German Law Journal (2024), pp. 1–11
doi:10.1017/glj.2023.102

ARTICLE

Addressing Algorithmic Errors in Data-Driven Border Control Procedures

Mirko Forti

Department of Economics, Engineering, Society and Business Organization, University of Tuscia, Viterbo, Italy
Email: mirko.forti@unitus.it

(Received 02 March 2023; accepted 08 June 2023)

Abstract

The gradual digitization of EU migration policies is turning external borders into AI-driven filters that limit access to fundamental rights for people from third countries according to risk indicators. An unshakeable confidence in the reliability of technological devices and their ability to predict the future behaviour of incoming foreigners is leading towards the datafication of EU external frontiers. What happens if the supposedly infallible algorithms are wrong? The article aims to understand the consequences of algorithmic errors on the lives of migrants, refugees and asylum seekers arriving in the European Union. This contribution investigates the socio-political implications of deploying data-driven solutions at the borders in an attempt to problematize the techno-solutionist approach of EU migratory policies and its fundamental rights impact on affected individuals.

Keywords: Data; artificial intelligence; borders; errors; migration; algorithms; European Union

A. Introduction

The European Union (EU) and its Member States increasingly rely on data-driven technologies to perform border control procedures and manage incoming migration flows. The progressive ratification[1] of EU external frontiers aims to supervise the movements of third-country nationals in the aftermath of the Schengen agreement[2] and the consequent abolition of internal borders between EU Member States.[3] Implementing digital frontiers with data-driven risk assessment procedures aims to deflect external safety and stability menaces, thus preventing those who represent a threat from entry. The increasing digitalization of migration management influences how the EU and its Member States assess international protection requests from incoming third-country nationals. Consequently, borders are gradually becoming data collection and elaboration

[1] Dennis Broeders, Huub Dijestelbloem, The datafication of mobility and migration management: The mediating State and its consequences, *in* Irma Van Der Ploeg & Jason Pridmore (eds), DIGITIZING IDENTITIES: DOING IDENTITIES IN A NETWORKED WORLD (2016) Routledge, 242–60.

[2] Convention implementing the Schengen Agreement of June 14, 1985, between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, Sept. 22, 200, 19–62.

[3] Evelien Brouwer, *Schengen and the administration of exclusion: Legal remedies caught in between entry bans, risk assessment and Artificial Intelligence*, (2021) 23 EUROPEAN JOURNAL OF MIGRATION AND LAW, 485–507; Niovi Vavoula, *Artificial Intelligence (AI) at Schengen borders: Automated processing, algorithmic profiling and facial recognition in the era of techno-solutionism*, (2021) 23(4) EUROPEAN JOURNAL OF MIGRATION AND LAW, 457–84.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

sites that serve social sorting processes for security purposes.[4] More specifically, the EU is gradually implementing an interoperable network of large-scale IT systems collecting all the relevant information retrieved from non-EU citizens entering EU territory.[5] The Schengen Information System (SIS II) provides public security authorities with data on people and objects passing through EU frontiers from abroad.[6] The Visa Information System (VIS) permits sharing of visa information between Schengen States.[7] The VIS aims to prevent visa shopping episodes and irregular migration through biometric matching for identification and verification purposes. The "Eurodac" is a crucial feature in managing EU asylum applications.[8] It processes the fingerprints of asylum seekers and irregular migrants who have passed through EU frontiers, preventing the duplication of asylum requests. The Entry/Exit System is currently under development; it will register through electronic means the time and place of entry and exit of third country-nationals to calculate the length of their authorized stay.[9]

The EU and the Member States are looking toward technological solutions with an unwavering amount of trust in their capabilities to analyze the surrounding context and forecast possible developments. More specifically, EU migratory policies adopt data-realism assumptions, according to which data present truthful representations of reality.[10] EU digital border policies move from this confidence in the descriptive capability of data to build complex and interlinked infrastructures that collect and process personal data of different categories from third-country nationals entering EU territory.[11]

Artificial Intelligence (AI) technologies could be crucial to elaborating on such information. In general terms, modern machine-learning algorithms identify hidden patterns between large amounts of "raw" information and produce diagnostic outcomes based on processed data.[12] In other words, these algorithms study the statistical inferences between training data (information used by the software to develop reasoning structures) to find correlations between a specific input

[4] Matthias Leese, Simon Noori & Stephan Scheel, *Data matters: The politics and practices of digital border and migration management*, (2022) 27 (1) GEOPOLITICS, 5–25.

