European Law Open (2026), **5**, 305–334
doi:10.1017/elo.2025.10064

CAMBRIDGE UNIVERSITY PRESS

CORE ANALYSIS

Cracking AI secrecy: (beyond) EU migration law and governance

Deirdre Curtin[1] and Tommaso Fia[2]

[1]Department of Law, European University Institute, Florence, Italy and [2]Faculty of Laws, University College London, London, UK
Corresponding author: Tommaso Fia; Email: t.fia@ucl.ac.uk

(Received 20 May 2025; revised 14 November 2025; accepted 24 November 2025; first published online 23 March 2026)

Abstract
In core government and for public tasks hugely sensitive for citizens such as migration governance in Europe, the use of AI systems developed and provided under contract gives migration authorities and private providers the power to keep their deployment secret and to refuse access to their key components. This article explores the complex interplay between public and private drivers of secrecy surrounding procured AI technologies in European migration governance, demonstrating how these forces converge and reinforce one another. It examines AI secrecy as an institutional framework shaped by both public and private law forms of secrecy, applying the spectrum of secrecy from deep (unknown unknowns) to shallow secrecy (known unknowns). Specifically, the paper looks into the sources of 'political secrecy' in migration and security authorities, highlighting how migration agencies and authorities keep the existence and use of AI systems from civil society and affected persons (such as third country nationals). Next, it analyses the legal frameworks that sustain AI vendors' private secrecy, such as trade secrecy, secrecy in procurement procedures and agreements. In examining the various secrecy points, it scrutinises the limited impact of the AI Act in addressing the entrenched secrecy of AI deployment and development in governing migration. Finally, we condense the main takeaways and examine the broader repercussions of AI secrecy beyond the context of border control, touching upon its implications for a new equilibrium transcending the conventional public/private divide.

Keywords: AI; secrecy; migration governance; border control; EU law

1. Introduction

We live in a world that depends on artificial intelligence ('AI'). The quest to unravel 'what is going on' in an AI system and the consequences of its usage are frequently referred to as 'transparency'. Transparency is in reality often more an aspiration than a fact, also for human decision making.[1] AI systems are rather known for their intrinsic opacity.[2] Barriers to understanding how AI systems work run the gamut from technical obstacles – for example, not being able to access their bits and components (eg, the source code, training data,

[1]See J Zerilli et al, 'Transparency in Algorithmic and Human Decision-Making: Is There a Double Standard?' 32 (2019) Philosophy & Technology 661. On problems with transparency in human decision-making in the public sector, see among others M Fenster, 'The Opacity of Transparency' 91 (2006) Iowa Law Review 885; DE Pozen, 'Seeing Transparency More Clearly' 80 (2020) Public Administration Review 326.

[2]See, in general, CA Tschider, 'Legal Opacity: Artificial Intelligence's Sticky Wicket' 106 (2021) Iowa Law Review Online 126. For an in-depth discussion on AI opacity in criminal law and procedure, see F Palmiotto, 'Artificial Intelligence and the Transformation of Criminal Trials in Europe' (PhD thesis, European University Institute 2023).

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

output data) – to epistemic challenges, such as the inability for humans to provide an explanation for the outcome of an AI system. The 'state of not knowing'[3] AI systems depends on multiple factors. A particularly significant one is that AI systems are utilised and developed behind closed doors. Design choices and processes operate within, and are nurtured by, a legal architecture that constructs and maintains secrecy on multiple levels. In outline, secrecy is both 'intentional' and 'legal'. It is 'intentional' because actors involved in AI governance, whether a private or a public actor, choose to rely on or at least find themselves operating in a regime enabling secrecy. It is 'legal' because it is fortified by and grounded on a plethora of legal frameworks that enable an information holder to keep information about AI (its components, and even more fundamentally the fact of being developed) secret.[4]

A secrecy-infused legal patchwork impacts the possibility for actors other than those in control to access their informational components (such as training data, algorithms, technical documentation and so forth). Yet, secrecy is an often-untold story when looking into public sector applications of AI systems. Of course, these tools offer great potential for making operations more efficient and effective. Key applications encompass the growing use of AI systems by public bodies even in areas hugely sensitive for citizens and their lives,[5] including experimentation at national level in the fields of migration, asylum, criminal justice, social welfare, education and taxation.[6] Governmental agencies and public bodies increasingly classify AI development and research, especially in domains with military or security implications, in order to safeguard AI-related information and maintain a strategic edge.[7] We will call these sources of AI political secrecy.[8] Political secrecy is preferred as a term rather than the more descriptive term of public secrecy to highlight the politically motivated aspects of secrecy in a public governance context.[9] When involved in developing AI, private developers can rely upon other secrecy regimes (such as trade secrets) which make algorithmic systems all the more inaccessible to the public. We can refer to these as forms of AI private secrecy.[10] Stated concisely, different strata of concealment, with different rationales and pertaining to different branches of law, apply to AI and operate in tandem.

A striking illustration of the coexisting secrecy trends is border governance in the EU. Migration has always been a site of intertwinement between public needs and private interests. The increasing algorithmisation of border control has turned such coalescing into a path dependency of EU agencies such as Frontex and eu-LISA, tying them to often large private vendors providing and maintaining state-of-the-art AI-driven technology. To a very significant

[3]J Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' 3 (2016) Big Data & Society 1, 4.

[4]F Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 6. See below Paragraphs 3–4.

[5]H Bloch-Wehba, 'Access to Algorithms' 88 (2020) Fordham Law Review 1265; M Busuioc, 'Accountable Artificial Intelligence: Holding Algorithms to Account' 81 (2021) Public Administration Review 825; NA Smuha, *Algorithmic Rule by Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law* (Cambridge University Press 2025).

[6]In general, see K Levy et al, 'Algorithms and Decision-Making in the Public Sector' 17 (2021) Annual Review of Law and Social Science 309. See also the examples of domestic experimentation in migration described in N Vavoula, Tr–AI–Ns forming Migration, Asylum and Border Management in the EU: The Roles of the AI Act, Interoperable Large-Scale It Systems and EU Migration Agencies (2024) SSRN 4–6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4765470> accessed 2 December 2024. The reliance for example by tax authorities in the Netherlands on a 'learning algorithm' as a decisional aid in childcare social welfare benefits assessments resulted in state-sanctioned discrimination and life changing consequences for affected individuals. See further D Hadwick and S Lan, 'Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany' 13 (2021) World Tax Journal 609.

[7]<www.justsecurity.org/104242/memorandum-ai-national-security> accessed 27 December 2025; <https://www.csis.org/analysis/addressing-national-security-implications-ai> accessed 27 December 2025; <https://carnegieendowment.org/research/2024/06/artificial-intelligence-national-security-crisis> accessed 27 December 2025.

[8]See Paragraph 3.

[9]See, too, B Rittberger and KH Goetz, 'Secrecy in Europe' 41 (2018) West European Politics 825, 826.

[10]See Paragraph 4.

extent European research funding gives academics and private consortia safe spaces to construct and develop often far-reaching systems of border control (for example, iBorderControl).[11] This development of AI systems, amply funded by public money, means that they are often not developed in house as such by European officials. The subsequently applied AI systems are frequently procured from private vendors, which are large conglomerates of the tech industry.[12] As AI development is thus often outsourced, private contractors may (and do) keep their AI systems opaque to bolster, in accordance with existing legal frameworks, their (ongoing) competitive advantage over other firms. That motive is then imported into public governance, the consequence being that officials may share or conceal bits of information internally in a whole host of ways.

The growing enmeshment of private and public actors in developing and employing AI systems makes it more difficult to consider one set of secrecy enablers separated from the others, albeit underscored by different motivations. The cross-cutting approach of the European AIA[13] even reinforces this coming together of public and private forms of secrecy,[14] and underscores the importance of considering both dimensions side by side. The compresence of secrecy across public and private domains is unprecedented in terms of scale and application across potentially all policy domains.[15] The secret development of AI ends up thwarting public values and normative foundations running the gamut from public accountability to transparency.

