

THE ROLE OF TECHNOLOGY IN MIGRATION MANAGEMENT. BALANCING SECURITY, ETHICS, AND HUMAN RIGHTS

Abstract:	<i>In the context of increasing migration and refugee flows, the integration of new advanced technologies into border security and their implications for human security requires considerable adjustment. AI-driven surveillance, biometric identification, and automated controls at the border have become part of strategic security measures. While these technologies seek to create “smart borders” for effective functionality, major concerns are raised for data privacy and civil liberties, and the potential for discriminatory practices against vulnerable populations. The analysis describes ethical and humanitarian dilemmas created by the technologization of border management concerning issues for access to international protection by asylum seekers under the 1951 Refugee Convention. It does so by drawing on comparative case studies from the member states of the European Union, illustrating how different geopolitical contexts shape the deployment and regulation of those technologies. This research calls for a balanced policy approach that incorporates the notion of border security with the principles of international human rights law, thereby advancing a framework that protects the dignity and rights of all individuals.</i>
Keywords:	Migration; human security; smart borders; refugee
Contact details of the authors:	E-mail: andreea.dragomir@ulbsibiu.ro (1) ana.morari@ulbsibiu.ro (2)
Institutional affiliation of the authors:	Lucian Blaga University of Sibiu, Faculty of Law (1) (2)
Institutions address:	Calea Dumbrăvii 34, Sibiu, Romania 550324 (1) (2)

Introduction

Migration management is fast assuming new dimensions, with advanced technologies taking center stage in the processes of border control worldwide. Added to protect against illegal migration and verify the identity of aliens and migrants, they raise difficult questions about their legal and ethical implications. A critical tension seems to arise between the need for strong measures of security and the imperatives of human rights to be upheld, including privacy, non-discrimination, and freedom of movement.

Enhanced migration is also impelling state and non-state actors to use ADT in innovative management frameworks. Abstract data use refers to the concept of abstract data types (ADTs), which are mathematical models that define data types based on their behavior rather than their implementation. A queue ADT can be used to handle the incoming traveler data in the order it is received hence ensuring efficiency in the processing at border checkpoints. When a traveler presents their identification, the system can rapidly carry out operations such as searching for alerts or verifying biometric information without exposing the underlying complexities of these processes¹.

The mechanism to manage the problems related to the massive influx of refugees and migrants, due to a political or economic connection in the state of origin, has increased the need to implement digital tools

¹ Yingxu Wang, Xinming Tan, Cyprian Ngolah, Philip Sheu, *The Formal Design Models of a Set of Abstract Data Types (ADTs)*, "International Journal of Software Science and Computational Intelligence (IJSSCI)", Vol. 2, No. 4, 2010, pp. 72-100, <https://doi.org/10.4018/jssci.2010100106> (30.10.2024)

capable of facilitating the exchange of information between agents, from artificial intelligence to other systems based on blockchain, web 3.0. RPA, etc.¹.

As a result, for example, the identity, visa status, and customs declarations of travelers can be stored on a blockchain, which unauthorized persons will find very difficult to alter. The unchangeable nature of blockchain means that once information is added, it cannot be changed without agreement from the network².

In the same way, Robotic Process Automation (RPA), a technology that automates repetitive, rule-based tasks commonly performed by humans using software robots or *bots*, can integrate data coming from different sources and systems without major infrastructure changes³. It can draw information from different databases—be it traveler records, security alerts, or even customs information—and present a single view of the information to the border officials⁴.

Technological adaptations—from biometric systems and AI-driven surveillance to remote sensors and data analytics—aim to bolster border security and streamline migration processes⁵.

As much as these technologies enhance security and efficiency, there are still concerns about their accuracy, especially in real situations where demographic diversity interferes with their efficacy. These potential negative impacts include biased outcomes, data privacy problems, systemic inequities, and transparency deficits—issues identified by stakeholders, especially within communities with historic disadvantages⁶.

“Smart borders” - erosion of due process

Smart borders have as part of their core highly innovative digital border technologies, from simple internet-enabled devices to advanced systems powered by algorithms, AI, and AD. Examples include machine learning, predictive analytics, facial recognition systems, biometric databases, drones, and other forms of surveillance mechanisms. Their integration furthers and optimizes the efficiency of border management⁷.