[5] Niovi Vavoula, *The "puzzle" of EU large-scale information systems for third-country nationals: Surveillance of movement and its challenges for privacy and personal data protection*, (2020) 3 EUROPEAN LAW REVIEW, 348–72.

[6] Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L312, 7/12/2018, 14–55.

[7] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ L 218, 13/8/2008, 60–81.

[8] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 180, 29/6/2013, 1–30.

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

[10] Georgios Gloutfsios & Stephan Scheel, *An inquiry into the digitisation of border and migration management: Performativity, contestation and heterogenous engineering*, (2021) 42 (1) THIRD WORLD QUARTERLY, 123–40.

[11] Vavoula, *supra*, note 3.

[12] Philip Boucher, *Artificial Intelligence: How does it work, why does it matter, and what can we do about it?* (2020) European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf (last accessed Feb. 9, 2023).

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

and the resulting output.[13] Well-functioning AI software can accurately identify the patterns retrieved from the training datasets in new circumstances.[14] The resulting statistical model should be able to forecast the outcome of a future prompt. Regarding border control and migration management goals, AI-powered software could verify the identity of already known persons and assess unknown individuals against risk indicators to evaluate threats to EU security and internal stability.[15]

The deployment of AI algorithms could benefit migration management operations, including the fast and efficient analysis of asylum applications and more expedited access to available information to make policy choices. According to a technical report,[16] AI technologies are crucial features of large-scale IT systems that perform several functions, which include IT infrastructure and service management, protection from cyberattacks, and optimization of data processing performances. The soon-to-be-released European Travel Information and Authorization System (ETIAS),[17] a visa waiver pre-evaluation framework for visa-exempt foreigners entering the EU territory, will conduct AI-driven risk assessment procedures to detect incoming security threats. This system will process data through AI algorithms against risk indicators to evaluate if the third-country nationals under investigation could threaten EU stability and safety. However, in the migration context, AI technologies raise risks for the rights of vulnerable people, including the migrants themselves. The recent proposal for a European Regulation on Artificial Intelligence (the AI Act) considers the use of AI systems in the field of migration to be a potential high risk to the health, safety, and fundamental rights of the people concerned (Annex III, Art. 7).[18] Thus, the legislative draft requires appropriate risk management procedures (Art. 9) to implement high-risk AI solutions. However, the AI Act does not provide any legal remedies in case of algorithmic errors.

This Article interrogates the EU regulatory framework on its adequacy in protecting the fundamental rights of people affected by misleading and erroneous algorithmic outcomes at the EU's external frontiers. The aim is to understand the legal consequences and policy implications of algorithmic errors in the context of EU migratory policies. The first part of this contribution deals with the notions and types of different AI flaws and addresses their potential causes. The second section analyzes how algorithmic errors could infringe on the fundamental rights framework. More specifically, this part of the Article highlights how incorrect AI outputs could exacerbate the vulnerabilities of migrants, refugees, and asylum seekers. Furthermore, the analysis explains the shortcomings of the existing legal remedies at the EU level to challenge misleading AI outcomes in migration management procedures due to an unclear accountability framework. The last section of the contribution formulates a few concluding remarks that suggest possible solutions to the problems raised by algorithmic errors. More specifically, the Article argues for a shift when implementing AI solutions at the borders; migrants should be considered as humans with specific rights, not data that requires processing.

[13] Matteo Pasquinelli, *How a machine learns and fails – A grammar of error for Artificial Intelligence*, (2019) 5 Spheres, https://spheres-journal.org/wp-content/uploads/spheres-5_Pasquinelli.pdf (last accessed Feb. 10, 2023).

[14] *Id.*

[15] Costica Dumbrava, *Artificial Intelligence at EU Borders. Overview of applications and key issues* (2021) European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/690706/EPRS_IDA(2021)690706_EN.pdf (last accessed Feb. 9, 2023).

[16] EU-Lisa, *Artificial Intelligence in the operational management of large-scale IT systems*, July 2020, https://op.europa.eu/en/publication-detail/-/publication/6173f7a8-d78a-11ea-adf7-01aa75ed71a1 (last accessed June 1, 2023).

[17] Regulation (EU) 2018/1240 of the European Parliament and of the Council of September 12, 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236, 19/9/2018, 1–71.