Our paper examines the intertwined range of public and private legal drivers of secrecy covering procured AI technology in the field of migration governance in Europe, illustrating how they come together and undermine affected persons (such as third country nationals), watchdogs, pressure groups and researchers. The paper comes in four consequential parts. Paragraph 2 reveals AI secrecy as an institutional framework that consists of both public law and private law forms of secrecy and is informed by varying degrees and layers of opacity (a spectrum of deep and shallow secrets). Paragraph 3 explores the sources of what we call 'political secrecy' of AI systems, variously manifesting in forms of secrecy operated by migration and security authorities in ways that tend to shield the existence and use of AI systems from public awareness. Paragraph 4 turns to analyse the legal frameworks that shape and maintain AI vendors' private forms of secrecy that are highly relevant in the context of migration governance. In analysing the various sources of political and private secrecy, we also refer to how the AIA barely makes a dent in the intertwined legal framework of AI secrecy. We then close by condensing the core takeaways and some countervailing strategies in Paragraph 5. The conclusion looks wider at the general implications of AI secrecy beyond migration governance, including national security, defence and law enforcement.

[11]See, EuroMed-Right and Statewatch, 'Europe's Techno Borders', July 2023, <https://euromedrights.org/wp-content/uploads/2023/07/EuroMed-Rights_Statewatch_Europe-techno-borders_EN-1.pdf> accessed 8 November 2025.

[12]L Tangi et al, *AI Watch. European Landscape on the Use of Artificial Intelligence by the Public Sector* (Publications Office of the European Union 2022); M Hickok, 'Public Procurement of Artificial Intelligence Systems: New Risks and Future Proofing' 39 (2024) AI and Society 1213; A Sanchez-Graells, 'Public Procurement of Artificial Intelligence' 2 (2024) Legal Tech LTZ 122. For a general overview on the leniency towards AI procurement, see also European Commission, *Adopt AI Study: Final Study Report* (Publications Office of the European Union 2024) 26 <https://digital-strategy.ec.europa.eu/en/library/eu-study-calls-strategic-ai-adoption-transform-public-sector-services?pk_source=ec_newsroom&pk_medium=email&pk_campaign=Shaping%20Europe%27s%20Digital%20Future%20website%20updates> accessed 9 April 2025. For an analysis on the public sector use of AI in the US, see D Freeman Engstrom et al, 'Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies' (2020) Report for the Administrative Conference of the United States 18 <www.acus.gov/sites/default/files/documents/Government%20by%20Algorithm.pdf> accessed 9 April 2025. The study shows that AI tools are 53 per cent of AI applications were being developed in-house, whereas the remaining 47 per cent were outsourced.

[13]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) OJ L 2024/1689 ('AIA').

[14]AIA, Art 78. Specifically on the AIA, see further Para 3.C below.

[15]See Conclusion.

2. Conjoining secrecy in AI law and governance

A. How and why private and political secrecy converge in public-sector AI

Inquiries into AI secrecy frequently come in silos. Conventional analyses tend to compartmentalise the private and public legal sources of secrecy, treating them as sort of separate, self-contained domains. Examples of these approaches abound. For instance, intellectual property law scholars are inclined to look into the extent to which trade secrecy and other IP rights cover AI systems[16] and how public interest limitations come into play.[17] Viewing private secrecy as an obstacle to public accountability, other authors falling in the same camp look to find legal doctrines (such as 'information publicity' in the US)[18] or exceptions and limitations[19] that can serve the purpose of disclosing corporate forms of secrecy. Not nearly as much ink has been spilled on public law forms of secrecy (such as state secrecy, security and classified information), which enable governments and public bodies to keep AI systems under wraps when they utilise AI systems.[20] The existing scholarship, more or less implicitly, tends to (over-)stress an analytical demarcation between the AI systems held secret by corporations and the secrecy regimes applied by public administrations to keep the functioning of AI systems secret in turn.

Yet, the reliance on such separation is particularly odd because current trends and practices in AI deployment in public governance frequently take an intertwined course via public procurement. These trends more broadly shape the dynamics of private–public relationships across various areas of interests. For one thing, the commingling of public and private actors in the employment of AI-driven technology for public functions responds to a narrow view of government efficiency, which ends up favouring procurement from the private sector over other arrangements.[21] Many of these applications rely on AI technology that is privately developed and made available to public actors. In Europe, both law and political science scholars have signalled the emergence of out-and-out 'migration markets' in the realm of European border and asylum governance.[22] The realisation of European-wide databases for governing entry of so-called third country nationals has traditionally involved large private vendors through large framework contracts. For example, in 2019 the implementation and maintenance of the Entry–Exit System (EES) was awarded to a consortium of IBM Belgium BVBA, Atos Belgium NV and Leonardo S.p.a. for 142 million euros.[23] The upkeeping of SIS II and Eurodac have been respectively procured from Atos, Accenture and HP, and from Bull Atos Technologies, Sopra Steria and Gemalto.[24]

[16]SK Sandeen and T Aplin, 'Trade Secrecy, Factual Secrecy and the Hype Surrounding AI' in R Abbott (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar 2022); U-M Mylly, 'Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information' 54 (2023) IIC International Review of Intellectual Property and Competition Law 1013.

[17]K Foss-Solbrekk, 'Searchlights across the Black Box: Trade Secrecy versus Access to Information' 50 (2023) Computer Law and Security Review 1.

[18]CJ Morten, 'Publicizing Corporate Secrets' 171 (2023) University of Pennsylvania Law Review 1319. See also SK Katyal, 'Private Accountability in the Age of Artificial Intelligence' 66 (2019) U.C.L.A. Law Review 54, 117ff.

[19]This is more common in the European perspectives. See Sandeen and Aplin (n 16).

[20]For an analysis of the US, see however AS Deeks, 'National Security AI and the Hurdles to International Regulation' (2023) The Digital Social Contract: A Lawfare Paper Series <https://www.lawfaremedia.org/article/national-security-ai-and-hurdles-international-regulation-0> accessed 12 November 2024; A S Deeks, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* (Cambridge University Press 2025).

[21]JE Cohen et al, 'Provisioning Digital Tools and Systems for Government Use' (2024) Preliminary Concept Paper-Redesigning the Governance Stack, Georgetown Law 8 <https://ssrn.com/abstract=4958214> accessed 11 November 2024; M Lemberg-Pedersen et al, 'Advancing Alternative Migration Governance: The Political Economy of Entry Governance' (2020) ADMIGOV Deliverable 1.3 <http://admigov.eu> accessed 4 December 2024.

[22]Lemberg-Pedersen et al (n 21) 16ff; D Bigo, 'The Digitalisation of Border Controls and Their Corporate Actors' in M Bosworth and L Zedner (eds), *Privatising Border Control: Law at the Limits of the Sovereign State* (Oxford University Press 2022); F Infantino, 'How Do Private Companies Shape Responses to Migration in Europe? Informality, Organizational Decisions, and Transnational Change' 18 (2024) Regulation and Governance 837.

[23]Lemberg-Pedersen et al (n 21) 69.

[24]Ibid., 70.

In 2020, Frontex and eu-LISA jointly commissioned a range of contractors (such as Leonardo and Unisys Belgium SA) under a sweeping Transversal Engineering Framework ('TEF') worth 181 million euros to design, support, maintain and test core business systems as well as interoperability components and infrastructure for new EU-wide systems.[25]

The vast majority (if not all) of these IT systems are (very probably) being enhanced with AI technology to further automate their operations.[26] This potentially hands private contractors vast technical and political clout about which we know very little overall. The first lot of the TEF (allotted to Unisys Belgium NV/SA, Unisystems Luxembourg SARL and Wavestone SA) involves the study, development and implementation of AI techniques to infer patterns from travellers data stored in the Central Repository for Reporting and Statistics ('CRRS').[27] Further, Frontex concluded in late 2024 several contracts to supply commanded aerial devices for operations related to its tasks and mandate, with vast sums of (public) money involved.[28] The tender to equip the agency with a medium-altitude, long-endurance remotely piloted aerial system is worth 184.3 million euro.[29] In fact, private companies have typically furnished a wider range of military and security equipment, including biometric identification systems.[30] Even though the procurement documentation is publicly available,[31] there is in any event a glaring absence of easily accessible information on whether AI is used, or how the making and implementation of the AI system is taking place.[32] Infantino speaks of 'a "black box" within the "black box" of policy implementation' in the field of migration governance in Europe.[33] Bigo highlights the wider (political) context of corporate actors who fundamentally shape the European IT architecture, their role being that of 'visionaries of a future in the making'.[34] Yet that critical part is entirely hidden from public view and scrutiny.[35]

[25] <https://ted.europa.eu/en/notice/-/detail/626975-2020> accessed 27 December 2025.