The increasing integration of digital technologies in border governance and their implications for migration politics highlights how states and private actors employ tools such as big data analytics and automated decision-making systems in border management. These technologies are utilized in identification documents, facial recognition systems, biometric databases, and surveillance mechanisms, aiming to enhance efficiency and security⁸.

Such smart border systems use biometric technologies for more accurate identification and verification of travelers through face recognition, fingerprints, or iris scans. Biometrics integrated with the border control

¹ Giuli Giguashvili, *Possibilities of Using Artificial Intelligence in the Process of International Migration Management*, “Innovative economics and management”, Vol. 10, No. 3, 2023, <https://doi.org/10.46361/2449-2604.10.3.2023.58-66> (30.10.2024)

² Sanket Pancharia, Deepak Kumar Byrappa, *Passport, VISA and Immigration Management Using Blockchain*, “2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM)”, 2017, pp. 8-17 <https://doi.org/10.1109/ADCOM.2017.00009>, (30.10.2024)

³ Hema G.B. Malini, *Automation of Big Data Analytics Using Robotic Process Automation*, “International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)”, Vol. 7, No. 2, 2021, pp. 602-605, <https://doi.org/10.32628/CSEIT2172124> (30.10.2024)

⁴ Georgios Glouftisios, *Governing border security infrastructures: Maintaining large-scale information systems*, “Security Dialogue”, Vol. 52, No. 5, 2020, pp. 452 – 470, <https://doi.org/10.1177/0967010620957230> (30.10.2024)

⁵ Bruno Oliveira Martins, Maria Gabrielsen Jumbert, *EU Border technologies and the co-production of security ‘problems’ and ‘solutions’*, “Journal of Ethnic and Migration Studies”, 48, 2020, pp. 1430-1447, <https://doi.org/10.1080/1369183X.2020.1851470> (30.10.2024)

⁶ United States Government Accountability Office, *Biometric Identification Technologies Considerations to Address Information Gaps and Other Stakeholder Concerns*, Report to Congressional Committees, 2024, <https://www.gao.gov/assets/gao-24-106293.pdf> (30.10.2024)

⁷ Lorna McGregor, Petra Molnar, *Digital Border Governance: A human rights based approach*, Online Study University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023, p. 8, <https://repository.essex.ac.uk/36656/1/Digital%20Border%20Governance%20-%20A%20Human%20Rights%20Based%20Approach.pdf> (30.10.2024)

⁸ Natasha Saunders, *Security, digital border technologies, and immigration admissions: Challenges of and to non-discrimination, liberty and equality*, “European Journal of Political Theory”, 2023 <https://doi.org/10.1177/14748851231203912> (30.10.2024)

system allow, under different EU initiatives such as the *Smart Borders Policy*, an automated entry/exit system with more reliability of data. These systems have been integrated with various frameworks, for instance, the *Schengen Border Code (SBC)*, allowing operations to proceed smoothly without compromising on the security level¹.

Smart borders have a reliance on biometric systems, which include facial recognition systems, that create a variety of risks. For example, Clearview AI scraped billions of images online to use in unauthorized facial recognition, while a breach at U.S. Customs exposed 100,000 facial images. It was reported that “studies had found facial recognition algorithms misidentify people of certain races at rates as much as ten times higher than others, with new concerns about discrimination”².

Furthermore, the systems exclude users who have disabilities or low technology literacy. Although laws such as the GDPR and some others regulate biometric data, inconsistent enforcement leaves gaps in privacy and accountability. These risks need to be addressed in a solution to make border management both ethical and secure³.

The performance and usefulness of smart borders are unquestionable, however raises concerns about the lack of transparency and accountability in deploying these digital border technologies. Limited public information is available regarding their use, often justified by states on grounds of national security and sovereignty. This opacity is further compounded when private actors are involved, consolidating knowledge and power within the private sector and hindering oversight⁴.

In response to these concerns, at the EU level, a pilot project has been set up to study and technically support operational systems involved in smart borders technology, with the aim of answering questions about their cost-effectiveness, reliability, and impact on fundamental rights. While at least at a technical level data security is provided some form of protection through this program, the lack of legal regulation raises concerns that critical decisions are being made in a way that bypasses meaningful public debate, limiting opportunities for citizens, civil society and legislators to scrutinize and shape the direction of these initiatives⁵.

