (*see paragraph 2 above*) [32], or prevented from boarding a flight due to an algorithmic decision that labels them as a security risk [31].

The importance of the right to explanation or explainability becomes paramount when the system flags an individual for reasons like suspected links to terrorism or a potential security threat [32]. If a person is flagged by a system like iBorderCtrl, they should not be left in the dark about the exact reasons why their freedom of movement has been restricted [31]. Was it a false positive? Was there an error in the algorithm's assessment? Or, more concerning, is there inherent bias in the system's programming that disproportionately flags certain groups of people? [72]

The right to explanation in this context suggests that automated decisions by these smart systems should be understandable, accountable, and, if necessary, contestable by the individual impacted. Without these rights, individuals could be unjustly penalised or denied entry without recourse, leading to violations of fundamental human rights [19]. For example, a person wrongly flagged for terrorism links could experience severe personal, legal, and social repercussions yet might not be able to challenge the decision because the process lacks transparency or an understandable rationale [12].

However, achieving a balance between security and explainability is not straightforward. On the one hand, the security concerns driving smart border controls are legitimate and pressing. The threat of terrorism, illegal immigration, and organised crime requires robust systems to protect national security [70]. Yet, on the other hand, the technology behind these systems, such as machine learning algorithms, is complex and often opaque, which creates a tension between ensuring public safety and respecting individual rights. In some cases, full transparency might compromise the security of the system itself, especially if the logic of the decision-making process is shared in such a way that malicious actors could exploit vulnerabilities in the system [70].

Therefore, the key challenge lies in finding a middle ground where security is prioritised, but human rights, particularly the right to an explanation, are respected. One potential solution is to implement a multi-layered approach to explainability [61]. For example, while the full details of an algorithm's inner workings may not be disclosed due to security concerns, a system could still provide a summary of the criteria that led to a decision. If an individual is flagged by a border control system, they could be informed that they were flagged due to a specific set of risk factors, such as recent travel to a high-risk country or a mismatch in biometric data, without revealing sensitive algorithmic details that could be exploited [61].

The use of smart border control systems represents a delicate balancing act. While these systems provide undeniable benefits in terms of national security and the ability to prevent harmful individuals from entering a country, they also pose significant challenges regarding transparency, fairness, and individual rights. Striking the right balance between security and the right to explanation will be key to ensuring that these systems can be both effective and just, protecting both national interests and the fundamental freedoms of individuals.

4.4 Integrating a sui generis explainability in AILD framework

As argued in 4.1, a right to explanation and explainability requirement play a crucial role in mitigating the issues discovered in the AILD. This is so because the opacity that often shrouds AI decision-making processes, creating a formidable barrier to establishing responsibility, can be dissipated through robust explainability mechanisms [73]. By integrating a sui generis explainability requirement in Article 3(1) or by obligating adherence to a right to explanation as provided in Article 86 of AIA to follow a decision, the AILD could ensure that the reasoning behind algorithmic decisions is accessible and comprehensible. In this way, deployers and users are mandated to ensure that the decision-making process of these complex algorithms is explainable. This transparency not only aids in identifying instances of bias or discrimination but also enables more effective oversight by regulatory bodies, NGOs, and collective redress organisations.

To fully realise the benefits of explainability within the AILD framework, several practical steps could be taken. The directive could be amended to require high-risk AI systems, including those used in border control, to incorporate a sui generis explainability requirement in Article 3 of the AILD. This would require an explanation to follow a decision of the algorithm or require that before establishing the plausible cause, those obligated in Articles 16 and 26 AIA, providers and users provide victims of algorithmic decision with an explanation for the said decision. This would align with the AIA's classification of border control AI systems as high-risk and the provisions of Article 86 AIA notwithstanding its shortcomings. This will provide a solid foundation for transparency and accountability. Additionally, an enforcement mechanism or procedure that a victim must adopt against users or providers depending on the facts of the case when an explanation is not provided. This makes it easier for claimants to establish plausibility, identify the responsible agency, alleviate the burden of proof and navigate the complex landscape of AI-driven decision-making, especially when ADMs are deployed in border control.