[26] N Vavoula, 'Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism' 23 (2021) European Journal of Migration and Law 457; Vavoula (n 6) 9–18 (mentioning facial recognition technologies and algorithmic profiling).

[27] eu-Lisa, 'AI in CRRS in the Context of ETIAS and Revised VIS Final Report', 14 November 2022, mentioned by C Jones and R Lanneau, 'Automating Authority: Artificial Intelligence in European Police and Border Regimes' (2025) Statewatch Report ch 3 <https://www.statewatch.org/automating-authority-artificial-intelligence-in-european-police-and-border-regimes/> accessed 30 April 2025 (in footnote).

[28] See the tender notice at <https://ted.europa.eu/en/notice/-/detail/527115-2024> accessed 30 January 2026. The contract was divided into two lots: Leonardo was awarded one lot, whereas Airbus subsidiary Airbus DS Airborne Solutions ('ADAS') the other. Airbus also engaged an Israeli government-owned subcontractor (Israel Aerospace Industries, 'IAI'), as indicated by the official statement from Airbus at <https://airbusds-airborne.com/> accessed 30 January 2026 and the press release by IAI at <https://www.iai.co.il/about/press-release/second-time-running-frontex-selects-airbus-partnership-israel-aerospace> accessed 30 January 2026). The IAI's statement confirms that ADAS and IAI were already awarded previous contracts, acknowledging a consolidated dominance in the provision of drones. The news also covered the procuring process. See among others 'EU's Frontex Procures New Israeli UAV for Maritime Surveillance' (Naval News, 19 December 2024) <www.navalnews.com/naval-news/2024/12/eus-frontex-procures-new-israeli-uav-for-maritime-surveillance/> accessed 24 April 2025; P Felstead, 'ADAS and IAI to Continue Supporting Heron Operations for Frontex' (*European Security & Defence*, 6 January 2025) <https://euro-sd.com/2025/01/major-news/41918/frontex-heron-ops-continue> accessed 24 April 2025.

[29] See <https://ted.europa.eu/en/notice/-/detail/527115-2024> accessed 27 December 2025.

[30] See Bigo (n 22); Lemberg-Pedersen et al (n 21).

[31] FRONTEX/2024/OP/0009, EU Funding & Tenders Portal <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/acc779af-00e9-4487-a475-2578220559ab-CN#anchorDocuments> accessed 24 April 2025.

[32] Hickok (n 12) 1221. In the example we have illustrated, for instance, the Data Processing Agreement between Frontex and the contractors states that 'due to the sensitive nature of the data', the specific categories of data subjects and data categories are disclosed 'upon award of the Framework Contract' (see FRONTEX/2024/OP/0009, n 30). However, the finalised Framework Contract concluded by the parties is not publicly accessible.

[33] Infantino (n 22) 838.

[34] Bigo (n 22) 241.

[35] See however the interesting field work and methodology applied by Infantino (n 22), to nonetheless show importance also of informal contacts and processes.

Ensconced in these environments, procurement of AI-driven migration technology from private actors challenges a clear separation between private and public (political) forms of secrecy in a formal setting. This makes migration a field where secrecy thrives more widely than in other settings. In fact, since both private agents (contractors or vendors) and deploying public agencies in migration are involved, both can leverage secrecy regimes and adopt secrecy-enhancing strategies. Broadly speaking, secrecy claims mutually reinforce one another. This does not mean that they respond to the same needs and interests, nor that they always align. Take the example of an individual (such as a migrant) or an entity such as an NGO making an access request. Even though public administrations intended to provide access to AI-related information on transparency grounds, private vendors may in turn reject any access to safeguard their own economic interests.[36] The public authority, for its part, may also not be willing to share access to AI-related information with an applicant on the ground of safeguarding public security.[37] Migration and security authorities may keep ongoing experimentations in AI use under wraps in a way that the public is not even aware of its occurrence. If a leak takes place, then journalists and researchers may seek more information and make the public aware of some details.[38]

The compresence of private and political secrecy over AI systems calls their demarcation into question because in the final analysis they equally contribute to undermining public transparency and accountability.[39] More specifically, two reasons substantiate why we should analyse private and political forms of secrecy together. First, ultimately affected are the people on the receiving end: individuals who ought to be served by public bodies acting in the public interest.[40] The accentuated vulnerability of the persons affected by public and private choices in border control (third-country nationals) makes the latter a particularly sensitive sector requiring careful design, implementation and management of algorithmic systems.[41] To ensure this, watchdogs and pressure groups are at the forefront of filing freedom of information requests to have the secrets disclosed to the public. Therefore, a holistic understanding and conceptualisation of the various sources of secrecy, together with the actors leveraging them, proves essential to keep up with the reality on the ground.

Second, in both private and political forms of secrecy, restricted reason giving is their final outcome. For one thing, governments and public administrations rely on political secrecy in areas of (national) security, arguing that classified decisions or information, or unclassified but restricted information need to remain internal and not be shared with the public or other audiences. Private actors, on the other hand, rely on variants of secrecy to keep their own

[36]See Para 4 below.

[37]See Para 3.A.

[38]This seems to be what happened in the UK government context where *The Guardian* revealed in April 2025 that the UK Ministry of Justice was internally developing a murder prediction tool that can predict the people most likely to kill (V Dodd, 'UK Creating "Murder Prediction" Tool to Identify People Most Likely to Kill' (*The Guardian*, 8 April 2025) <www.theguardian.com/uk-news/2025/apr/08/uk-creating-prediction-tool-to-identify-people-most-likely-to-kill> accessed 24 April 2025). The NGO Statewatch had obtained documentation about the project via access to information requests and shared these materials (including the data sharing agreement) publicly online ('UK: Ministry of Justice secretly developing "murder prediction" system' (*Statewatch*, 8 April 2025) <www.statewatch.org/news/2025/april/uk-ministry-of-justice-secretly-developing-murder-prediction-system/#_ftn5> accessed 24 April 2025).

[39]On the interplay between trade secrecy and public accountability, see Hickok (n 12) 1220–1; J Villasenor, 'Artificial Intelligence, Trade Secrets, and the Challenge of Transparency' 25 (2024) North Carolina Journal of Law & Technology 495. More generally on the (contested) interrelation between intellectual property and public security, see C Duan, 'Of Monopolies and Monocultures: The Intersection of Patents and National Security' 36 (2019) Santa Clara High Technology Law Journal 369; P Drahos, 'Immoral Intangibles: Engaging with Ned Snow's Intellectual Property and Immorality' 28 (2023) Jerusalem Review of Legal Studies 124.

[40]S Ranchordás and L Scarcella, 'Automated Government for Vulnerable Citizens: Intermediating Rights' 30 (2021) William & Mary Bill of Rights Journal 373.

[41]C Isabel Velasco Rico and M Laukyte, 'ETIAS System and New Proposals to Advance the Use of AI in Public Services' 54 (2024) Computer Law & Security Review 1.

commercial interests over AI systems away from their competitors, but also from the public more generally, and even from government officials. So, the very outcome of both political and private secrecy remains largely the same, much as the undergirding reasons and rationales for adopting secrecy regimes may differ.

B. AI secrecy in migration governance: unearthing deep and shallow secrets

Placing political and private secrecy on the same analytical plane warrants their examination through a unitary conceptual lens. More fundamentally, focusing on the structure of a secret and its strength or weakness shifts debates on AI secrecy onto another level: that of positioning the sources of secrecy within the social practices, relational networks and power disparities the governmental use of procured AI systems triggers. Pozen's seminal analysis of 'deep secrecy' in the governmental sector, which draws and expands on previous research conducted by Scheppele in the realm of contract law,[42] is a helpful benchmark to understand better private and public (AI) secrecy and its implications for migration governance.

