Diana Lubandy, MA
Akademia Humanitas
e-mail: info@diananowek.com
ORCID: 0000-0002-9759-2238

DOI: 10.26410/SF_1/26/7

BETWEEN SECURITY AND HUMAN RIGHTS. THE CASES OF AVATAR AND iBorderCtrl

Abstract

The dynamic development of artificial intelligence technologies is significantly transforming the protection of the European Union's external borders. Increasing importance is being attributed to systems that employ data analytics, biometric technologies, algorithmic profiling, and elements of behavioural analysis to support the assessment of traveller risk. The aim of this article is to examine the opportunities and limitations associated with the use of artificial intelligence systems in border security management through the case studies of the AVATAR and iBorderCtrl projects. The paper presents the origins of both programmes, their technological foundations, and their potential operational applications in border control procedures. Particular attention is devoted to the compatibility of these solutions with fundamental rights, personal data protection requirements, and the principle of non-discrimination. The literature review indicates that AI-based technologies may enhance the efficiency of border control processes. However, they simultaneously generate risks related to algorithmic errors, limited transparency of decision-making procedures, and potential violations of human rights. Consequently, the implementation of such systems requires a substantial degree of human oversight, independent scientific validation, and effective mechanisms for review and appeal.

Keywords

artificial intelligence, border security, iBorderCtrl, AVATAR, human rights, border management, behavioural analysis

Introduction

The protection of state borders constitutes one of the fundamental functions of modern states and represents a key pillar of the European Union's security architecture[1]. In recent years, increasing international mobility, terrorist threats, irregular migration, and transnational crime[2] have intensified the search for innovative technological solutions capable of supporting border management authorities and enhancing situational awareness at border crossing points[3].

One of the most rapidly developing trends in this field is the application of artificial intelligence (AI) technologies to the automated analysis of traveller data, risk profiling, and decision-support processes[4] [5]. Within the framework of the European Union's Smart Borders initiative, several large-scale information systems have been developed, including the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS)[6]. Alongside these operational systems, a number of research and innovation projects have explored the use of biometric technologies, machine learning algorithms, and behavioural analysis for border security purposes[7]. Among the most prominent examples are the AVATAR (Automated Virtual Agent for Truth Assessments in Real-Time) and iBorderCtrl projects, which sought to evaluate the feasibility of automated traveller risk assessment based on biometric and behavioural indicators[8] [9].

The deployment of such technologies has generated significant debate among researchers, policymakers, and human rights advocates[10]. While AI-supported systems may enhance the efficiency of border controls, improve resource allocation, and facilitate the identification of potential security threats, concerns have been raised regarding the protection of personal data, transparency and explainability of algorithmic decision-making, accountability for automated assessments[11], and compliance with the

1 Frontex, *Technical and Operational Strategy for European Integrated Border Management Strategy*, European Commission, Warsaw 2019.

2 E. Guild, *Security and Migration in the 21st Century*, Polity Press, Cambridge 2009.

3 D. Broeders, H.Dijstelbloem, *The datafication of mobility and migration management*, [w:] H. Dijstelbloem, A. Meijer (red.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016, pp. 242–260.

4 P. Lehtonen, P.Aalto, *Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States*, „European Security" 2017, nr 26(2), pp. 207–225,

5 M. Minkin, *Human rights and AI-based border technologies*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, nr 33(1), pp. 34–40.

6 eu-LISA, *Single Programming Document 2025-2027*, European Union Agency for the Operational Management of Large-Scale IT Systems, Tallinn 2025.

7 L. Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, Duke University Press, Durham 2020.

8 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Project Factsheet.

9 A. Gajda, *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, p. 120.

10 European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, Publications Office of the European Union, Luxembourg 2020.

11 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, nr 25(3), pp. 413–430.

Charter of Fundamental Rights of the European Union[12]. Particular controversy surrounds the use of behavioural analytics and automated deception detection technologies, whose scientific validity remains contested within the academic community[13]

The objective of this article is to analyse the potential and limitations of artificial intelligence systems used for risk assessment at the external borders of the European Union and to evaluate their implications for both security and human rights. Using the AVATAR and iBorderCtrl projects as case studies, the paper examines the technological assumptions underlying these systems, their operational applications, and the legal, ethical, and security challenges associated with their implementation. The AVATAR and iBorderCtrl projects are particularly relevant because they represent some of the first attempts to integrate artificial intelligence, biometric identification, and automated behavioural assessment into border security procedures[14].