In addition to mandating adherence to explanatory rights and measures, we suggest implementing a tiered plausibility standard. At the initial stage, claimants should face a lower threshold for proving plausibility, which would grant them access to limited disclosure of relevant evidence, *id est*, the explanation of a decision of an algorithm alongside other relevant information. This preliminary disclosure could include technical documentation or logs under Art 18 and 19 of the AIA, providing the claimant with a clearer understanding of the AI system's role in the alleged harm and how the decision causing the harm was reached. As the case progresses and more evidence becomes available, the standard for proving plausibility could be incrementally raised, requiring the claimant to present stronger evidence to justify further disclosure or compensation. This graduated approach balances the need for transparency with the difficulty of proving harm in AI-driven systems, especially when initial evidence may be inaccessible or difficult to interpret due to the system's complexity and opacity.

While the introduction of the explainability rights covers the individual remedy and vouchsafes immigrants the required information to establish plausibility and challenge algorithmic decisions at border control, the inclusion of solutions such as the extension of the prohibition of the use of biometrics, polygraphs and other emotion recognition technologies in the AIA to border control and management would be a welcome development. In this situation, it eliminates the possible violation of human rights or possible harm caused by these systems before they occur.

Finally, we also propose that AILD could introduce regulatory sandboxes—controlled environments where potential claimants could test high-risk AI systems for plausible harm. These sandboxes would allow claimants to interact with the AI system under regulated conditions, without risking full disclosure of the system's proprietary algorithms or sensitive data. Such an approach would provide claimants with valuable insights into how the system operates and whether harm could have occurred, while also protecting the IP of developers and users. By establishing these controlled environments, the AILD would balance the claimant's need for transparency and the developer's right to safeguard their IP, offering a practical way to evaluate harm without compromising confidentiality.

The integration of explainability into the liability framework rectifies some issues identified in the AILD proposal. By addressing the knowledge paradox, bridging the liability gap, meeting the plausibility requirement, and unravelling the opacity that obfuscates responsibility, explainability enhances the effectiveness of the AILD in protecting victims, and in this context migrants' rights by ensuring just outcomes in the context of AI-driven border control systems [63, 64]. This approach not only fosters trust and accountability but also paves the way for more equitable and transparent implementation of AI technologies in sensitive domains like migration management.

5 Conclusion: towards a balanced approach to accountability and innovation

The integration of AI systems in border control presents both opportunities and challenges. While the AILD, now withdrawn, represents a crucial step towards addressing these challenges, our analysis has revealed significant shortcomings in its current form. The directive's plausibility requirement, knowledge paradox, and the exclusion of human-in-the-loop scenarios create substantial barriers for potential claimants, undermining its effectiveness in protecting individuals' rights and ensuring accountability.

To address these issues, we propose integrating explainability into the AILD framework. This approach would help bridge knowledge and liability gaps, empower claimants, and enhance transparency in AI decision-making processes. Our recommendations include integrating a sui generis explainability requirement, expanding disclosure requirements, implementing a tiered plausibility standard, and introducing regulatory sandboxes. These considerations aim to influence and make recommendations for any future proposals for an AI liability regime and to foster a regulatory environment that encourages both the development and use of AI technologies to be responsible and accountable, ensuring that AI-driven or smart border control systems enhance security and efficiency while upholding fundamental rights and human dignity.

However, in pursuing these improvements, we must strike a delicate balance between accountability and innovation. The path forward requires a nuanced approach that fosters accountability without stifling technological advancement. This could involve developing standardised explainability methods that provide sufficient transparency without compromising IP.

With these considerations in mind, we can move towards a future where AI-driven border control systems enhance security and efficiency while upholding the principles of justice, fairness, and human dignity. The goal should be to create a regulatory environment that encourages the development of AI technologies that are not only advanced and efficient but also transparent, fair, and respectful of fundamental rights.

Author contributions U.N. wrote the main part of the manuscript, while C.G. wrote a substantial part of the manuscript. Both U.N. and C.G. reviewed and revised the manuscript.

Funding No funds, grants, or other support was received.