Pozen distinguishes deep secrets from shallow secrets. Secrecy is deep 'if a small group of similarly situated officials conceals its existence from the public and from other officials, such that the outsiders' ignorance precludes them from learning about, checking, or influencing the keepers' use of the information'.[43] National security decision making has traditionally been considered a deep secret protected by extensive and interlocking classification systems of documents and information.[44] Systems of information security (classified information) protect the executive power both as a matter of internal security and of external security and make it very difficult to hold the executive to account.[45] Conversely, secrets are shallow 'if ordinary citizens understand they are being denied relevant information and have some ability to estimate its content'.[46] Shallow secrets are capable of being known, in the sense that some reference is made to them. Further details on shallow secrets may for example be requested in freedom of information requests (and may subsequently be denied because of a plethora of legal exceptions: trade secrecy, privacy or public security). By contrast, deep secrets typically emerge into public view if there is leaking or whistleblowing from within the security administration.

This structural conceptualisation that pivots on depth is particularly effective and apt to describe governmental secrets in the way it visualises them according to the degree of unearthing by inside or outside forces. The bottom line is that there is no rigid dichotomy. Secrets are not set in stone. They rather flow along a continuum and are more or less deep (or more or less shallow) based on the degree to which four indices come into play. First, how many people know: the more members of a community know, the shallower the secret becomes.[47] Another element is what sort of people know, or more precisely, what kinds of public officials and administrations are aware of the concealed information.[48] Thirdly, it is important to consider how much they know: the less one is aware about the processes and the 'functional understandings' that lead to certain outcomes, the deeper is the secret.[49] Fourth, secrecy depth (or shallowness) is affected by the passage of time. A secret can be extremely deep at inception, but the information, its content and workings can progressively trickle out of its keeper.[50] Secrecy may thus become more translucent over time and grow shallower. Taken together, the four indices of secrecy point to a dynamic and contextual

[42]K Lane Scheppele, *Legal Secrets: Equality and Efficiency in the Common Law* (University of Chicago Press 1988).
[43]DE Pozen, 'Deep Secrecy' 62 (2010) Stanford Law Review 257, 274.
[44]Ibid., 275.
[45]See US Secretary of Defense Donald Rumsfeld's quote on the difference between 'known unknowns' and 'unknown unknowns' at Ibid., 259.
[46]Ibid., 274.
[47]Ibid., 268.
[48]Ibid., 269.
[49]Ibid., 270.
[50]Ibid., 273.

notion of secrecy. Thus, it is key to ask, '*how* deep or shallow [a secrecy] is to *society as a whole*',[51] as well as to consider how even deeper secrets are being or may be unearthed and brought more into (shallower) light, also in the context of AI.

Pozen's conceptualisation may usefully be employed to describe secrecy of AI use by public bodies for migration governance. Depending on the level of concealment, both forms of private and public secrecy relate to the public fundamentally in two different ways. Some secrets around AI are deeper than others. This is the case when the publics (in the realm of border control, third country nationals, EU citizens, researchers and watchdogs) are 'in the dark about the fact that they are being kept in the dark' about AI, if you will. For instance, the deepest forms of secrecy occur when the publics do not have the slightest idea that a public body or agency has been using an AI system that affects their position in some way or another. Lacking this knowledge, they are not in the position to trigger the legal protection afforded to them. As Paragraph 3 shows, cases vary, with researchers and pressure groups often suspecting the use of AI systems and therefore being driven to make access requests. AI-related deep secrecy does not have quite the same pedigree in AI governance literature as its conceptual opposite, shallow secrecy. If a secret is shallow, the party from which information about AI is withheld is conscious about the AI system existing and operating. They might well not appreciate how it operates and functions, but they might know that they are exposed to an AI system. They are in the state of 'not knowing' for the reasons we have referred to in the Introduction, that is because AI is in and of itself opaque,[52] or because meanwhile information about AI has come to public attention.

With this framing in mind, the following sections will now probe deeper into how deep or shallow both political and private forms of secrecy of AI systems are utilised for migration governance.

3. Political secrecy

Political secrecy is traditionally linked to struggles over the distribution and preservation of political power.[53] For an important part, it was constructed around fortresses designed to prevent secret unearthing by anyone other than those with (strict) security clearances. As such, it comes with powerful 'privileges', also for the democratic state,[54] traditionally nestled within core government administration, mainly in matters of security and defence. Today, it has come to include ever widening circles of officials and private actors involved in the broader business of governing.[55]

Nowadays a much broader securitisation environment[56] provides fertile breeding ground for AI-related deeper secrets to thrive, and Frontex has been in the vanguard of policing its secrets often on very general grounds. Further political decisions may be hidden from view in datafication processes, including (big) databases, and their subsequent algorithmisation.[57] There are several examples in the EU where it is possible to discern political power in technical implementation, but

[51] Ibid., 267.

[52] That is the meaning and contexts of secrecy on which literatures in AI secrecy routinely concentrate. On AI opacity, see generally Burrell (n 3).

[53] Rittberger and Goetz (n 9); D Mokrosinska, *State Secrecy and Democracy: A Philosophical Inquiry* (Routledge 2024).

[54] M Fenster, *The Transparency Fix: Secrets, Leaks, and Uncontrollable Government Information* (Stanford University Press 2017).

[55] See, for example, Lemberg-Pedersen et al (n 21); C Batka and J Bátora, 'The European Union's Use of Contractors in Security and Defence: Blazing Its Own Path of Institutional Change?' [2024] European Security 1.

[56] On the securitisation narrative and Frontex, see M Gkliati and J Kilpatrick, 'Crying Wolf Too Many Times: The Impact of the Emergency Narrative on Transparency in FRONTEX Joint Operations' 17 (2021) Utrecht Law Review 57.

[57] See A Karaiskou and N Vavoula, 'Extrajudicial and Judicial Remedies in Algorithm-Assisted Decision-Making: The Case of EU IT Systems for Migration and Security' (2024) EUI LAW Working Paper 2024/21 <https://hdl.handle.net/1814/77692> accessed 24 April 2025; N Vavoula, 'Algorithmic Accountability Through the "Human over the Loop" in Interoperable and EU AI-Reliant Large-Scale IT Systems for Migration and Security' 9 (2024) European Papers 1228.

not that many (yet) where it is clear whether AI components are being used.[58] As Musco Eklund aptly observes, 'recognising the political in the technical' is key where technology has regulating power and inherent normative force.[59]

To map further the legal terrain of political secrecy in European migration governance, Paragraph 3 is divided into a further two subparagraphs that each highlight a different legal regime that regulates different aspects of political secrecy. In the Access Regulation[60] we observe how exceptions of public security, formulated almost three decades ago, can largely trump public access to AI-related information held by migration authorities in the digital era (Paragraph 3.A). In Paragraph 3.B the focus is on the evolving roles of the European Border Guard Agency ('Frontex') and eu-LISA, also in relation to the ETIAS data system which has been delayed to being operationalised in 2026.[61] Lastly, Paragraph 3.C looks into how the AIA leaves political secrecy untouched.

A. Seeing the political domination of 'public' security claims

Executive power is reinforced in practice and incrementally at the supranational level in a non-centralised and non-unitary way, in particular in European agencies. Frontex, the European Border and Coast Guard Agency, is a case in point. Frontex has emerged already for some years as an unseen (sub-)political actor operating below the constitutional radar with overtly technical governance that at the same time is substantively political. It is a 'a hub for surveillance and data sharing'.[62] Some see in the way Frontex exercises its political discretion today that it in reality is 'more akin to a national security or intelligence agency, rather than a civilian border management agency'.[63] Frontex is in any event considered at the forefront of quasi militarised, highly securitised enforcement practices in Europe,[64] and is thus readily able to resist disclosure of many of its documents and the documents it holds of others on grounds of public security.

The mandatory public security exception in the Access Regulation, in effect, furnishes the ideal legal framework to build secrecy around AI use[65] by Frontex. The existence of AI systems being used by security and migration authorities is surrounded by secrecy leaning towards the deep camp. In fact, the public is generally not aware of its ongoing existence and experimentation. This

[58]See Commission, 'Communication to the Commission – Artificial Intelligence in the European Commission (AI@EC) – A strategic vision to foster the development and use of lawful, safe and trustworthy Artificial Intelligence systems in the European Commission' (2024) 380 final. The examples given by the Commission all concerned internal complaint handling and competition law and, on the whole, do not affect individuals directly. Yet, systems like the 'Complaints Handling with AI (CHAI)' aim to detect fraud/cybersecurity/disinformation and may determine the individual final administrative decision in a decisive way.