Legal initiatives to regulate data sharing

The EU has increasingly applied digital systems to monitor, regulate, and control the flows of migration, changing how migration has been traditionally regulated within its member states. These systems are meant to enhance border security and administrative efficiency while making it easier to identify and track who is crossing in and out of territories⁶.

Schengen information system

The Schengen Information System is the EU’s largest information-sharing platform, which is indispensable in the management of borders and assurance of security within the Schengen Area⁷. In place since 1995 and, in its second generation, since 2013, the SIS has so far allowed member states and associated

¹ Mohamed Abomhara, Sule YildirimYayilgan, Livinus ObioraNweke, ZoltánSzékely, *A comparison of primary stakeholders'views on the deployment of biometric technologies in border management: Case study of SMart mobilLity at the European land borders*, *Technology in Society*, Vol. 64, February, 2021, <https://doi.org/10.1016/J.TECHSOC.2020.101484> (30.10.2024)

² Blaž Meden, Peter Rot, Philipp Terhörst et al., *Privacy–Enhancing Face Biometrics: A Comprehensive Survey*, “IEEE Transactions on Information Forensics and Security”, Vol. 16, 2021 <https://ieeexplore.ieee.org/ielx7/10206/9151439/09481149.pdf> (01.11.2024)

³ *Idem*

⁴ Natasha Saunders, *Op. cCit.*, pp.10-12

⁵ Didier Bigo, Julien Jeandesboz, Jorrit Rijpma, *Smart Borders Revisited: An Assessment of the Commission’s Revised Smart Borders Proposal*, “European Parliament Research Report”, November 2016, p. 52 <https://sciencespo.hal.science/hal-03459136v1/document> (30.10.2024)

⁶ Bruno Oliveira Martins, Kristoffer Lidén, Maria Gabrielsen Jumbert, *Border security and the digitalization of sovereignty: insights from EU borderwork*, “European Security”, Vol. 31, No. 3, 2022, pp. 475-494 <https://doi.org/10.1080/09662839.2022.2101884> (30.10.2024)

⁷ European Commission, *Schengen Information System*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en (30.10.2024)

countries to share, in real-time, alerts on persons and objects—a missing person, a stolen vehicle, or a fraudulent document¹.

As of 2023, the system knows new alert categories and improved information processing. This SIS contains biometric data, such as fingerprints and photographs of people, to increase the correct identification of people at border control or in police services². Specific rights linked to transparency and given to individuals have always represented one of the main modalities in which SIS develops this concept. According to SIS II legal regulations, such people also acquire rights to have access, correctness with some elements, and lawful deletion regarding the data of the owner that has been processed through this system³.

Several mechanisms put SIS at responsibility: The Schengen Evaluation and Monitoring Mechanism provides for regular assessment to be carried out by the Commission on the implementation of member states regarding the Schengen acquis⁴.

The respective EU data protection laws binding SIS on the collection, storage, and exchange of personal data, including special legislation contained within the Schengen Convention, regard the personal data as sensitive information, including biometric identifiers, available only to the competent authority authorized and then only when it is strictly necessary for a legitimate end. Each participating state will have an established and independent body known as the National Supervisory Authority responsible for overseeing this area of law to deter and discuss any misuse of the data⁵.

Visa information system (VIS)

The Visa Information System is a central database allowing the Schengen States to exchange visa information, thus supporting the implementation of the European Union's common visa policy. It connects consulates based in non-EU countries with all external border crossing points of the Schengen States, managing data and decisions related to short-stay visa applications for persons planning to visit or transit through the Schengen Area.

One of the most important features of VIS is the possibility to prevent “visa shopping” by allowing member states to detect and stop any further applications following a rejection⁶. It also supports asylum procedures by helping to identify the state responsible under the Dublin Regulation by checking the visa history records. Additionally, VIS helps law enforcement in investigating serious crimes, including terrorism, subject to strict legal conditions⁷.

EURODAC (European Asylum Dactyloscopy Database)

The European Asylum Dactyloscopy Database (EURODAC) is a centralized system established in 2003 to streamline asylum application processes within the EU and associated countries. It plays a pivotal role in supporting the implementation of the Dublin Regulation, which determines the EU Member State responsible for examining an individual's asylum application⁸.