Data availability No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

References

1. Cockerell I. GreeceAimsLong-RangeSoundCannonsatMigrantsacrossItsBorder. Coda Story. 2021. https://www.codastory.com/authoritarian-tech/sound-cannons-greece/. Accessed 27 July 2024.
2. Molnar P. Robo Dogs and Refugees: The Future of the Global Border Industrial Complex (www.theborderchronicle.com). https://www.theborderchronicle.com/robo-dogs-and-%20refugees-thefuture?utm_source=url. Accessed 27 July 2024.
3. Molnar P. The walls have eyes. New York: The New Press; 2024.
4. Daniels J. Lie-detecting computer kiosks equipped with Artificial Intelligence Look like the Future of Border Security. CNBC15. 2018. https://www.cnbc.com/2018/05/15/lie-detectors-with-artificial-intelligence-are-future-of-border-security.html. Accessed 3 Jan 2024
5. Article 29 Data Protection Working Party, Opinion 2/2017 on Data Processing at the Unemployment Stage. 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 Accessed 26 Jan 2025
6. Beer D. Why Humans Will Never Understand AI. BBC Future. 2023. https://www.bbc.co.uk/future/article/20230405-why-ai-is-becoming-impossible-for-humans-to-understand Accessed 26 Jan 2025
7. Veale M, Edwards L. Clarity, surprises, and further questions in the article 29 working party draft guidance on automated decision-making and profiling. Comput Law Secur Rev. 2018;34:398.
8. Fink M. Robo Swarm sand Polygraphs: the future of European border management and its costs. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4883130. Accessed 27 July 2024
9. Nalbandian L. An eye for an "I:" a critical assessment of artificial intelligence tools in migration and asylum management. Comp Migr Stud. 2022. https://doi.org/10.1186/s40878-022-00305-0.
10. Everuss L. The Routledge Social Science Handbook of AI (Anthony Elliot, Routledge). 2021.
11. Hacker P. The European AI liability directives—critique of a half-hearted approach and lessons for the future. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4279796. Accessed 11 Nov 2024.
12. Digital Border Governance: A Human Rights Based Approach Digital Border Governance: A Human Rights Based Approach 2 Acknowledgments. 2023. https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-_Rights-Based-Approach.pdf. Accessed 12 July 2024
13. Jean-Sebastien Boghetti. Civil Liability for Artificial Intelligence: what should its basis be? La Revue des Juristes deSciences Po.
14. Sylvia Lu, 'Why the GDPR may fail to protect individuals from privacy risks produced by artificial intelligence applications and a new transparency-based approach to AI governance ma help. https://sites.duke.edu/thefinregblog/2022/03/01/why-the-gdpr-may-fail-to-protect-individuals-from-privacy-risks-%20produced-by-artificial-intelligence-applications-and-a-new-transparency-based-approach-to-ai-governance-may-%20help/. Accessed 13 Nov 2024.
15. Andrew Swarback, Artificial Intelligence and Liability, key takeaways from recent EU initiatives, https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability. Accessed 10 Oct 2024.
16. European Commission. AI Act Enters into Force on 1 August 2024. European Commission. 2024 https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en Accessed 26 Jan 2025
17. Briefing EU Legislation in progress, New Product Directive, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf. Accessed 5 Oct 2024.
18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 of the European Parliament and of the Council and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 of the European Parliament and of the Council (Artificial Intelligence Act) [2024] OJ L 202, 53. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng. Accessed 24 Apr 2025.