[18] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 21/04/2021, COM (2021) 206 final.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

B. Algorithmic Errors and their Potential Causes

Artificial Intelligence is a general term that indicates a vast array of technologies and software deployed for an ever-growing variety of scopes. Therefore, providing a legal definition of algorithmic errors that could fit within different contexts is challenging. Scott and Yampolskiy assess errors as static conditions that may lead to AI failure, resulting in the algorithmic system's inability to perform its functions in the surrounding circumstances.[19] Insofar as border control is concerned, this Article considers algorithmic errors when AI-driven frontiers deliver misleading and erroneous outputs. Thus, it wrongly identifies migrants and results in poorly performing risk-assessment operations. Moving from these assumptions, I will make a few considerations about the limits of modern AI technologies.

Machine learning technologies use complex mathematical functions to establish the correlation between input and output according to processed datasets. AI algorithms provide human observers with a statistical explanation of the relationship intercurring between two or more elements. However, such technologies cannot describe the logical causation between input and output.[20] Correlations do not necessarily infer a cause-effect relationship between such objects.[21] Policy choices can rely on falsely predicting algorithmic outcomes.

AI algorithms can process vast amounts of data because they previously compressed such information. Data compression mechanisms may imply the loss of differences and peculiarities within the reality under analysis.

More specifically, such algorithms interpret data relevant to a specific subject against categories and benchmarks elaborated on with information about other elements.[22] Insofar as risk assessment procedures are concerned, these AI-powered programs make predictions about a person based on group data. Consequently, subjects not belonging to the statistical majority represent an anomaly to the AI software.[23] Regarding migration management purposes, digital borders may become data-driven filters[24] that limit access to fundamental rights according to potentially discriminatory factors such as race, ethnicity, language, nationality, and religion.[25]

Machine learning programs may fall within so-called feedback loops, which occur when algorithmic outputs misinterpret the surrounding reality and influence the implementation of training datasets to update and develop algorithms.[26] Misleading outputs may become erroneous inputs for other machine-learning routines. Algorithms are overfitting when they rely too much on training data and only look for exact matches while disregarding similarities and correlations between elaborated information.[27] On the contrary, underfitting problems occur when AI software cannot identify patterns from the training data and fit them within the surrounding reality.[28]

[19] Peter J. Scott & Roman V. Yampolskiy, *Classification schemas for Artificial Intelligence failures*, (2019) 2 DELPHI – INTERDISCIPLINARY REVIEW OF EMERGING TECHNOLOGIES, 186–99.

[20] Pasquinelli, *supra*, note 8.

[21] Naomi Altman & Martin Krzywinski, *Association, correlation and causation*, (2015) 12 NATURE METHODS, 899–900.

[22] Tetyana Krupiy, Why the proposed Artificial Intelligence Regulation does not deliver on the promise to protect individuals from harm, July 23, 2021, European Law Blog, https://europeanlawblog.eu/2021/07/23/why-the-proposed-artificial-intelligence-regulation-does-not-deliver-on-the-promise-to-protect-individuals-from-harm/ (last accessed Feb. 15, 2023)

[23] Anja Bechmann, *Data as humans: representation, accountability, and equality in Big Data*, *in* Rikke Frank Jørgensen (ed.), HUMAN RIGHTS IN THE AGE OF PLATFORMS, (2019) MIT Press, London, 73–94.

[24] William Walters, *Rethinking borders beyond the State, (*2006) 4 COMPARATIVE EUROPEAN POLITICS, 141–59.

[25] Leese, Noori & Scheel, *supra*, note 4.

[26] European Union Agency for Fundamental Rights, *Bias in algorithms. Artificial Intelligence and discrimination*, December 8, 2022, https://fra.europa.eu/en/publication/2022/bias-algorithm (last accessed Feb. 15, 2023).

[27] Xue Ying, *An overview of overfitting and its solutions*, (2019) 1168 (2) JOURNAL OF PHYSICS: CONFERENCE SERIES, 1–7.