¹ Izabella Majcher, *The Schengen-wide entry ban: how are non-citizens' personal data protected?*, “Journal of Ethnic and Migration Studies”, Vol. 48, 2020, pp. 1944 – 1960 <https://doi.org/10.1080/1369183X.2020.1796279> (01.11.2024)

² European Commission, *What is SIS and how does it work?*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en (01.11.2024)

³ Christian Janssen, Jonas Kathmann, *Legal Requirement Elicitation, Analysis and Specification for a Data Transparency System.*, Springer Nature Link, 2020, pp. 3-17, https://doi.org/10.1007/978-3-030-53337-3_1 (01.11.2024)

⁴ EU Monitor, Annexes to COM (2020)779 - Functioning of the Schengen Evaluation and Monitoring Mechanism under Article 22 of Council Regulation (EU) No. 1053, 2013, https://www.eumonitor.eu/9353000/1/j4nvirkkr58fyw_j9vvik7m1c3gyxp/vle219lgtgzy (01.11.2024)

⁵ Sebastian Kaniewski, *Genesis And Significance Of The Schengen Information System (SIS)*, “Edukacja Humanistyczna”, Vol. 2, No. 33, 2015, pp. 89-96, <https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-f24892b7-07af-49b9-b6e2-cdac93f96390> (01.11.2024)

⁶ Georgios Glouftsiotis, Stephan Scheel, *An inquiry into the digitization of border and migration management: performativity, contestation and heterogeneous engineering*, Third World Quarterly”, No. 42, 2020, pp. 123-140 <https://doi.org/10.1080/01436597.2020.1807929> (01.11.2024)

⁷ *Idem*

⁸ European Commission, *EURODAC (European Asylum Dactyloscopy Database)*, 2022, https://knowledge4policy.ec.europa.eu/dataset/ds00008_en (01.11.2024)

By collecting and comparing fingerprint data, EURODAC ensures consistency and fairness in processing applications while preventing multiple submissions in different countries¹. The revised EURODAC regulation introduces important changes in migration governance. The age threshold for taking fingerprints has been lowered from 14 to 6 years. The system has been upgraded with the inclusion of facial images and biometric details².

The EU's adoption of digital systems like SIS, VIS, and EURODAC has modernized migration management, improving border security, administrative efficiency, and tracking capabilities.

Human security risks

Privacy and data protection

One of the most serious problems linked to reinforcing borders with advanced digital technologies is what mechanism exists to balance enhanced security with respect for human rights. AI-driven surveillance, collection of biometric data, and predictive analytics can be quite powerful means of managing migration flows. Meanwhile, these are susceptible to raising serious concerns about over-surveillance, racial profiling, and erosion of privacy rights³.

A report in 2018 noted the vulnerabilities of the Schengen Information System (SIS), with insufficient encryption measures, exposing personal data breaches⁴. The use of drone AI cameras in countries like Hungary and Greece to monitor migrant movements has been criticized as a means of racial profiling and a violation of data privacy laws⁵.

The 2019 breach of Bulgaria's National Revenue Agency database, which exposed sensitive personal data of nearly 5 million citizens, is an exceptional example of how centralized systems can be hacked⁶. Mechanisms must therefore be in place to ensure that the deployment of new technologies is in line with obligations under international human rights. Underlining this, the OSCE Office for Democratic Institutions and Human Rights (ODIHR) stresses the importance of integrating human rights considerations into the development and use of border technologies by guaranteeing strong legislative frameworks, independent oversight mechanisms, and impact assessments during technology development⁷.

Moreover, independent oversight mechanisms should be in place to monitor the use of surveillance technologies at borders. Training border personnel in human rights standards can help ensure that these technologies are used responsibly and ethically. Otherwise, there is a chance that automated decision-making will result in discrimination against asylum seekers and refugees, further increasing systemic inequalities.

Discrimination

Automated profiling mechanism at borders causes discriminatory situations, disproportionately affecting migrants and refugees.