[59]A Musco Eklund, 'Limits to Discretion and Automated Risk Assessments in EU Border Control: Recognising the Political in the Technical' 30 (2024) European Law Journal 103.

[60]Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L145/43 (Access Regulation).

[61]See, European Commission, Revised timeline: <https://travel-europe.europa.eu/revised-timeline-ees-and-etias-2025-03-07_en#:~:text=The%20EES%20is%20expected%20to,the%20last%20quarter%20of%202026> accessed 27 December 2025.

[62]S Gandhi, 'Frontex as a Hub for Surveillance and Data Sharing: Challenges for Data Protection and Privacy Rights' 53 (2024) Computer Law & Security Review 1.

[63]This is how the complainant puts it in European Ombudsman Decision in Case 344/2023/PVV on how the European Border and Coast Guard Agency (Frontex) dealt with a request for public access to documents concerning social media monitoring related to migration routes [2024] para 32.

[64]It has been from its inception: see A Neal, 'Securitization and Risk at the EU Border: The Origins of FRONTEX' 47 (2009) Journal of Common Market Studies 333; Gkliati and Kilpatrick (n 56) 59.

[65]Access Regulation, Art 4(1) ('the institutions shall refuse access to a document where disclosure would undermine the protection of: (a) the public interest as regards: [...] public security'). See further Deirdre Curtin and Adrian Rubio, 'Regulation 1049/2001 on the Right of Access to Documents Including the Digital Context: Study Commissioned by Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament' (2024) <www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2024)762890> accessed 24 April 2025.

is not only a matter of original political design, but of ongoing and intentional concealment by politicised bureaucracies. Twenty-five years into the Access Regulation's regime, this is all the more striking since the context has radically changed and the necessity of the concealment of automated decision making affecting vulnerable individuals is not a given 'in the public interest'. If Frontex wishes to keep the public in the dark as to its tools and methods and obfuscate reality, then the Access Regulation positively assists this deliberate concealment.[66] This is so even when the same public authority has been actively exploring the utility of using AI in certain contexts for some years.[67] Researchers and NGOs trying in their perception of the public interest to unearth some of the facts, to get even a sense of the existence of AI tools being piloted or developed, are overall stopped in their tracks as the Access Regulation allows EU institutions to rely on secrecy where the institution or agency in question claims 'public security in the public interest'.[68] In fact, secret-keeping on 'public' security (for whatever reason) is considered 'in the public interest'. Hence the conclusion that the exact use of AI thus remains a deep secret. Interestingly, public interest considerations also inform migration authorities' conduct in their capacity as public buyers in procurement procedures. When deciding on the contract award and the information to provide to candidates and tenderers, contracting authorities may, among other things, 'decide to withhold certain information where its release would impede law enforcement' or 'would be contrary to the public interest'.[69] Even more fundamentally, the contracting authority may decide to declare a contract secret.[70] This ends up embedding deep secrecy in the fabric of the private–public relationship.

If some partial access is given, then some vistas of shallowness emerge with the prospect of more information in the future. Given the explicit terminology in the Access Regulation, there is however little to be done even where a negative decision is appealed to a court or the Ombudsman other than to ask the administration to double check the number of documents requested to see if some (partial) access can be given, or to confirm (having seen the documents in question, which anyway to be requested will need to be a relatively shallow secret) that the risk to 'public security' is not hypothetical.[71]

[66]For pre-AI account on Frontex, see M Fink and M Hillebrandt, 'Access to Documents and the EU Agency Frontex: Growing Pains or Outright Obstruction?' in M Hillebrandt et al (eds), *(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice* (Routledge 2023).

[67]See, for example, the research report commissioned by Frontex already in 2021 from RAND Europe: RAND Europe, 'Artificial Intelligence Capabilities for the European Border and Coast Guard: Final Report' (2021) <www.rand.org/pubs/external_publications/EP68583.html> accessed 24 April 2025. See too EuroMed Rights and Statewatch, 'Europe's Techno Borders' (2023) <https://euromedrights.org/wp-content/uploads/2023/07/EuroMed-Rights_Statewatch_Europe-techno-borders_EN-1.pdf> accessed 24 April 2025.

[68]See Gkliati and Kilpatrick (n 56). See too Statewatch, 'Research on AI-based Capabilities for Frontex' (*Statewatch*, 16 January 2021) <www.statewatch.org/observatories/frontex/access-to-documents-requests/research-on-ai-based-capabilities-for-frontex/> accessed 24 April 2025.

[69]Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union (recast), OJ L 2024/2509, Art 173(3).

[70]Regulation (EU, Euratom) 2024/2509, annex I, points 11(1)(i) and 38(2). It is unclear the extent to which contracting authorities may declare contracts secret under procurement rules regarding European institutions and agencies (such Frontex and eu-LISA). The procurement framework applicable to national public bodies provides an exclusion of contracts that are essential to protect national security interests (Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, OJ L 94/65 (Public Procurement Directive), Art 34).

[71]See, for example, European Ombudsman Decision Case 1087/2022/SF on how the European Border and Coast Guard Agency (Frontex) dealt with a request for data concerning the resources deployed in two joint operations [2023]; European Ombudsman Decision Case 1838/2021/DL on how the European Commission dealt with a request for public access to documents concerning a procurement procedure related to strategic communication services [2022]; European Ombudsman Decision Case 233/2021/OAM on how the European Border and Coast Guard Agency (Frontex) dealt with a request for public access to documents concerning tracking data of vessels used in Frontex maritime operations [2021]; European Ombudsman Decision Case 1558/2024/NH on the refusal by Frontex to provide full public access to documents related to Joint Operation Opal Coast [2025]; European Ombudsman Decision Case 1497/2024/ACB in which the EO found that the refusal of access to two decision from the Frontex's FR office was excessive and recommended Frontex to reconsider its position [2025].

By and large, there are several still relatively shallow furrows being ploughed by civil society applicants in search of even a little more precision on whether (when suspected) and how automated techniques like AI are (already) being used. Thus, information concerning use of publicly available data on social media platforms for example by Frontex (scraping profiles of migrants and asylum seekers) relating to migration routes is sought[72] because they are often used in order to train algorithms and in order to develop AI solutions (algorithms).[73] Such information is used for the agency's risk analysis according to Article 29 of the EBCG Regulation,[74] and subsequently for the conception and formulation of operational responses. But whether and how they are actually used for such purposes may remain a deep secret even after appeals to the European Ombudsman. Furthermore, it is hard to imagine that not just citizens and researchers, but also public officials outside those directly involved in migration governance are in the know of AI technologies being employed for migration governance. Yet, Frontex has already argued some years back in favour of the use of more publicly available data from social media in the framework of the democratisation of AI.[75]

The contemporary role of Frontex includes as well more overtly political tasks, such as carrying out high-scale, AI-driven surveillance using procured technologies like drones.[76] On the website of Frontex a private contractor elaborates: '[o]ur drone detection software uses artificial intelligence and detection algorithms to look for unique patterns defining drone/RC protocols of communications, efficiently discriminating drones from other objects'.[77] That drones are being used emerges also through access to documents cases, but Frontex steadfastly refuses to give any access to documents or information, not even to an investigation report into the crash of a Frontex drone.[78] Interestingly, this latter decision shows that the private contractor was consulted about the request to access its documents and they refused any disclosure.[79] Frontex also argued that disclosing the document would affect its current and future ability to negotiate contracts of a similar kind. It relied on its wide margin of discretion whether disclosing certain information could pose a risk to the public interest as regards public security.

B. Technical and operational secrecy by political design: keeping ETIAS under wraps

Frontex will also run the European Travel Information and Authorisation System (ETIAS) that will grant travel authorisations to third country and non-EU travellers (TCN travellers) once it is launched finally in 2026. It has been under preparation (and its technical and design details under wraps) for almost a decade. ETIAS travel authorisations (they can be compared to

[72]RAND Europe (n 67) 26.

[73]See J Milaj and J Pia Mifsud Bonnici, 'Transparency as the Defining Feature for Developing Risk Assessment AI Technology for Border Control' [2024] International Review of Law, Computers & Technology 1.

[74]Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and Repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L295/1 (EBCG Regulation).