Research methodology

This article employs a qualitative case study approach to examine the use of artificial intelligence systems in risk assessment at the external borders of the European Union. The AVATAR and iBorderCtrl projects were selected as case studies because they represent some of the earliest and most widely discussed attempts to integrate artificial intelligence, biometric technologies, and behavioural analysis into border control procedures. The main research question guiding this article is:

- What opportunities and limitations arise from the use of artificial intelligence systems for traveller risk assessment at the external borders of the European Union,
- and how do these technologies affect the relationship between security objectives and the protection of fundamental rights?

The research is based on a review of scientific literature, European Union policy documents, project reports, and legal sources concerning border security, artificial intelligence, data protection, and fundamental rights. Comparative case study analysis was used to identify similarities and differences in the objectives, technological assumptions, operational applications, and ethical implications of both projects.

The analytical framework adopted in this study focuses on two dimensions:

1. security effectiveness, including the potential contribution of AI technologies to risk assessment and border management,
2. compliance with human rights standards, particularly regarding privacy, transparency, non-discrimination, and accountability.

By examining these dimensions simultaneously, the article seeks to assess whether AI-supported border technologies can enhance security while remaining

12 M. O'Neill, *The Politics of Deceptive Borders*, Routledge, London–New York 2021.

13 A. Vrij, *Detecting Lies and Deceit: Pitfalls and Opportunities*, wyd. 2, John Wiley & Sons, Chichester 2008.

14 J.F. Nunamaker, D.C. Derrick, A.C. Elkins, J.K. Burgoon, M.W. Patton, *Embodied conversational agent-based kiosk for automated interviewing*, „Journal of Management Information Systems" 2012, nr 28(1), pp. 17–48.

consistent with the legal and ethical standards underpinning the European Union's system of fundamental rights protection. The study does not seek to evaluate the technical performance of individual algorithms

Smart Borders and the Development of AI-Based Border Management Systems

The Smart Borders concept refers to the use of advanced information technologies to enhance border control procedures and improve the management of movements across the external borders of the European Union[15]. a key component of this approach is the deployment of large-scale information systems, including the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), the Schengen Information System (SIS II), the Visa Information System (VIS), and Eurodac[16].

The ETIAS system employs algorithmic profiling and automated risk assessment models for visa-exempt third-country nationals travelling to the Schengen Area. Traveller data are analysed using predefined risk indicators and information obtained from interoperable European databases, enabling the identification of individuals who may pose security, migration, or public health risks[17] [18] [19].

In parallel, the Entry/Exit System (EES) is being implemented to record entries and exits of third-country nationals through the use of biometric data, including facial images and fingerprints. Recent studies identify EES as one of the most advanced examples of biometric surveillance and automated identity verification within the European border management framework[20].

Growing attention has also been devoted to technologies that combine artificial intelligence with behavioural assessment and biometric monitoring. These solutions seek to identify behavioural indicators potentially associated with deception, risk, or anomalous conduct during border control procedures. At the same time, scholars have highlighted concerns regarding algorithmic bias[21], automated decision-making,

15 K. Latos, *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej*, „Rocznik Integracji Europejskiej" 2023, nr 17, pp. 181–198.

16 G. Balawajder, *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, t. 6, nr 3, pp. 215–230.

17 Á. Mohay, *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations*, „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1, pp. 1–20.

18 A. Thommandru, V. Mone, F. Shokhijakhon, G. Mirzayev, *Algorithmic Profiling and Facial Recognition in EU Border Control: Examining ETIAS Decision-Making*, Privacy and Law, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

19 C.I. Velasco Rico, M. Laukyte, *ETIAS System and New Proposals to Advance the Use of AI in Public Services*, „Computer Law & Security Review" 2024, t. 54, art. 106017.

20 A. Catano, *The Entry/Exit System of the EU: TCNs Between the Processing of Personal Data and AI Applications at the Borders*, SSRN Electronic Journal, 2026.

21 J. Sánchez-Monedero, L. Dencik, *The Politics of Deceptive Borders: 'Biomarkers of Deceit' and the Case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3, pp. 413–430.

privacy protection[22], and compliance with fundamental rights standards within the European Union[23].