The Federal Anti-Discrimination Agency in its recent expert report, highlights that the use of algorithms in border control often relies on datasets that reflect existing social disparities, which in turn lead to biased outcomes. Profiling mechanisms in European Union border operations are more likely to target people

¹ European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Eurodac statistics, <https://data.europa.eu/data/datasets/eurodac-statistics?locale=en> (01.11.2024)

² Niovi Vavoula, *The Transformation of Eurodac from an Asylum Tool into an Immigration Database*, "EU Immigration and Asylum Law and Policy", 2024, <https://eumigrationlawblog.eu/the-transformation-of-eurodac-from-an-asylum-tool-into-an-immigration-database/> (01.11.2024)

³ Mirko Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, in "BioLaw Journal – Rivista di BioDiritto", No.2, 2021, pp. 433-451, <https://doi.org/10.15168/2284-4503-833> (01.11.2024)

⁴ Freddy S. Singaraj, *Shroud of Surveillance and Its Threat to Fundamental Rights and Civil Liberties*, "Journal of Emerging Technologies and Innovative Research", 2019, <https://www.jetir.org/papers/JETIRBH06007.pdf> (01.11.2024)

⁵ Panagiotis Loukinas, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, "Surveillance and Society", Vol. 15, No. 3/4, 2017, pp. 439-446, <https://doi.org/10.24908/SS.V15I3/4.6613> (02.11.2024)

⁶ Georgios Glouftsiotis, Stephan Scheel, *An inquiry into the digitization of border and migration management: performativity, contestation and heterogeneous engineering*, "Third World Quarterly", No. 42, 2020, pp. 123-140, <https://doi.org/10.1080/01436597.2020.1807929> (01.11.2024)

⁷ Gemma Galdon Clavell, *Protect rights at automated borders*, "Nature", No. 543, 2017, pp. 34-36, <https://doi.org/10.1038/543034a> (01.11.2024)

of African and Middle Eastern descent as security threats based on historical trends, rather than analyzing individual behavior¹.

Algorithmic profiling creates spurious classifications, like a “risky population”, based on correlations within changing datasets using variables such as income or postal codes rather than protected attributes which makes discrimination much harder to detect². Strong data governance mechanisms form the backbone for managing this sensitive information within AI systems. Organizations should perform Privacy Impact Assessments to consider and alleviate potential risks to individuals regarding the deployment of these technologies. The proactive approach will help them find loopholes in data handling practices, ensuring full transparency under the GDPR regarding how data will be used³.

Therefore, in the implementation of AI algorithms or automated digital systems in the management of data flow at borders, it is necessary to adopt a legal framework capable of eliminating the consequences of discrimination of a system that builds its image because of bias or innocuous data.

Non-refoulement breaches

Automated border systems may even designate individuals for deportation without proper consideration of asylum applications or the risks they may face in their home countries. The difficulty with this lies in reliance upon biometric and digital technologies that might not engage with the messy particularities of individual situations.

The breaches of non-refoulement are more visible in the EU with the emergence of *digital pushbacks* – a process where information systems are being misused to perpetuate asylum rights violations⁴. The case law on the CJEU on art. 47 of the EU Charter requires deep scrutiny of SIS alerts; however, constraints in national judicial systems impede proper cross-border examination. As a result, migrants often struggle with no means to challenge such alerts, compromising their right to fair asylum procedures⁵.

Technologies like iBorderCtrl developed to determine credibility, and AI-driven systems put into use in Germany for determining the origins of asylum seekers are criticized for keeping old discriminations and marginalization alive, possibly violating the non-refoulement principle. While projects like GeoMatch and AI-based mobile solutions aim to support refugees, their misuse by states or malicious actors could endanger asylum seekers⁶.

Technological failures, such as app crashes and errors in geolocation, have excluded many migrants without smartphones or access to the internet, disproportionately affecting Black migrants and Haitians due to facial recognition biases and language barriers⁷. These issues effectively denied protection to vulnerable people, in effect violating international law in potentially exposing them to refoulement.

Study Case

Greece’s use of AI-powered surveillance at borders

Greece’s use of AI-powered surveillance at its borders represents a significant shift in migration management, especially at the Evros land border with Turkey.