[28] Daniel Bashir and others, *An information-theoretic perspective on overfitting and underfitting,* (2020) AI 2020: ADVANCES IN ARTIFICIAL INTELLIGENCE, 347–58.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

Data misinterpretation could produce erroneous algorithmic outcomes and propagate and amplify biases. This term indicates one reason to choose a specific data generalization instead of another, thus losing the inherent complexities of the reality under analysis.[29]

Pasquinelli proposes a tripartite classification of biases that could influence the working routine of machine learning algorithms:[30] i) world biases indicate how the algorithms reproduce and propagate prejudices and inequalities already occurring in the real world. Datasets represent reality, including its stereotypes; ii) data biases occur during elaborating and implementing training datasets. Marcuse explained through the concept of technological rationality how the deployment of specific technologies could influence the rationality of society.[31] Deploying ever more sophisticated and advanced technologies shapes the state and its citizens' relationship.[32] Data processing activities are not neutral operations but adopt peculiar perspectives and social hierarchies to analyze surrounding circumstances. Using unreliable taxonomies and data categorizations could portray an inaccurate view of reality, disregarding data peculiarities and features. Foucault explained the normative potentialities of data, addressing them not as a matter of fact but as a matter of concern;[33] iii) algorithmic biases propagate the above-mentioned discrepancies through computational failures and information compression mechanisms.

Therefore, the highest data quality standards are crucial in implementing reliable and accurate AI-driven technologies. The General Data Protection Regulation (GDPR) states reliability and accuracy as founding principles of data processing activities (Art. 5(1)(d)).[34] However, EU information databases in the area of Freedom, Security and Justice have been suffering from data quality issues for a long time.[35] Spelling errors, mistakes in translating names into the Latin alphabet, the recording of erroneous and misleading birth certificates, technical failures, and lack of training in dealing with digital infrastructures are only a few reasons to explain low-quality data within such border management information systems.[36] AI algorithms receiving data inputs with such flaws will logically deliver unreliable outcomes.

Data processing aims to give a truthful representation of the reality under scrutiny. However, deciding what is the correct picture of reality is a choice that has policy and legal implications.[37] Accepting a specific margin of error, intended as the difference between reality and its representation delivered by data elaboration operations, could have fundamental rights and consequences worth mentioning.

[29] Diana F. Gordon & Marie DesJardinis, *Evaluation and selection of biases in machine learning,* (1995) 20 MACHINE LEARNING, 5–22.

[30] Pasquinelli, *supra*, note 8.

[31] Herbert Marcuse, *Some social implications of modern technology*, (1941), IX STUDIES IN PHILOSOPHY AND SOCIAL SCIENCES, 138–62.

[32] Matthias Leese*, Data quality in governance: A definition and a research agenda,* (2022) CURATE Working Paper 1, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/581434/CURATEWorkingPaperNo.1_DataQuality.pdf?sequence=5&isAllowed=y (last accessed Feb. 18, 2023).

[33] Bruno Latour, *Why has critique run out of steam? From matters of facts to matters of concern*, (2004) 30(2) CRITICAL INQUIRY, 225–48.

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 04/05/2016, 1–88.

[35] Vavoula, *supra,* note 3.

[36] European Union Agency for Fundamental Rights, *Fundamental rights and the interoperability of EU information systems: Border and security*, July 7, 2017, https://fra.europa.eu/en/publication/2017/fundamental-rights-and-interoperability-eu-information-systems-borders-and (last accessed Feb. 18, 2023).

[37] Leese, *supra,* note 25.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

C. Algorithmic Errors and Fundamental Rights Consequences

Erroneous algorithmic results can dramatically affect the lives of migrants, refugees, and asylum seekers, exacerbating their vulnerabilities behind misplaced confidence in the efficiency and reliability of data-driven frontiers. The widespread use of technological solutions to assist border control may produce incorrect AI results that infringe on fundamental rights and freedoms, resulting in unfair treatment: that is, the right to life and liberty, the right to privacy, and principles of non-discrimination.[38] In addition, the inherent opaqueness of AI algorithms may make identifying possible errors difficult, which prevents affected individuals from challenging biased administrative decisions.

I. Algorithmic discrimination and false prophecies

"We are black and border guards hate us. Their computers hate us too." Adissu, an Eritrean migrant living undocumented in Brussels, describes how EU border guards treated him and his fellow migrants.[39] Technological devices in border management risk repeating and amplifying systemic prejudices and discriminatory attitudes already present in modern society.