The AVATAR Project as a Precursor of AI-Assisted Border Risk Assessment

The AVATAR (Automated Virtual Agent for Truth Assessments in Real-Time) project was developed in the United States by researchers from the University of Arizona between approximately 2007 and 2012, with the first operational prototypes emerging around 2009[24]. It was an experimental system designed to support security screening and traveller risk assessment through automated interviewing and behavioural analysis[25]. The project's primary objective was to create a virtual border officer capable of conducting short interviews with travellers and identifying behavioural indicators potentially associated with deception or elevated security risk.

Although AVATAR was not formally developed within the European Union, it remains highly relevant to the European border security context. Between 2009 and 2013, the technology was evaluated in cooperation with Frontex through a series of workshops, demonstrations, and field experiments conducted in several European countries, including Poland, the Netherlands, and Romania[26]. These activities were intended to assess the feasibility of automated interviewing and behavioural risk assessment technologies for future application within European border management systems. Consequently, AVATAR can be regarded as an important technological precursor to later EU-funded initiatives, particularly iBorderCtrl[27].

The AVATAR system combined an embodied conversational agent with a range of biometric and behavioural sensors. During the interview process, travellers interacted with a computer-generated avatar that asked standardized questions while simultaneously collecting behavioural data. The system analysed facial expressions, eye movements, gaze patterns, body posture, vocal characteristics, response latency, and other observable indicators using machine-learning algorithms designed to identify anomalies and behavioural patterns potentially associated with deceptive responses[28].

22 MForti, Addressing Algorithmic Errors in Data-Driven Border Control Procedures, „German Law Journal" 2024, t. 25, nr 5, pp. 1047–1068.

23 Y. Yang, F.Z. Borgesius, P. Beckers, E. Brouwer, *Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks for Human Rights*, SSRN Electronic Journal, 2024.

24 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control*, European Parliamentary Research Service (EPRS), Publications Office of the European Union, Brussels 2014.

25 D.C. Derrick, T.O. Meservy, J.L. Jenkins, J.K. Burgoon, J.F. Nunamaker, *Detecting deceptive responses via automated interviewing*, „Journal of Management Information Systems" 2011, t. 28, nr 1, pp. 41–68.

26 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Publications Office of the European Union, Brussels 2019.

27 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Research and Innovation Programme, Grant Agreement No. 700626, Brussels 2019.

28 J.F. Nunamaker, D.C. Derrick, A.C. Elkins, J.K. Burgoon, M.W. Patton, *Embodied conversational agent-based kiosk for automated interviewing*, „Journal of Management Information Systems" 2012, t. 28, nr 1, pp. 17–48.

Importantly, AVATAR was not intended to replace border officers. Instead, it was conceived as a decision-support tool generating a risk score and recommending whether a traveller should undergo additional screening. The final decision remained with a human officer, reflecting an early implementation of the human-in-the-loop principle that remains central to contemporary discussions regarding trustworthy AI systems[29].

Initial experimental studies suggested that the system could improve the efficiency of traveller screening and assist in allocating border control resources more effectively. However, the project's developers acknowledged that most validation studies were conducted under controlled laboratory conditions and that further research was necessary before operational deployment could be considered[30]. These limitations mirror broader concerns within deception research regarding the reliability of behavioural indicators as predictors of deception, risk, or malicious intent[31]. For these reasons, AVATAR is best understood as a proof-of-concept demonstrating the potential integration of artificial intelligence, behavioural analysis, and automated interviewing in border security rather than as a scientifically validated operational solution.

The iBorderCtrl Project and the Evolution of Behaviour-Based Risk Assessment in the European Union

The Horizon 2020-funded iBorderCtrl (Intelligent Portable Border Control System)[32] project represented one of the most ambitious attempts to operationalise artificial intelligence-assisted traveller risk assessment within the European Union. The project aimed to develop an integrated platform supporting border guards during the assessment of travellers crossing the EU's external land borders. Pilot testing was conducted in Hungary, Greece, and Latvia between 2018 and 2019[33].