¹ Carsten Orwat, *Risks of Discrimination through the Use of Algorithms*, Federal Anti-Discrimination Agency, Institute for Technology Assessment and Systems Analysis (ITAS), 2019, https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/EN/publikationen/Studie_en_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.pdf?__blob=publicationFile&v=2 (04.11.2021)

² Monique Mann, Tobias Matzner, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, “Big Data&Society”, Vol. 6, No.2, 2019, <https://doi.org/10.1177/2053951719895805> (04.11.2021)

³ Yordanka Ivanova, *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI.*, “Materials Performance eJournal”, 2020, <https://doi.org/10.2139/ssrn.3584219> (04.11.2021)

⁴ Romain Lanneau, *Digital pushbacks at European borders: an ongoing threat to the rule of law in the Schengen area*, “Cahiers de l’EDEM”, Special Issue, August, 2022, pp. 63-69, <https://uclouvain.be/fr/instituts-recherche/juri/cedie/actualites/lanneauaout2022.html> (04.11.2021)

⁵ *Idem*

⁶ *Idem*

⁷ Austin Kocher, *Glitches in the Digitization of Asylum: How CBP One Turns Migrants’ Smartphones into Mobile Borders*, “Societies 2023”, Vol.13, No.6, 2023, p. 149, <https://doi.org/10.3390/soc13060149> (04.12.2024)

These policies are deeply rooted in the historical context of exclusionary nationalism in Greece, which defines migrants (predominantly from Muslim countries) as the “Other”, associating them with perceived security threats and cultural differences¹.

Following the 2015 migrant crisis, in which more than 850.000 people arrived in Greece, this nation implemented several legislative, political, and technological initiatives to lower migration with EU assistance. These included the blocking of the Western-Balkan route, the *EU-Turkey Agreement* for the return of illegal migrants, and joint NATO operations².

Greek authorities’ actions, which have been widely denounced as pushbacks, have drawn significant international criticism following the tragic deaths of 12 migrants in February 2022 due to freezing temperatures at the Turkish border, illustrating the gravity of these practices. These actions, as stated in art. 33 of the Refugee Convention, which prohibits sending individuals to locations where they could be in danger of persecution, is clearly against the principle of non-refoulement³.

Coupled with these technological systems in Greece are aggressive pushback strategies that include denial of access to asylum, mass deportations, and endangerment of migrants' lives. While the border laws of Greece claim to align with EU legal frameworks like the *Schengen Borders Code*, the integration of artificial intelligence into an already racially prejudiced and violent border regime further escalates the tension between sovereignty, security, and human rights.

Conclusions

These technologies often coincide in settings where basic rights, like non-refoulement and discrimination, are frequently being breached. Greek border control strategies demonstrate how utilizing advanced technology can exacerbate preexisting racial prejudices and inequities, particularly when combined with forceful actions like pushbacks.

Relying only on AI-driven tools without legal protections and transparency can disrupt the balance between sovereignty and human rights, putting at risk vulnerable migrant populations by marginalizing and endangering them. Strong supervision, strict legal structures, and active public monitoring will ensure that technological changes in border control are used effectively while still respecting human dignity and basic freedoms. The commitment to ensuring safe and ethical migration governance will remain an unattainable goal without the implementation of these measures.

A pragmatic conclusion is that while technology can improve border management, it must be implemented with strict oversight and in compliance with international human rights standards. This includes ensuring transparency in how data is collected and used, safeguarding against bias in automated systems, and protecting the rights of vulnerable populations. Effective migration management in an era of technological progress requires a careful balance between strengthening security measures and upholding fundamental human rights.

Bibliography

Books

1. Hemat, Lise, Endregard, *‘Just’ Research: A Case Study of EU-funded Research with Experimental Artificial Intelligence Technology for Border Control*, The Peace Research Institute Oslo (PRIO), Oslo, 2022

¹ Lena Karamanidou, Bernd Kasperek, *From Exception to Extra-Legal Normality: Pushbacks and Racist State Violence Against People Crossing the Greek–Turkish Land Border*, “State Crime Journal”, Vol. 11, No. 1, Special Issue on Migration and Racist State Violence, 2022, pp. 12-32, <https://www.jstor.org/stable/48675911>, (04.12.2024)

² Panagiotis Loukinas, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, “Surveillance and Society”, Vol. 15, No. 3/4, 2017, pp. 439-446, <https://doi.org/10.24908/SS.V15I3/4.6613> (02.11.2024)

³ Lise Endregard Hemat, *‘Just’ Research: A Case Study of EU-funded Research with Experimental Artificial Intelligence Technology for Border Control*, The Peace Research Institute Oslo (PRIO), 2022, <https://www.prio.org/publications/13182> (04.12.2024)