As explained before, technologies influence society. More specifically, socio-political, economic, and cultural variables can influence the working routine of AI-powered devices. A study shows how a decision-making algorithm used in several US hospitals usually shows that White patients are more likely to be potential users of social programs that address complex health issues.[40] The researchers found that the algorithm assigned lower risk values to Black people despite having the same medical issues as White patients. AI software calculated how much a single person spent over the year in health expenses to evaluate appropriate risk scores on the assumption that fewer expenses indicate fewer health needs. However, a close examination of the dataset showed that Black patients exhibited far more severe health issues than White subjects despite the same healthcare expenditures. According to the data, Black people spent an average of $1,800 (US) less per year compared to White individuals with identical health problems. The lack of trust in the medical system and racial discrimination from healthcare personnel are but a few symptoms of a discriminatory attitude that impacts Black patients. Thus, the algorithm has introjected and reproduced systemic racism that prevents Black people from accessing medical services for Black people.

Notwithstanding these concerns, the EU places great trust in the reliability of algorithmic outcomes, relying on technological neutrality beliefs and disregarding any political implications of data processing activities for border management purposes.[41] As an example of this dangerous techno-solutionism tendency,[42] the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-Lisa) is considered as "noise data" to be eliminated from their info-systems due to migrants' unwillingness to share information about themselves.[43] Such an approach disregards how data processing operations impact the affected individuals.

[38] Petra Molnar, *Technological testing grounds. Migration management experiments and reflections from the ground up*, EDRI, November 9, 2020, https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf (last accessed Feb. 21, 2023).

[39] EDRI, *Technological testing grounds. Border tech is experimenting with people's lives*, November 9, 2020, https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/ (last accessed Feb. 21, 2023).

[40] Heidi Ladford, *Millions of black people affected by racial bias in health-care algorithms*, (2019) 574 NATURE, 609–609.

[41] Adil Habib, The ongoing digitisation of Europe's borders, Digital Freedom Fund, June 18, 2021, https://digitalfreedomfund.org/the-ongoing-digitisation-of-europes-borders/ (last accessed Feb. 21, 2023).

[42] Ana Valdivia and others, *Neither opaque nor transparent: A transdisciplinary methodology to investigate datafication at the EU borders*, (2022) 9 (2) BIG DATA & SOCIETY, 1–22.

[43] Hito Steyerl, A sea of data: pattern recognition and corporate animism, *in Clemens Apprich & others* (eds.), PATTERN DISCRIMINATION, (2019), University of Minnesota Press, 1–22, https://pure.rug.nl/ws/portalfiles/portal/125646593/9783957961457_Pattern_Discrimination.pdf (last accessed Feb. 22, 2023).

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

Insofar as border control procedures are concerned, AI-powered frontiers could exacerbate the inherent vulnerabilities of people on the move, preventing them from accessing their fundamental rights. The working mechanisms of machine learning algorithms could propagate discriminatory biases, reinforcing prejudicial treatments against migrants, refugees, and asylum seekers. Profiling activities and risk assessment procedures targeting these categories may be considered unreliable data or a result of misinterpretations of reality. As explained before, feedback loops might mislead future diagnostic activities. Biased algorithms could lead to self-fulfilling algorithmic prophecies.[44] In other words, algorithms could label specific individuals or minority groups as potential security threats, thus justifying additional security controls against them for no other reason than algorithmic outcomes.[45] Such a trend could produce networked discrimination phenomena, according to which discriminatory treatments originate from previous biases.[46] Restrictions on freedom of movement, actions of deprivation of liberty, and surveillance procedures may be justified by incorrect algorithmic results, upon which the EU bases its migration policy due to its unshakeable confidence in the reliability and impartiality of technology.

II. The algorithmic black box and its consequences on procedural rights

Machine learning algorithms find hidden patterns between a given input and a specific output. More specifically, AI-powered solutions elaborate on complex mathematical functions that find statistical correlations between data using their vast computational power, which is way beyond human capability. An additional layer of complexity is due to the mutating nature of the algorithms themselves. More specifically, such algorithms adapt their working routine to the mutating circumstances, developing and improving their diagnostic capabilities according to data inputs subject to concept drifts.[47]

The term "black box barrier" indicates the impossibility for external human observers to identify, understand, and replicate the reasoning patterns chosen by machine learning algorithms.[48] The rationale behind a specific output remains obscure behind the curtains of technological complexities.

Explainable Artificial Intelligence is a highly debated issue in legal scholarship.[49] Implementing the principle of explanation within the algorithmic working routine would ensure meaningful human control over the AI-driven decision-making process.[50] Figuring out the reasons behind a specific algorithmic output would make human actors morally accountable for its implementation.