[75]See the documents cited in <www.edps.europa.eu/system/files_en?file=2023-01/2022-0977_002_redacted.pdf> accessed 27 December 2025, in the context of European Ombudsman Decision on how the European Border and Coast Guard Agency (Frontex) dealt with a request for public access to documents concerning social media monitoring related to migration routes (case 344/2023/PVV) <www.ombudsman.europa.eu/en/decision/en/192720> accessed 24 April 2025.

[76]This is very evident in the Pylos shipwreck case. See European Ombudsman Case OI/3/2023/MHZ on how the European Border and Coast Guard Agency (Frontex) complies with its fundamental rights obligations with regard to search and rescue in the context of its maritime surveillance activities, in particular the Adriana shipwreck (2023).

[77]CERBAIR, 'Protecting from Malevolent Drones' <www.frontex.europa.eu/assets/EUresearchprojects/Documents_for_the_news/CERBAIR_C-UAS_presentation.pdf> accessed 24 April 2025.

[78]Decision on the refusal by the European Border and Coast Guard Agency (Frontex) to give public access to an investigation report into the crash of a Frontex drone (case 632/2024/OAM) <www.ombudsman.europa.eu/en/decision/en/187040> accessed 24 April 2025.

[79]See further Para 4.D.

'light visas')[80] will be based on automated risk assessments as well as the social media scraping of migrants and asylum seekers. These automated risk assessments will be carried out by a profiling algorithm, called 'screening rules' in the Regulations' nomenclature.[81] Moreover, ETIAS's automated risk assessment may also draw on AI-driven management of the CRRS, which pools and renders interoperable statistical and historical data providing evidence for migration governance policymaking.[82]

Overall, competent authorities appear intent on concealing (or downplaying at best) their use of AI in public discourse. In the words of Derave and others, 'it is an open question whether ETIAS screening rules and their underlying profiling algorithms will be effectively based on AI'.[83] As Vavoula observes, 'recourse to the term "algorithm" may be seen as either a means of avoiding the loaded term of "AI" or as leaving this issue open for introducing AI in the future'.[84] For now, although the potential use of AI in ETIAS risk assessment 'is hidden into the different technical specifications of the systems',[85] there is a clear (public) intention to use it in future. This makes efforts to get more information more possible. It is no deep secret that AI is contemplated quite actively to augment ETIAS. An Eu-LISA report from 2020 indicated that ETIAS can employ AI tools in several different ways,[86] and this falls very well in line with a detailed report by Deloitte on the same theme prepared for the Commission in 2020.[87] Thus, automated risk assessments under the ETIAS Regulation amount to AI secrets positioned within the shallow camp.

Yet, Frontex has actively challenged the politics around the use of (the term) AI, and has in effect denied its use even in complaints. For example, when a group of researchers at the Université Libre de Bruxelles sought public access from Frontex on the details of ETIAS' risk assessment algorithm, Frontex insisted that it would be more appropriate to talk about filtering queries than algorithms and responded that no sophisticated analysis methods or any form of AI is involved in the risk assessment.[88] That was a few years ago now, but the explicit use of AI in this

[80]N Vavoula, 'European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications' (2017) Queen Mary School of Law Legal Studies Research Paper No. 256/2017 <https://ssrn.com/abstract=2928082> accessed 24 April 2025.

[81]See Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624, OJ L236/1 (ETIAS Regulation), recital 27 and Art 33. The ETIAS screening rules are an algorithm enabling profiling to check the data in the application form against specific indicators designed to identify if the person may pose a specific risk to security, irregular migration or a high epidemic risk (see ETIAS Regulation, Art 33). In addition, the Entry/Exit System (EES) has just entered into force. It is a complementary automated system of biometric data processing and risk analysis of third country nationals travelling within the EU for a short stay, <https://eur-lex.europa.eu/EN/legal-content/summary/the-european-union-s-entry-exit-system.html> accessed 27 December 2025.

[82]Vavoula (n 57) 1234; Jones and Lanneau (n 27) ch 3.; A Karaiskou, 'Immigration and Algorithmic Discrimination in Europe' (PhD Thesis, European University Institute forthcoming). See also references in n 27.

[83]C Derave et al, 'The Risks of Trustworthy Artificial Intelligence: The Case of the European Travel Information and Authorisation System' 13 (2022) European Journal of Risk Regulation 389, 391.

[84]Vavoula (n 57) 1234.

[85]Ibid., 1236.

[86]European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, *Security and Justice, Artificial Intelligence in the Operational Management of Large-scale IT Systems – Research and Technology Monitoring Report – Key Findings* (Publications Office of the European Union 2020) <https://data.europa.eu/doi/10.2857/989139> accessed 24 April 2025.

[87]European Commission, Deloitte and Directorate-General for Migration and Home Affairs, *Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security: Volume 1, Main Report* (Publications Office of the European Union 2020) <https://op.europa.eu/en/publication-detail/-/publication/c8823cd1-a152-11ea-9d2d-01aa75ed71a1/language-en> accessed 24 April 2025.

[88]Derave et al (n 83) 404.

context remains a shallow secret even though this far-reaching border entry system is scheduled to enter into force late in 2026.[89]

Frontex is not the only EU agency involved in ETIAS. eu-LISA is the agency responsible for its technical development and management.[90] The ETIAS regulation leaves considerable technical discretion to eu-LISA on how the algorithm will enable profiling by comparing special risk indicators with data in the application file.[91] How this is in fact to be done by eu-LISA, and with what software specifics, is nevertheless not public and is kept secret on grounds of public security.[92] eu-LISA in fact possesses significant discretion in relation to how the software, which will enable the ETIAS system, is being developed and designed for imminent application. eu-LISA is already using algorithms for biometric matching[93] in three existing systems, all of which are based on fingerprints and facial images (Schengen Information System (SIS II), Visa Information System (VIS), European Dactyloscopy (Eurodac)).[94] It is not excluded that AI-related information may be shared with other internal executive actors, such as Europol, with access to EU databases such as ETIAS.

C. Hiding in plain sight: fencing digital borders off from the AIA

The AIA constitutes the first attempt to regulate AI in migration and border management,[95] albeit in the broader context of horizontal legislation applying to all AI systems placed on the market or used in the Union falling under its scope. For a variety of reasons, the regulation reinforces the wide margin of discretion that competent authorities already possess to keep AI systems used under wraps in some way or another. The following subparagraphs will illustrate how this plays out.

Public privilege through material and temporal exclusion

Competent authorities in migration governance are subject to a material and a temporal exemption, both placing them outside the scope of transparency requirements for high-risk systems provided by the AIA.[96]

The AIA builds on the assumption that 'migration, asylum and border control management' AI systems are being used inter alia by Union institutions, bodies, offices or agencies. The regulation labels as 'high-risk' some migration applications of AI systems. Paragraph 7 of Annex III lists four specific use cases of AI systems in this area as falling within its scope as high risk systems: use as 'polygraphs or similar tools',[97] use to 'assess a risk, including a security risk, a risk of irregular

[89]See the revised timeline entry into force EES and ETIAS at <~https://travel-europe.europa.eu/revised-timeline-ees-and-etias-2025-03-07_en#:~:text=ETIAS%20is%20expected%20to%20follow,European%20countries%20using%20the%20system> accessed 27 December 2025.

[90]ETIAS Regulation, Art 6(1).

[91]ETIAS Regulation, Art 33(1). See also ETIAS Regulation, Art 20, which provides a description of the automated processing system, albeit with a high level of abstraction.

[92]There seems to be only one ETIAS case of relevance before the European Ombudsman, with no access to the documents or description of the case. See <https://www.ombudsman.europa.eu/en/case/en/66784> accessed 27 December 2025.

[93]Biometric matching is the automated comparison of visa applicants' biometric data with biometric templates acquired from all the other EU information systems, except for ETIAS which does not hold such data. 'The aim of this type of automated processing is to verify the identity of foreign travellers based on their facial features and fingerprints, and assist authorities in detecting cases of fraudulent identities, as well as in identifying those who are registered in any of these other systems as "dangerous" or undesirable' (Karaiskou and Vavoula (n 57) 18).

[94]Eurodac for example allows the collection of fingerprints (biometric data) of those who seek asylum. All fingerprints are gathered in a database (the Eurodac database), which can now be accessed by Europol and by national police forces when they are investigating some serious crimes, including terrorism. See further, N Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?' 26 (2020) EPL 131.