The system architecture consisted of several interconnected modules, including biometric identification, automated document authentication, access to external information databases, a Risk-Based Assessment Tool (RBAT), and the Automatic Deception Detection System (ADDS). Together, these components were designed to facilitate traveller screening and identify individuals requiring enhanced inspection[34]. The most controversial element of the project was the ADDS module, which

29 European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights*, Publications Office of the European Union, Luxembourg 2020.

30 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Publications Office of the European Union, Brussels 2019.

31 V. Denault, N.E. Dunbar, *Credibility assessment and deception detection in courtrooms: Hazards and challenges for scholars and legal practitioners*, [w:] T.Docan-Morgan (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019, pp. 769–790.

32 European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Project Factsheet.

33 A. Gajda, *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, t. 15, nr 4, p. 150–170.

34 D. Minkin, L.T. Brandner, *Borderline decisions?: Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40

attempted to move "from biometrics to biomarkers of deceit"[35]. Prior to arrival at the border, travellers participated in a short automated interview conducted by a virtual avatar. During this interaction, machine-learning algorithms analysed facial movements, micro-expressions, gaze behaviour, and other behavioural characteristics in order to identify patterns potentially associated with deception or elevated risk[36].

The conceptual foundations of iBorderCtrl were closely related to those previously explored within the AVATAR project. Both systems relied on automated interviews, behavioural analysis, facial expression recognition, and AI-assisted risk assessment. However, iBorderCtrl expanded the AVATAR concept by integrating multiple technological components into a broader border management platform. While AVATAR primarily focused on automated interviewing and behavioural assessment, iBorderCtrl combined behavioural analytics with biometric identification, document verification, database interoperability, and algorithmic risk scoring, thereby reflecting the broader objectives of the EU Smart Borders initiative[37].

Despite these technological advances, the scientific assumptions underpinning the system remain highly contested. The project drew heavily upon theories linking deception to behavioural leakage, emotional micro-expressions, cognitive load, behavioural control, and so-called "duping delight." Such assumptions originate largely from the work of Paul Ekman and subsequent research on facial expressions and deception[38]. However, contemporary research increasingly questions whether deception can be reliably inferred from facial expressions alone. Numerous studies have concluded that no single behavioural indicator consistently distinguishes truthful from deceptive individuals across different contexts and populations[39].

Questions have also been raised regarding the operational effectiveness of automated deception detection systems. Available project documentation reported an accuracy rate of approximately 76% during testing phases[40], indicating that nearly one-quarter of classifications could potentially be incorrect. In large-scale border control environments involving thousands of travellers daily, such error rates may result in substantial numbers of false positives and false negatives, potentially affecting both security outcomes and individual rights. Beyond technical limitations, iBorderCtrl has become a focal point in debates concerning artificial intelligence, border security, and fundamental rights.

---

35 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, nr 25(3), p. 413–430.

36 D. Minkin, L.T. Brandner, *Borderline decisions?: Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40

37 European Commission, *Smart Borders Package: Communication from the Commission to the European Parliament and the Council* (COM(2013) 95 final), European Commission, Brussels 2013.

38 P. Ekman, *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, wyd. 4, W.W. Norton & Company, New York–London 2009.

39 W.D. Woody, *The history, present, and future of police deception during interrogation*, [w:] T.Docan-Morgan. (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019, pp. 391–411.

40 J. Sánchez-Monedero, L. Dencik, *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3, p. 413–430.

Ethical, Legal, and Human Rights Challenges

Alongside their potential security benefits, AI-supported border management systems raise significant legal, ethical, and human rights concerns. One of the most frequently discussed challenges concerns the transparency and explainability of algorithmic decision-making[41]. Many machine-learning systems operate as highly complex statistical models whose outputs may be difficult to interpret or explain. Consequently, individuals classified as high-risk travellers may find it difficult to understand the reasons underlying a particular assessment or to effectively challenge potentially erroneous decisions[42].

A second concern relates to algorithmic bias and indirect discrimination. If training datasets contain existing social, cultural, or institutional biases, AI systems may reproduce or amplify these patterns during risk assessment processes. This issue is particularly relevant in relation to third-country nationals, asylum seekers, refugees, and minority groups, who may be disproportionately affected by inaccurate classifications or discriminatory profiling practices[43].