19. Nnawuchi U, George C. A Grand Entrance Without A Blueprint: A Critical Analysis of the right to ExplanationIn Article 86 Of The European Union Artificial Intelligence Act
20. Andrews C. European Commission Withdraws AI Liability Directive from Consideration. IAPP. https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration. Accessed 5 Oct 2024
21. European Commission, 'Proposal for a Directive of the European Parliament And of the Council on liability for defective products COM/2022/495 final (AI Product Liability Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0495. Accessed 24 Apr 2025.
22. European Parliament. New Product Liability Directive. Legislative Train Schedule, European Parliament 2023. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-new-product-liability-directive Accessed 26 Jan 2025
23. Malcheva M. AI Liability and Artificial Intelligence. European Journal of Law and Technology. 2020; 11
24. Novelli C, Casolari F, Hacker P, Spedicato G, Floridi L, Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4694565. Accessed 6 Oct 2024.
25. Kilpatrick J, Jones C. A Clear and Present Danger Missing Safeguards on Migration and Asylum in the EU's AI Act 2 Authors. 2022. https://www.statewatch.org/media/3285/sw-a-clear-and-present-danger-ai-act-migration-11-5-22.pdf. Accessed 20 July 2024
26. European Digital Rights (EDRi), Migration and Technology Monitor, the Platform for International Cooperation on Undocumented Migrants (PICUM) and Statewatch, 'Use of AI migration and border control: a fundamental rights approach to the artificial intelligence act'. https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf. Accessed 24 Apr 2025.
27. Arcila B. AI liability in Europe: how does it complement risk regulation and deal with the problem of human oversight? Computer Law and Security Review. Volume 54
28. The EU General Data Protection Regulation 2016. Accessed 5 Nov 2024.
29. Barrett et al. Emotional expressions reconsidered: challenges to inferring emotion from human facial movements, 2019. https://doi.org/10.1177/1529100619832930
30. Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Accessed 26 Sep 2024.
31. Sánchez-Monedero J, Dencik L. The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl. Inf Commun Soc Ibid. 2022;25:419–23.
32. Gallagher R, Jona L. We tasted Europe's new lie detector for travellers—and immediately triggered false positives, The Intercept. 2019. https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/. Accessed 14 Nov 2022.
33. Pause Giant AI Experiments: An Open Letter. Future of Life Institute. 2023. https://futureoflife.org/open-letter/pause-giant-ai-experiments/. Accessed 31 July 2023.
34. McGregor L, Murray D and Ng V. International human rights law as a framework for algorithmic accountability. 2019; pp. 309–43.
35. EDRi. Uses of AI in migration and border control: a fundamental rights approach to the artificial intelligence act. https://edri.org/wp-content/uploads/2022/05/Migration_2-%20pager-02052022-for-online.pdf. Accessed 15 Nov 2024.
36. Sorelle Friedler SV and others. The problems with a moratorium on training large AI systems. 2023. https://www.brookings.edu/articles/the-problems-%20with-a-moratorium-on-raining-large-ai-systems/. Accessed 31 July 2023.
37. Chesterman S. From ethics to law: why, when, and how to regulate AI (Forthcoming in *The Handbook of the Ethics of AI*, NUS Law Working Paper No. Edward Elgar Publishing Ltd 2023/014. 2023.
38. Hanna R, Kazim E. Philosophical foundations for digital ethics and AI ethics: a dignitarian approach. AI Ethics. 2021. https://doi.org/10.1007/s43681-021-00009-4.
39. Gkritsi E. The long and winding road to implement the AI Act. Euractiv, 2024. https://www.euractiv.com/section/digital/news/the-long-and-winding-road-to-implement-the-ai-act/. Accessed 2 May 2024.
40. Kaminski M. The developing law of AI regulation: a turn to risk regulation. Lawfare, 2022. https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation. Accessed 15 Nov 2024.
41. Marta Z, Mökander J, Novelli C, Casolari F, Taddeo M, Floridi L. AI liability directive: a rational proposal to the causal conundrum. 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4470725. Accessed 15 Nov 2024.
42. Gkritsi E. The long and winding road to implement the AI Act. Euractiv. 2024. https://www.euractiv.com/section/digital/news/the-long-and-winding-road-to-implement-the-ai-act/. Accessed 2 May 2024
43. Kelder K. Relative importance of the AI act right to explanation. https://digi-con.org/on-the-relative-importance-of-the-ai-act-right-to-explanation/. Accessed 28 Sep 2024.
44. EDRi et al. An EU artificial intelligence act for fundamental rights: a civil society statement. 2021. https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf. Accessed 30 Oct 2023
45. Edwards L. Regulating AI in Europe: four problems and four solutions. 2022
46. Ada Lovelace Institute; Marco Almada and Nicolas Petit, The EU AI Act: Between product Safety and Fundamental Rights. 2022. https://ssrn.com/abstract=4308072. Accessed 30 Oct 2023
47. EU AI Liability Directive on hold: what lies ahead, https://www.linklaters.com/en/insights/blogs/productliabilitylinks/2024/june/eu-ai-liability-directive-on-hold. Accessed 18 Sept 2024.
48. Malcheva M. AI Liability and Artificial Intelligence. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4400410. Accessed 18 Oct 2024.
49. Heller J. Catch-22. New York: Simon & Schuster; 1961.
50. Burrell J. How the machine 'thinks': understanding opacity in machine learning algorithms. Big Data Soc. 2016. https://doi.org/10.1177/2053951715622512.
51. European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR) (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221.
52. Charter of Fundamental Rights of the European Union [2000] OJ C 364/1.
53. Norros O. Admissibility of a National limitation period under the principle of effectiveness in EU Law. Eur Rev Private Law. 2020;28(5):1113–42.
54. Tyler TR. What is procedural justice? Criteria used by citizens to assess the fairness of legal procedures. Law Soc Rev. 1988;22(3):301–55.