[95]LS Stewart, 'The Regulation of AI-Based Migration Technologies under the EU AI Act: (Still) Operating in the Shadows?' 30 (2024) European Law Journal 122.

[96]AIA, Chapter III.

[97]Ibid., Annex III, para 7(a).

migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State',[98] use to support authorities in assessing migration applications and evidence,[99] and use to identify individuals, excluding travel document checks.[100] Leaving the competences of the Member States regarding national security untouched,[101] the AIA however does not apply to systems employed for military, defence or national security purposes.[102] As the boundaries of 'national security' are highly contested, 'some Member States might be eager to expand the protective veil of national security upon other situations of public security or even border management'.[103]

Secondly, the regulation provides a sweeping temporal exclusion. Article 111(2) of the AIA stipulates that '[i]n any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by 2 August 2030'. Therefore, competent authorities in migration enjoy a substantial grace period before they become bound by the requirements for high-risk AI.[104] By the same token, Article 111(1) temporarily stipulates that 'AI systems which are components of the large-scale IT systems' in AFSJ (established by the legal acts listed in Annex X) that have been placed on the market before 2 August 2027 only need to be brought into compliance with the AIA by 31 December 2030. This includes by specific mention ETIAS, as well as virtually all the other databases in border control and immigration (such as the Schengen Information System (SIS), the Visa Information System (VIS) and Eurodac),[105] and grants the institutions and agencies until the end of 2030 to comply with any of the provisions of the AIA. This demonstrates in our view that the AIA itself assumes that ETIAS is likely to feature AI systems within the meaning of the AIA, as otherwise there would be no need to exclude it or make a temporal derogation.[106] Further, the delayed conformity with the AIA comprises a buffer period in which public authorities have vast leeway in terms of keeping AI deployment under wraps in the ways we have analysed above.[107]

As a matter of fact, migration and security actors enjoy a safe harbour that keeps AI implementation into ETIAS and other databases away from public scrutiny. What is striking is that the vast material and temporal exemptions in the AIA effectively sanction opaque practices involving both public and private actors in migration. However, even if the AIA were to apply to high-risk AI systems under Paragraph 7 of Annex III, it would only cover cases in which the use of AI for border control directly impacts a natural person.[108] By invoking the derogation in Article 6(3) of the AIA, competent authorities may in fact classify AI systems as non-high risk, thus sidestepping the Act's key accountability and transparency obligations under Chapter III. Conversely, a risk assessment AI tool 'used for strategic intelligence'[109] and orienting the general operations of the competent authorities in migration may fall outside the scope of high-risk AIs.

[98]Ibid., para 7(b).

[99]Ibid., para 7(c).

[100]Ibid., para 7(d).

[101]Art 4 TEU provides that national security remains the exclusive competence of the Member States.

[102]AIA, Art 2(3). Strikingly, the wording extends the scope of 'national security' in contradiction with the CJEU case law. See P Vogiatzoglou, 'The AI Act National Security Exception' (*Verfassungsblog*, 9 December 2024) <https://verfassungsblog.de/the-ai-act-national-security-exception/> accessed 14 April 2025.

[103]Vogiatzoglou (n 102).

[104]F Palmiotto, 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' [2025] European Journal of Risk Regulation 1, 20–1.

[105]Jones and Lanneau (n 27) ch 2.

[106]See too Derave et al (n 83) 382.

[107]See Paras 3.A and 3.B.

[108]Milaj and Bonnici (n 73) 7.

[109]Ibid. This holds true especially because the EU Parliament's proposal of including the forecasting of trends related to migration movements and border crossing did not make its way into the final legislative text.

Absent stringent requirements for non-high-risk AIs, authorities are effectively granted a licence to keep their design and implementation under wraps.

In the AI register, but behind a non-public wall

In line with all other high-risk AI systems, AI border and migration systems must be registered in a centralised and (in principle) publicly accessible database to be managed by the Commission.[110] According to the Commission, the registration in this database is supposed to 'increase public transparency, and oversight and strengthen ex-post supervision by competent authorities'.[111] However, Article 49 (4) AIA provides that: '[f]or high-risk AI systems referred to in points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration, asylum and border control management, the registration referred to in paragraphs 1, 2 and 3 of this Article shall be in a secure *non-public* section of the EU database referred to in Article 71 and shall include only the following information, as applicable (. . .)'.[112] This means that only the Commission and the EDPS as the designated supervisor for EU systems and agencies will have access to the registered details and will know of their existence. Once again, the logics of (deeper) secrecy inform this provision, reflecting 'the fears of Member States that revealing information could compromise national security'.[113] In a bid to increase transparency, the European Parliament proposal suggested to scrap the exception to register high-risk AI systems used in migration governance that the Commission originally proposed.[114] The exemption eventually made its way into the final text under pressure from the Council, as provisions furthering transparency were viewed as 'harmful to law enforcement and migration'.[115]

For the public and civil society seeking to use public access laws the use of high-risk AI systems in the areas of law enforcement, migration, asylum and border control will likely remain deep secrets, unless some leaking takes place or partial access is granted. Even if the institution or agency concerned pleads the public security exception, it is not excluded that the European Ombudsman, in particular after an own inspection of the documents in question, comes to a negotiated arrangement with the EU deployer to release at least some information publicly. But this all remains highly contingent. The European Ombudsman may indeed be more reluctant in the future to intervene where there is a specific exclusion in the AIA and the EDPS is the designated supervisor. The publication of the EDPS audits of the AI components of EU IT systems could also support transparency in this field, even if not directly (like access to documents would).

Ubiquitous secrecy: Article 78 AIA

Article 78 of the AIA is arguably very far reaching both in terms of what is covered as who is covered. It is one of the most important provisions in the legislation as it places market supervisory authorities and – quite broadly – 'any other natural or legal person involved in the application of this Regulation' under an absolute legal obligation to respect the confidentiality of information and data they obtain as they perform their duties (Article 78(1) AIA). This confidentiality requirement does not create formal limits to the information-gathering powers conferred on the market surveillance authorities ('MSAs'), and in fact it is provided elsewhere that they can have full access from providers.[116] Yet, it does prevent these supervisory authorities from

[110] AIA, Art 71.

[111] Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' (Communication) COM (2021) 206 final, 14.

[112] See also AIA, Art 71(4).

[113] Stewart (n 95) 131.

[114] Palmiotto (n 104) 14.

[115] Ibid., 21.

[116] AIA, Art 74(13)(a).

disclosing information about AI systems after it has been given to them. It is in fact a striking illustration of how political secrecy spreads beyond the executive or administration deploying the AI system to its supervision, and how in that context supervisors who are at a clear remove from the deployment must keep all the secrets, whether of public or private nature. This is admittedly not a novel idea, but simply parallels political secrecy rules that have previously been applied to accountability forums such as courts, parliaments and the European Ombudsman.[117] Article 78 moreover gives special protection explicitly to both public *and* private interests, such as national and public security[118] and intellectual property rights and trade secrets,[119] which often clash with the public interests promoted by transparency in AI systems and elsewhere.[120]

Article 78 instead reinforces the way that political secrecy is simply the subterranean narrative of the AIA that in practice dominates transparency, no matter how unpicked and reformulated. There are two main implications of this. For one thing, direct access to their documentation is only possible to staff members of the MSAs holding the appropriate level of security clearance. In fact, MSAs can be drawn from various sectors. If you have a consumer watchdog or a telecoms regulator there, they might struggle to develop the kind of internal structures they need to deal with information classification.[121] On the other hand, any mediated public disclosure of information by the MSA requires the user of the AI system, namely the public body deploying the system[122] to be consulted before disclosure is agreed. So, providers and certain types of users (and particularly public sector users of high-risk AI systems for law enforcement and asylum, migration, and border control management) can effectively maintain secrecy.[123]

The public(s)' limited agency to counter political secrecy in the AIA

Under the AIA, individuals and organisations are provided with limited countervailing rights to resist secrecy. On the one hand, natural and legal persons have a right to lodge a complaint with market surveillance authorities if the AIA has been infringed.[124] In migration governance, the limited application of high-risk AI requirements to AI systems used in the migration makes it all too easy to bypass this provision.[125]

Relatedly and more restrictively, affected persons enjoy a right to explanation of the individual decision-making 'taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III'.[126] The regulation nevertheless only applies to affected persons 'that are located in the Union'.[127] Consequently, third country nationals and other individuals that are not in the EU territory are barred from exercising the right to explanation.[128] Moreover, it is not clear how civil society organisations and pressure groups can gain access to the relevant information by raising this point.[129] In light of the non-public section of the AI register, it is hard to see how

[117]See earlier D Curtin, 'Second Order Secrecy and Europe's Legality Mosaics' 41 (2018) West European Politics 846.
[118]AIA, Art 78(1)(c).
[119]AIA, Art 78(1)(a).
[120]See too M Busuioc et al, 'Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act' 2 (2023) European Law Open 79. See further Para 4.A.
[121]We thank Marco Almada for bringing our attention to this point.
[122]AIA, Art 78(2), which also establishes the need to consult the originating national competent authority, that is, the authority that obtained information from the user.
[123]See further Busuioc et al (n 120).
[124]AIA, Art 85.
[125]See Para 3.C 'Public privilege through material and temporal exclusion'.
[126]AIA, Art 86(1).
[127]AIA, Art 2(1)(g).
[128]Jones and Lanneau (n 27) s 2.
[129]Stewart (n 95) 134–5.