[44] Owen C. King & Mayli Mertens, *Self-fulfilling prophecy in practical and automated prediction*, (2023) 26 ETHICAL THEORY AND MORAL PRACTICE, 127–52. https://link.springer.com/article/10.1007/s10677-022-10359-9 (last accessed Feb. 22, 2023).

[45] Will Douglas Heaven, Predictive policing algorithms are racist. They need to be dismantled, MIT Technology Review, July 17, 2020, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (last accessed Feb. 22, 2023).

[46] Lorna McGregor et al., *International Human Rights Law as a framework for algorithmic accountability*, (2019) 68 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY, 309–43.

[47] Pierre-Xavier Loeffel, Adaptive machine learning algorithms for data streams subjects to concept drifts, (2017) Doctoral Thesis – Université Pierre et Marie Curie – Paris VI, https://theses.hal.science/tel-01812044/document (last accessed 23/02/2023).

[48] Yavar Bathaee, *The Artificial Intelligence black box and the failure of intent and causation,* (2018) 31(2) HARVARD JOURNAL OF LAW AND TECHNOLOGY, 890–938.

[49] Sandra Wachter, Brent Mittelstadt & Lucia Floridi, *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, (2017) 7(2) INTERNATIONAL DATA PRIVACY LAW, 76–99; Gianclaudio Malgieri*, Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, (2019) 35(5) COMPUTER LAW & SECURITY REVIEW, 1–26; Adrien Bibal et al., *Legal requirements on explainability in machine learning,* (2021) 29 ARTIFICIAL INTELLIGENCE AND LAW, 149–69.

[50] Filippo Santoni de Sio & Jeroen van den Hoven, *Meaningful human control over autonomous systems: A philosophical account,* (2018) 5(15) FRONTIERS IN ROBOTICS, 1–14.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

Insofar as AI-powered devices for public affairs are concerned, explainable algorithms comply with the right to good administration, raising an obligation for governments and public offices to justify their decisions (Art. 41 EU Charter of Fundamental Rights – EUCFR). Understanding the reasoning behind algorithmic outcomes would make it possible to question and challenge legal and administrative measures based on such AI outputs, thus complying with the right to an effective remedy and a fair trial (Art. 47 EUCFR). The inherent opaqueness and undetectability of AI algorithms prevent the identification of errors and biases, thus permitting the propagation of incorrect algorithmic results.

The importance of algorithmic outputs in the decision-making process of human operators (for example, border guards, administrative courts, etc.) is ever-growing. Human decision-makers may suffer from automation bias and unreasonably regard algorithmic outputs as unquestionably correct,[51] thereby failing to consider the risks of flaws and errors in the working routine of the algorithms themselves. Due to this worrying tendency, the affected individuals may face additional difficulties in challenging judicial and administrative decisions. Who should be held responsible? The human judge or the algorithm?

Agents working in the field of migration management may also lack the appropriate knowledge to evaluate the correctness of the algorithmic information they have access to in their decision-making processes. Therefore, the EU and its Member States should provide their migration management agents with appropriate training opportunities. Furthermore, standardized guidelines on the role of algorithmic outcomes in international protection request assessments would ensure the applicants' rule of law safeguards, including legal certainty and procedural predictability.

D. The Lack of Appropriate Legal Remedies to Challenge Algorithmic Errors and their Consequences

Migrant people face significant difficulties accessing justice to protect their rights from abuses by the EU and its Member States in data-driven border control procedures. More specifically, interested individuals may struggle to find suitable reasons to appeal adverse migration decisions based on data processing activities due to the inherent opaqueness of the algorithmic working routine. It may be technically impossible to detect AI mistakes and identify the subjects responsible for them. Insofar as EU digital borders are concerned, the interoperable nature of databases operating in the Areas of Freedom, Security and Justice causes additional complexities from a procedural perspective. More specifically, these IT systems contain data from several sources and serve various purposes. These variables may prevent the identification of the subject accountable for having entered unreliable data within the networked digital archives.