The protection of personal data constitutes another major challenge[44]. Contemporary border management systems process vast amounts of biometric, biographical, behavioural, and travel-related information. Ensuring compliance with the principles of data minimisation, proportionality, purpose limitation, and accountability therefore remains essential for maintaining compatibility with European data protection standards and fundamental rights guarantees[45].

Particularly controversial is the use of automated emotion recognition and deception detection technologies. Critics of iBorderCtrl argue that systems relying on micro-expression analysis and behavioural indicators lack sufficient scientific validation to justify their deployment in high-stakes environments such as border control[46]. The risk of false classifications may result in unnecessary secondary inspections, delays, restrictions on freedom of movement, or potentially unjustified refusals of entry.

Consequently, the central challenge facing policymakers is not whether artificial intelligence should be used in border management, but rather under what conditions

41 Y. Yang, F.Z. Borgesius, P. Beckers, E. Brouwer, *Automated decision-making and artificial intelligence at European borders and their risks for human rights*, „SSRN Electronic Journal" 2024.

42 M. Forti, *Addressing algorithmic errors in data-driven border control procedures*, „German Law Journal" 2024, t. 25, nr 5, pp. 1047–1068.

43 A. Thommandru, V. Mone, F. Shokhijakhon, G. Mirzayev, *Algorithmic profiling and facial recognition in EU border control: Examining ETIAS decision-making, privacy and law*, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

44 G.Z. Kolasa, *Sztuczna inteligencja (AI) vs. ochrona danych osobowych (RODO) – jak zapewnić zgodność rozwiązań AI z podstawowymi mechanizmami systemu ochrony danych osobowych w ramach Unii Europejskiej?* Acta Iuridica Resoviensia 2024, 1(6), pp. 71–88. Wydawnictwo Uniwersytetu Rzeszowskiego.

45 M. Pop, *Artificial Intelligence and Fundamental Rights in the European Union: Challenges and Perspectives*, „Journal of Law and Administrative Sciences" 2025, nr 24, pp. 65–79.

46 D. Minkin, L.T. Brandner, *Borderline decisions? Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1, p. 34–40.

such technologies can be deployed in a manner that remains compatible with democratic values, fundamental rights, and the rule of law.

Conclusions

Despite ongoing controversies, the development of artificial intelligence systems forms an integral part of the European Union's broader Smart Borders strategy and the concept of European Integrated Border Management (EIBM). These initiatives seek to improve the protection of external borders through the use of interoperable databases, biometric technologies, predictive analytics, and risk assessment tools capable of supporting border authorities in increasingly complex operational environments[47]. From a security studies perspective, several potential benefits may arise from the deployment of AI-supported border technologies.

First, artificial intelligence systems can enhance traveller pre-screening by processing and analysing large volumes of data that would be difficult or impossible for human operators to evaluate manually. Automated risk assessment tools may enable border guards to allocate resources more efficiently and focus attention on travellers presenting elevated security risks[48]. Second, biometric technologies strengthen identity verification and support the detection of fraudulent documents, identity theft, and attempts to circumvent border procedures. The integration of systems such as SIS, VIS, Eurodac, ETIAS, and EES allows authorities to conduct a more comprehensive assessment of traveller information than was possible under traditional document-based border control models[49]. Third, machine-learning systems may contribute to the analysis of migration patterns, the identification of emerging smuggling routes, and the forecasting of changes in border-crossing volumes. Such capabilities can support strategic planning, operational preparedness, and risk management within border security agencies[50].

The AVATAR project additionally demonstrated the potential use of automated interviewing kiosks operated by virtual agents. Pilot studies conducted in cooperation with Frontex indicated that the system was capable of conducting interviews lasting approximately 30–90 seconds while simultaneously generating a risk assessment score for border officials[51]. Such solutions may contribute to reducing waiting times and increasing throughput at busy border crossing points.

More broadly, AI-supported systems offer the possibility of transitioning from reactive border control toward intelligence-led and risk-based border management.

47 Z. Vasilkov, V. Ristić, *Artificial Intelligence and EU Integrated Border Management*, „Pravo – Teorija i Praksa" 2025, t. 42, nr 1, pp. 89–105.

48 A. Mohay, *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations*, „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1, pp. 1–20

49 K. Latos, *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej*, „Rocznik Integracji Europejskiej" 2023, nr 17, pp. 181–198.