55. Nawaz S. The Proposed EU AI Liability Rules: Ease or Burden? (European Law Blog, 7 November 2022). https://europeanlawblog.eu/2022/11/07/the-proposed-eu-ai-liability-rules-ease-or-burden/. Accessed 12 Apr 2024
56. Santoni de Sio F, Mecacci G. 'Four responsibility gaps with artificial intelligence: why they matter and how to address them. Philos Technol. 2021;34:1057.
57. EDPS. Opinion of the EDPS 42/2023 on the Proposal for two Directives on AI liability rules. https://www.edps.europa.eu/system/files/2023-10/23-10-11_opinion_ai_liability_rules.pdf. Accessed 27 Sep 2024.
58. Binns R, Vaele M. Is that your final decision? Multi-stage profiling, selective effects, and Art 22 of the GDPR. Int Data Privacy Law. 2021;11(4):319–32.
59. Court of Justice of the European Union, Judgment in Case C-634/21, OQ v. Land Hessen and SCHUFA Holding AG. 2023.
60. Fort K. Migration management in the era of AI: how emerging technologies shape the border space (LSE International Development12 January 2024) https://blogs.lse.ac.uk/internationaldevelopment/2024/01/12/migration-management-in-%20the-era-of-ai-how-emerging-technologies-shape-the-border-space/. Accessed 27 July 2024.
61. Nnawuchi U. Proposing a Protocol to the CoE Convention on Artificial Intelligence, Establishing and Implementing a Legal Right to Explanation of Machine Learning Social Science Research Network. 2024 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4747094. Accessed 13 July 2024.
62. Cath C. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. Philos Technol. 2018;6(4):311–32.
63. Panigutti C. The role of explainable AI in the context of the AI Act. FAccT '23: proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency 2023; 1139–1150.
64. Inam R, Terra A, Mujumdar A, Fersman E, Feljan AV. Explainable AI: How humans can trust AI. Ericsson White Paper GFTL-21:000529Uen.
65. Vredenburgh K. The right to explanation'. Wiley J Polit Philos. 2022;30(2):209–29.
66. Eubanks V. Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martins Press; 2018.
67. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the general data protection regulation. Int Data Privacy L. 2017;7:76.
68. Matulionyte R. Reconciling trade secrets and explainable AI: face recognition technologies as a case study. Eur Intellect Prop Rev 46. 2022;44(1):14.
69. Case C-203/22 Dun & Bradstreet Austria GmbH v. Rolands SIA (ECJ, 7 December 2023) ECLI:EU:C:2023:963.
70. König M. The borders, they are A-Changin! The emergence of socio-digital borders in the EU. Internet Policy Rev. 2016. https://doi.org/10.14763/2016.1.403.
71. David E Spiro, 'Criminalizing Immigration: The Social Construction of Borders and National Security. SSRN. 2009. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1515466. Accessed 16 Nov 2024.
72. Angwin J, Larson J, Mattu S, Kirchner L. Machine Bias. ProPublica. 2016.
73. Molner P. The EU's AI Act and Its Human Rights Impacts on People Crossing Borders in Brief DIALOGUE on TECH and MIGRATION a Project of the Migration Strategy Group on International Cooperation and Development. 2022.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.