The Court of Justice of the European Union has jurisdiction over the European Border and the Coast Guard Agency (Frontex) and its data-driven border control operations. According to EU Regulation 2019/1896 (Frontex Regulation), the European Border Surveillance System (EUROSUR) should function as a surveillance framework and communication network for the exchange of information and operational cooperation between Frontex and EU Member States to improve situational awareness and increase reaction capabilities for border management aims (Art. 18). More specifically, EUROSUR has to monitor, detect, identify, track, and intercept any unauthorized border crossing of EU external frontiers (Art. 19). Frontex, acting as a Eurosur coordinator, can take advantage of numerous surveillance tools such as drones, cameras, and sensors to collect crucial data to provide the EU Commission and its national coordination centers

[51] Kathleen L. Mosier & Linda J. Skitka, *Automation use and automation bias*, (1999) 43(3) PROCEEDINGS OF THE HUMAN FACTORS AND ERGONOMICS SOCIETY MEETING, 344–48.

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

with a detailed and updated analysis of the pre-frontier areas and the EU's external borders (Arts 26–27). In spite of the above considerations, existing legal remedies at the EU level may fall short of efficiently addressing data analysis errors made by Frontex (and their consequences). According to the CJEU, interested subjects could request the annulment of unclear, insufficiently detailed, or unsubstantiated reasons that caused the EU to act (Art. 263 TFEU).[52] However, Nicolosi rightly points out that annulment actions against Frontex operations could be in vain.[53] Frontex border management duties take the form of factual conduct, which does not often require the adoption of legally binding acts and is thus not compliant with the requirements prescribed by Art. 263 TFEU. Insofar as the scope of this contribution is concerned, AI-powered risk assessment procedures, digital pushbacks, and other data-driven forms of border control actions may not be amenable to annulment action. An action for damages (Art. 340 (2) TFEU) may provide shortcomings in protecting individuals from the consequences of algorithmic errors. They may have difficulty proving that the harmful conduct is attributable to Frontex because of the opacity of the algorithms. In addition, the coexistence of several actors cooperating for the same goals could make it impossible to distinguish between the EU and its Member States' competences (and related responsibilities).[54]

The European Commission recently released a proposal for a directive on adapting non-contractual civil liability rules to Artificial Intelligence, introducing the so-called "fault-based liability" approach (Recital 7), according to which claimants must prove the defendants' prior guilty behavior before holding them liable.[55] The draft would allow interested subjects to request developers of high-risk AI products to disclose relevant evidence to prove alleged harmful events deriving from their products (Art. 3). Furthermore, a rebuttable presumption of causality applies when claimants can demonstrate defendant failures in complying with the AI act norms (Art. 4).

Notwithstanding these measures, migrants face a difficult journey to obtain damages due to harmful algorithmic events.[56] Migrants, refugees, and asylum seekers do not have the means to break through the algorithmic Black barrier, identify those potentially responsible for border control and surveillance activities, and demand the necessary evidence from them to prove their responsibility for the harm caused by AI-driven border operations.

E. Concluding Remarks

This contribution demonstrates the inadequacy of the current EU legal framework in protecting affected individuals from the consequences of algorithmic errors that occur at the EU's external borders. Several technical and legal factors contribute to such a critical situation. On the one hand, the inherent opaqueness of the mechanisms by which the AI-powered software operates could prevent human observers from timely identifying and fixing algorithmic errors. Such AI programs continually change their cognitive processes to adapt to mutating external circumstances, making it technically difficult to detect AI errors and their causes. Furthermore, the networked nature of digital infrastructures at EU borders may favor the propagation of misleading AI outcomes.

On the other hand, the EU legal framework struggles to keep pace with rapidly evolving AI technologies. The lack of a proper legal definition of algorithmic errors testifies to the difficulties

[52] Court of Justice of the European Union, Order of the General Court (Ninth Chamber) of 7 April 2022, *SS and ST v European Border and Coast Guard Agency*, Case T-282/21, para. 33.

[53] Salvo Nicolosi, *Frontex and migrants' access to justice*, September 7, 2022, Verfassungsblog, https://verfassungsblog.de/frontex-and-migrants-access-to-justice/ (last accessed Feb. 28, 2023).

[54] *Id.*

[55] European Commission, Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to Artificial Intelligence, COM (2022) 496 final, September 28, 2022.

[56] Maximilian Gahntz & Claire Pershan, *The long road to redress: Mozilla's comments on the EU's proposal for an AI liability directive'*, https://foundation.mozilla.org/en/blog/the-long-road-to-redress-mozillas-comments-on-the-eus-proposal-for-an-ai-liability-directive/ (last accessed Mar. 1, 2023).