50 D. Broeders, H. Dijstelbloem, *The datafication of mobility and migration management*, [In:] H. Dijstelbloem, A. Meijer (Ed.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016, p. 242–260.

51 A.C. Elkins, D.C. Derrick, J.K. Burgoon, J.F. Nunamaker, *Appraising the AVATAR for Automated Border Control, European Parliamentary Research Service (EPRS)*, Brussels 2019.

By integrating multiple sources of information and identifying potentially relevant patterns in real time, these technologies may strengthen situational awareness and support more effective decision-making by border authorities. However, the extent to which these benefits can be realised depends largely on the scientific validity, reliability, transparency, and operational performance of the underlying technologies.

Recommendations

Several limitations should be considered when interpreting the findings of this article. First, the analysis is based primarily on scientific literature, policy documents, project reports, and publicly available information concerning the AVATAR and iBorderCtrl projects. Limited access to complete technical documentation and proprietary algorithms prevents an independent assessment of the systems' actual performance. Second, both AVATAR and iBorderCtrl remained largely research and development initiatives and were not deployed as large-scale operational border management systems. Consequently, most available evidence derives from pilot studies, laboratory experiments, and limited field trials rather than long-term operational use. Third, artificial intelligence technologies and their regulatory frameworks continue to evolve rapidly. Ongoing implementation of the AI Act, ETIAS, EES, and other border technologies may substantially alter the technological and legal landscape examined in this article. Finally, automated deception detection remains a highly interdisciplinary and scientifically contested field situated at the intersection of security studies, psychology, computer science, law, and communication research. The absence of a clear scientific consensus regarding the reliability of behavioural indicators requires caution when interpreting both claims of effectiveness and criticisms of such systems. Future research should focus on independent validation studies, longitudinal assessments of operational deployments, and the development of evidence-based frameworks for integrating behavioural analysis, biometric technologies, and artificial intelligence within the context of European Integrated Border Management.

Bibliography

Amoore L., *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, Duke University Press, Durham 2020.

Balawajder G., *Instytucjonalny wymiar ochrony granic zewnętrznych Unii Europejskiej w kontekście bezpieczeństwa państw członkowskich*, „Pogranicze. Polish Borderlands Studies" 2018, t. 6, nr 3.

Broeders D., Dijstelbloem H., *The datafication of mobility and migration management,* [w:] Dijstelbloem H., Meijer A. (red.), Migration and the New Technological Borders of Europe, Palgrave Macmillan, London 2016.

Catano A., *The Entry/Exit System of the EU: TCNs Between the Processing of Personal Data and AI Applications at the Borders*, „SSRN Electronic Journal" 2026.

Denault V., Dunbar N.E., *Credibility assessment and deception detection in courtrooms: Hazards and challenges for scholars and legal practitioners*, [w:] Docan-Morgan T. (red.), The Palgrave Handbook of Deceptive Communication, Palgrave Macmillan, Cham 2019.

Derrick D.C., Meservy T.O., Jenkins J.L., Burgoon J.K., Nunamaker J.F., *Detecting deceptive responses via automated interviewing*, „Journal of Management Information Systems" 2011, t. 28, nr 1.

Ekman P., *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage,* wyd. 4, W.W. Norton & Company, New York–London 2009.

Elkins A.C., Derrick D.C., Burgoon J.K., Nunamaker J.F., *Appraising the AVATAR for Automated Border Control*, European Parliamentary Research Service (EPRS), Publications Office of the European Union, Brussels 2019.

eu-LISA, *Single Programming Document 2025-2027,* European Union Agency for the Operational Management of Large-Scale IT Systems, Tallinn 2025, https://www.eulisa.europa.eu/sites/default/files/documents/eu-lisa-spd-2025-2027.pdf.

European Commission, *Smart Borders Package: Communication from the Commission to the European Parliament and the Council* (COM(2013) 95 final), European Commission, Brussels 2013, https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493026/IPOL-LIBE_ET(2013)493026_EN.pdf.

European Commission, *iBorderCtrl – Intelligent Portable Border Control System*, Horizon 2020 Research and Innovation Programme, Grant Agreement No. 700626, Brussels 2019, https://cordis.europa.eu/project/id/700626.