2. McGregor, Lorna; Molnar, Petra, *Digital Border Governance: A human rights-based approach*, Online Study University of Essex and the Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023

Studies and Articles

1. Abomhara, Mohamed; Yayilgan, Sule, Yildirim; Nweke, Livinus, Obiora; Székely, Zoltán, *A comparison of primary stakeholders' views on the deployment of biometric technologies in border management: Case study of SMart mobILity at the borders*, "Technology European Land in Society", Vol. 64, February 2021, <https://doi.org/10.1016/J.TECHSOC.2020.101484>
2. Bigo, Didier; Jeandesboz, Julien; Rijpma, Jorrit, *Smart Borders Revisited: An Assessment of the Commission's Revised Smart Borders Proposal*, "European Parliament Research Report", 2016, hal-03459136f, <https://sciencespo.hal.science/hal-03459136v1/document>
3. Clavell Gemma Galdon, *Protect rights at automated borders*, "Nature", No. 543, 2017, <https://doi.org/10.1038/543034a>
4. Forti, Mirko, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, "BioLaw Journal – Rivista di BioDiritto", No. 2, 2021, <https://doi.org/10.15168/2284-4503-833>
5. Giguashvili Giuli, *Possibilities of Using Artificial Intelligence in the Process of International Migration Management*, "Innovative Economics and Management", Vol. 10, No. 3, 2023, <https://doi.org/10.46361/2449-2604.10.3.2023.58-66>
6. Glouftsiou, Georgios, *Governing border security infrastructures: Maintaining large-scale information systems*, "Security Dialogue", Vol. 52, No. 5, 2020, <https://doi.org/10.1177/0967010620957230>
7. Glouftsiou, Georgios; Scheel Stephan, *An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering*, "Third World Quarterly", No. 42, 2020, <https://doi.org/10.1080/01436597.2020.1807929>
8. Ivanova Yordanka, *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI*, "Materials Performance eJournal", 2020, <https://doi.org/10.2139/ssrn.3584219>
9. Janssen Christian, Kathmann Jonas, *Legal Requirement Elicitation, Analysis and Specification for a Data Transparency System*, Springer Nature Link, 2020, https://doi.org/10.1007/978-3-030-53337-3_1
10. Kaniewski, Sebastian, *Genesis and Significance of the Schengen Information System (SIS)*, "Edukacja Humanistyczna", Vol. 2, No. 33, 2015
11. Karamanidou, Lena; Kasperek, Bernd, *From Exception to Extra-Legal Normality: Pushbacks and Racist State Violence Against People Crossing the Greek–Turkish Land Border*, "State Crime Journal", Vol. 11, No. 1, Special Issue on Migration and Racist State Violence, 2022, <https://www.jstor.org/stable/48675911>
12. Kocher, Austin, *Glitches in the Digitization of Asylum: How CBP One Turns Migrants' Smartphones into Mobile Borders*, "Societies 2023", Vol. 13, No. 6, 2023, <https://doi.org/10.3390/soc13060149>
13. Lanneau, Romain, *Digital pushbacks at European borders: an ongoing threat to the rule of law in the Schengen area*, "Cahiers de l'EDM", Special Issue, August 2022, <https://uclouvain.be/fr/instituts-recherche/juri/cedie/actualites/lanneauaout2022.html>
14. Loukinas, Panagiotis, *Surveillance and Drones at Greek Borderzones: Challenging Human Rights and Democracy*, "Surveillance And Society", Vol. 15, No. 3/4, 2017, <https://doi.org/10.24908/SS.V15I3/4.6613>
15. Majcher, Izabella, *The Schengen-wide entry ban: how are non-citizens' personal data protected?*, "Journal of Ethnic and Migration Studies", Vol. 48, 2020, <https://doi.org/10.1080/1369183X.2020.1796279>
16. Malini Hema G.B., *Automation of Big Data Analytics Using Robotic Process Automation*, "International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT)", Vol. 7, No. 2, 2021, <https://doi.org/10.32628/CSEIT2172124>
17. Mann, Monique; Matzner, Tobias, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, "Big Data & Society", Vol. 6, No. 2, 2019, <https://doi.org/10.1177/2053951719895805>
18. Martins, Bruno, Oliveira; Jumbert, Maria, Gabrielsen, *EU Border technologies and the co-production of security 'problems' and 'solutions'*, "Journal of Ethnic and Migration Studies", Vol. 48, 2020, <https://doi.org/10.1080/1369183X.2020.1851470>