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

of integrating such an ever-changing world within legal norms and regulations. This crucial shortcoming also relies on the "technosolutionist" approach of EU policies that move responsibilities from human actors to technologies.[57]

The unwavering confidence in the reliability and impartiality of AI outcomes shown by EU policymakers and regulators prevents the problematization of the accuracy of AI-driven devices operating for public governance goals. According to a document on implementing biometric identification mechanisms within the Entry/Exit System,[58] the European Commission accepts a margin of error of 0.1% for false positive matches (biometric matches not indicating the subject under exam) and 1% for missed identification outcomes. Such negligible percentages may extend to a significant number of individuals when addressing vast amounts of data (a 1% margin of error in 100,000 searches may affect 1,000 people). Tolerating specific margins of error implies political consequences: the EU and its Member States consider the migration context as an ideal laboratory to experiment on technological solutions without considering the effects that such technologies have on people on the move.[59]

The deployment of data-driven technologies is gradually transforming Eu external frontiers in social sorting sites that classify migrants accordingly to their data on the bases of policies of control and mistrust. The progressive "datafication" process of EU external frontiers is transforming borders into social sorting sites that address migrants as data to be processed to create their "data double" to manage based on policies of control and mistrust.[60] Data-driven borders contribute to identifying individuals labelled as risks to EU stability and security, thus justifying restrictive migration policies because of assumptions of technological reliability. This contribution rejects the "dataism" paradigm,[61] believing in data as faithful representations of reality. Moving from these thoughts, a "dataistic" approach assumes that data processing activities can predict the future behaviors of targeted individuals. This Article suggests addressing digital border control policies from a data justice perspective, bringing into discussion the neutrality and reliability of data. Such a point of view aims to understand the sociopolitical dynamics that influence data elaboration practices and their products. Insofar as the scope of this Article is concerned, a data justice approach investigates the mutual relationship between algorithmic errors and the surrounding circumstances. In other words, it aims to problematize AI's mistakes by understanding how these failures impact interested individuals while considering sociopolitical influences as possible causes of misleading algorithmic outputs.

Regarding data-driven border control practices, this Article also proposes a few solutions to mitigate the consequences of AI mistakes. First and foremost, clear governance frameworks should be prerequisites for deploying AI-powered technologies at EU external frontiers. This measure would help to attribute the responsibilities of the alleged wrongful conduct, thus overcoming algorithmic opaqueness. In addition, clear accountability schemes would provide interested individuals with indications on how to be held responsible for their rights and put data-driven borders under democratic scrutiny. Periodic checks should oversee the persistence of necessity and proportionality requirements to justify digital border control mechanisms.

[57] Philippa Metcalfe & Lina Dencik, *The politics of big borders: Data (in)justice and the governance of refugees*, (2019) 4 FIRST MONDAY, 1–25.

[58] Commission implementing decision laying down the specifications for the quality, resolution, and use of fingerprints and facial images for biometric verification and identification in the Entry/Exit System (EES), C/2019/1280 final, February 25, 2019.

[59] Petra Molnar, *Technology on the margins: AI and global migration management from a human rights perspective*, (2019) 8(2) CAMBRIDGE INTERNATIONAL LAW JOURNAL, 305–30.

[60] Metcalfe & Dencik, *supra*, note 57.

[61] Dario Petri, *Big Data, dataism and measurement*, (2020) IEEE INSTRUMENTATION & MEASUREMENT MAGAZINE, 32–34, https://ieee-ims.org/sites/ieeeims/files/2020-08/Big%20Data.pdf (last accessed March 1, 2023).

https://doi.org/10.1017/glj.2023.102 Published online by Cambridge University Press

According to Art. 263 (5) TFEU, acts establishing EU bodies and agencies may lay down specific requirements that allow potentially interested individuals to bring actions against the measures producing legal effects against them. Moving from these considerations, introducing complaint procedures that address EU acts by relying on algorithmic errors could be crucial to ensure people on the move receive the highest fundamental rights protections and rule of law safeguards in the AI era.

Acknowledgments. An earlier version of this article was presented at the STS-Migtec & Processing Citizenship Workshop 2023. I wish to thank the reviewers for the comments. All errors are mine.

Funding Statement. None.

Competing Interests. None.

Cite this article: Forti M (2024). Addressing Algorithmic Errors in Data-Driven Border Control Procedures. *German Law Journal*, 1–11. https://doi.org/10.1017/glj.2023.102