European Union Agency for Fundamental Rights (FRA), *Getting the Future Right: Artificial Intelligence and Fundamental Rights,* Publications Office of the European Union, Luxembourg 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf.

Forti M., *Addressing algorithmic errors in data-driven border control procedures*, „German Law Journal" 2024, t. 25, nr 5.

Frontex, Technical and Operational Strategy for European Integrated Border Management Strategy, European Commission, Warsaw 2019, https://www.frontex.europa.eu/publications/technical-and-operational-strategy-for-european-integrated-border-management-2023-2027-lep99d.

Gajda A., *Wykorzystywanie systemów sztucznej inteligencji (SI) na zewnętrznych granicach Unii Europejskiej. Możliwości, zagrożenia i wyzwania*, „Krytyka Prawa" 2023, t. 15, nr 4.

Guild E., *Security and Migration in the 21st Century*, Polity Press, Cambridge 2009.

Kolasa G.Z., *Sztuczna inteligencja (AI) vs. ochrona danych osobowych (RODO) – jak zapewnić zgodność rozwiązań AI z podstawowymi mechanizmami systemu ochrony danych osobowych w ramach Unii Europejskiej?*, „Acta Iuridica Resoviensia" 2024, t. 1, nr 6.

Latos K., *Wzmacnianie bezpieczeństwa strefy Schengen: problematyka wielkoskalowych systemów informacyjnych w polityce bezpieczeństwa Unii Europejskiej,* „Rocznik Integracji Europejskiej" 2023, nr 17.

Lehtonen P., Aalto P., *Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States*, „European Security" 2017, t. 26, nr 2.

Minkin D., Brandner L.T., *Borderline decisions? Lack of justification for automatic deception detection at EU borders*, „TATuP – Journal for Technology Assessment in Theory and Practice" 2024, t. 33, nr 1.

Mohay Á., *Algorithmic Immigration Control? The ETIAS Between Technological Benefits and Fundamental Rights Considerations,* „Hungarian Journal of Legal Studies" 2025, t. 66, nr 1.

Nunamaker J.F., Derrick D.C., Elkins A.C., Burgoon J.K., Patton M.W., *Embodied conversational agent-based kiosk for automated interviewing,* „Journal of Management Information Systems" 2012, t. 28, nr 1.

O'Neill M., *The Politics of Deceptive Borders, Routledge*, London–New York 2021.

Pop M., *Artificial Intelligence and Fundamental Rights in the European Union: Challenges and Perspectives*, „Journal of Law and Administrative Sciences" 2025, nr 24.

Sánchez-Monedero J., Dencik L., *The politics of deceptive borders: 'Biomarkers of deceit' and the case of iBorderCtrl*, „Information, Communication & Society" 2022, t. 25, nr 3.

Thommandru A., Mone V., Shokhijakhon F., Mirzayev G., *Algorithmic Profiling and Facial Recognition in EU Border Control: Examining ETIAS Decision-Making, Privacy and Law*, „WIREs Data Mining and Knowledge Discovery" 2025, t. 15, nr 2, art. e1548.

Vasilkov Z., Ristić V., *Artificial Intelligence and EU Integrated Border Management*, „Pravo – Teorija i Praksa" 2025, t. 42, nr 1.

Velasco Rico C.I., Laukyte M., *ETIAS System and New Proposals to Advance the Use of AI in Public Services*, „Computer Law & Security Review" 2024, t. 54, art. 106017.

Vrij A., *Detecting Lies and Deceit: Pitfalls and Opportunities*, wyd. 2, John Wiley & Sons, Chichester 2008.

Woody W.D., *The history, present, and future of police deception during interrogation*, [w:] Docan-Morgan T. (red.), *The Palgrave Handbook of Deceptive Communication*, Palgrave Macmillan, Cham 2019.

Yang Y., Borgesius F.Z., Beckers P., Brouwer E., *Automated decision-making and artificial intelligence at European borders and their risks for human rights*, „SSRN Electronic Journal" 2024.

About the author:

Diana Lubandy – MA in International Relations from the University of Warsaw. She has served as a strategic advisor and consultant to international organisations and agencies, including the United Nations Office of Counter-Terrorism (UNOCT), the United Nations Office on Drugs and Crime (UNODC), the International Organization for Migration (IOM), and Frontex.