19. Martins, Bruno, Oliveira; Lidén, Kristoffer; Jumbert, Maria, Gabrielsen, *Border security and the digitalization of sovereignty: insights from EU borderwork*, “European Security”, Vol. 31, No. 3, 2022, <https://doi.org/10.1080/09662839.2022.2101884>
20. Meden, Blaž; Rot, Peter; Terhörst, Philipp et al., *Privacy–Enhancing Face Biometrics: A Comprehensive Survey*, “IEEE Transactions on Information Forensics and Security”, Vol. 16, 2021, <https://ieeexplore.ieee.org/ielx7/10206/9151439/09481149.pdf>
21. Orwat, Carsten, *Risks of Discrimination through the use of Algorithms*, *Federal Anti-Discrimination Agency*, Institute for Technology Assessment and Systems Analysis (ITAS), 2019, https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/EN/publikationen/Studie_en_Diskriminierungsrisiken_durch_Verwendung_von_Algorithmen.pdf?__blob=publicationFile&v=2
22. Panchamia, Sanket, Byrappa; Deepak Kumar, *Passport, VISA and Immigration Management Using Blockchain*, “2017 23rd Annual International Conference in Advanced Computing and Communications (ADCOM)”, 2017, <https://doi.org/10.1109/ADCOM.2017.00009>
23. Saunders, Natasha, *Security, digital border technologies, and immigration admissions: Challenges of and to non-discrimination, liberty and equality*, “European Journal of Political Theory”, 2023, <https://doi.org/10.1177/14748851231203912>
24. Singaraj, S., Freddy, *Shroud of Surveillance and Its Threat to Fundamental Rights and Civil Liberties*, “Journal of Emerging Technologies and Innovative Research”, 2019, <https://www.jetir.org/papers/JETIRBH06007.pdf>
25. Vavoula, Niovi, *The Transformation of Eurodac from an Asylum Tool into an Immigration Database*, “EU Immigration and Asylum Law and Policy”, 2024, <https://eumigrationlawblog.eu/the-transformation-of-eurodac-from-an-asylum-tool-into-an-immigration-database/>
26. Wang, Yingxu; Tan, Xinming; Ngolah, Cypryan; Sheu, Philip; *The Formal Design Models of a Set of Abstract Data Types (ADTs)*, “International Journal of Software Science and Computational Intelligence (IJSSCI)”, Vol. 2, No. 4, 2010, <https://doi.org/10.4018/jssci.2010100106>

Documents

1. EU Monitor, *Annexes to COM(2020)779 - Functioning of the Schengen Evaluation and Monitoring Mechanism under Article 22 of Council Regulation (EU) No. 1053*, 2013, https://www.eumonitor.eu/9353000/1/j4nvirkkkkr58fyw_j9vvik7m1c3gyxp/vle2l9l1tgzy
2. European Commission, *EURODAC (European Asylum Dactyloscopy Database)*, 2022, https://knowledge4policy.ec.europa.eu/dataset/ds00008_en
3. European Commission, *Schengen Information System*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en
4. European Commission, *Visa Information System (VIS)*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en
5. European Commission, *What is SIS and how does it work?*, https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en
6. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, *Eurodac statistics*, <https://data.europa.eu/data/datasets/eurodac-statistics?locale=en>
7. European Union, *Eurodac statistics*, <https://data.europa.eu/data/datasets/eurodac-statistics?locale=en>
8. United States Government Accountability Office, *Biometric Identification Technologies Considerations to Address Information Gaps and Other Stakeholder Concerns*, Report to Congressional Committees, 2024, <https://www.gao.gov/assets/gao-24-106293.pdf>

Websites

1. <https://data.europa.eu/>
2. <https://eumigrationlawblog.eu/>
3. <https://home-affairs.ec.europa.eu/>
4. <https://ieeexplore.ieee.org/>
5. <https://knowledge4policy.ec.europa.eu/>

6. <https://sciencespo.hal.science/>
7. <https://uclouvain.be/fr/>
8. <https://www.antidiskriminierungsstelle.de/>
9. <https://www.eumonitor.eu/>
10. <https://www.gao.gov/>
11. <https://www.jstor.org/>