NGOs, watchdogs and so forth can seek public access under the Access Regulation, or even file an adequate complaint if there is in effect no information.

4. Private secrecy

AI procurement in migration governance, we have seen above, gets private actors involved in developing AI systems deployed by migration and security authorities. The crux of the problem is that vendors can leverage harbours of private secrecy to prevent disclosure of AI systems, absent mandates in public contracts to do so.[130] Private secrets are, in essence, forms of shallow secrecy.[131] What is not known is not the existence or the use of the (procured) AI system *per se*, but the content and the workings of such AI system. A claimant, in fact, needs to be aware of the existence of an AI system being used by authorities to raise private secrecy. The public body has then acknowledged it some way or another and therefore resorts to the vendor to open up information on the AI system (eg, training datasets, algorithms, information about its workings and functioning, and so forth). Interestingly, the vendor may in principle assert secrecy claims even against the deploying public body and is therefore able to exert effective control over the deployed AI system. Thus, not only are NGOs, affected persons (such as third country national) and researchers impacted by private secrecy, but potentially migration agencies and other public bodies as well. That said, contractual practice regarding AI technology migration governance seems to put contracting authorities in the position of controlling the AI-related data and information.

Industry players in migration governance carve out secrecy in a variety of ways. The two primary tools are trade secrecy and contractual measures. The former provides legally safeguarded exclusivity that in principle enables providers to eschew public scrutiny over AI systems (Paragraph 4.A).[132] Even where trade secret claims cannot stretch, contractors and public buyers can rely on contractual arrangements erecting factual secrecy (Paragraph 4.B). Persons affected by AI systems as well as watchdogs and NGOs are instead denied access to AI-related information (Paragraphs 4.C and 4.D).

A. EU trade secrecy law shields AI systems from public authorities' oversight

More than questions as to its proprietary nature, the crux of trade secrecy protection[133] in the AI realm is that firms can leverage its flexibility to shield AI systems from access requests by public authorities.

[130]On private secrecy in AI procurement, see Hickok (n 12) 1220; A Sanchez-Graells, *Digital Technologies and Public Procurement: Gatekeeping and Experimentation in Digital Public Governance* (Oxford University Press 2024) 35. See also I Gallego Córcoles, 'Trustworthy Artificial Intelligence and Public Procurement' in E Gill-Pedro and A Moberg (eds), *YSEC Yearbook of Socio-Economic Constitutions 2023* (Springer 2023) Sec 1., stating that '[t]here are a number of challenges linked to the public procurement of artificial intelligence: [. . .] (d) intellectual property rights and trade secrecy and their relation to the transparency of algorithms'.

[131]In fact, private companies are keen on advertising products and services they develop as AI-enabled, whatever role AI artefacts or components ultimately play. In the hope of striking a deal with public counterparts and capitalise on AI, the promises of more efficient migration management prompt industry players to organise promotional campaigns around the idea of effective AI usage and implementation for border control and migration governance. See for example the presentations by industry players at Frontex's Industry Days (<https://www.frontex.europa.eu/innovation/announcements/general-industry-days-all-innovation-for-borders-is-welcome-TnvSOi> accessed 27 December 2025). See further Para 5.2.

[132]For an analysis of the US framework, see A Kapczynski, 'The Public History of Trade Secrets' 55 (2022) UC Davis Law Review 1367.

[133]On trade secret protection in the EU, see generally J Schovsbo, 'The Directive on Trade Secrets and Its Background' in J Schovsbo et al (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar 2020); Jens Schovsbo et al, 'An Appraisal of the EU Directive on Trade Secrets' in J Schovsbo et al (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar 2020).

For one thing, the protection requirements[134] are broad enough to cover the vast majority of informational assets and components of AI systems, such as algorithms, data, but also potentially crucial technical documentation.[135] Trade secrecy revolves around the concept of information. The Trade Secret Directive provides three prerequisites for an 'information' to access protection: its secrecy, its commercial value due to its secrecy, and its being subject to reasonable steps to keep the information secret.[136] Among them, it has been observed that information coming from publicly accessible sources or collected 'in plain sight' does not meet the secrecy requirement.[137] The Court of Justice of the EU seems to have endorsed this view in *Pari Pharma*, a case concerning pharmaceuticals.[138] In this case, the EMA requested access to documentation illustrating the clinical results of a novel drug for curing respiratory diseases. This documentation formed part of reports drawn up by the Committee for Medicinal Products for Human Use ('CHMP'). Here, Pari Pharma, the applicant, claimed that 'information contained in the CHMP reports (namely raw data generated on its behalf or the compilation and analysis of publicly-accessible data) constitutes a trade secret',[139] and therefore should not be disclosed. The court found that information in the CHMP reports does not meet the 'secrecy' requirement, since these are mostly made up of information that is assembled in compliance with specific 'regulatory requirements' and is directed 'by the EMA's precise questions'.[140] Moreover, the information, specifically relating to a niche subject matter and 'coming from bodies and associations well known to pharmaceutical undertakings, could be obtained without difficulty and without any particular inventiveness'.[141] Therefore, a more nuanced understanding of the correct qualification can be drawn 'between the publicly-accessible information and that which falls within the scope of the market survey and the applicant's own conclusions'.[142] Public accessibility of information is the strongest element of resistance to recognising secrecy in unprocessed data observed from reality. Datasets used to train AI systems made up of easily accessible information available to the public (such as data scraped from social media by Frontex)[143] would thus not enjoy trade secret protection. The same arguably holds true for when public authorities procure AI systems from private providers furnishing them with detailed instructions on what data needs to be injected into the system. However, algorithms and model architecture may well be trade secrets, as well as the source code and the technical documentation used for model development.

Secondly and more importantly, trade secrecy operates upon assertion of its holder.[144] No public or regulatory authority is involved in the initial allocation of trade secret status in information. (Putative) trade secret holders are thus prompted to (over)claim protection even if the legal prerequisites are plainly not fulfilled at inception.[145] So, what makes trade secrecy a

[134]Trade Secret Directive, Art 2(1).

[135]See more specifically Sandeen and Aplin (n 16); T Fia, 'Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data' (2022) 53 IIC – International Review of Intellectual Property and Competition Law 917; Mylly (n 16).

[136]Trade Secret Directive, Art 2(1).

[137]L Determann, 'No One Owns Data' 70 (2018) Hastings Law Review 1, 16; J Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' 8 (2017) Journal of Intellectual Property, Information Technology and E-Commerce Law 257, 269; Sandeen and Aplin (n 16) 453.

[138]Case T–235/15 *Pari Pharma GmbH v European Medicines Agency* [2018] EU:T:2018:65, para 113.

[139]*Pari Pharma*, para 104.

[140]Ibid, para 113.

[141]Ibid.

[142]Ibid.

[143]See Para 3.B.

[144]See Para 4.A.

[145]J Drexl et al, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Max Planck Institute for Innovation & Competition Research Paper No. 22-05 101; T Aplin, 'The Data Act and Trade Secrets: An Experiment in Compulsory Licensing' in Andreas Sattler and Herbert Zech (eds), The Data Act: First Assessments (Digital Recht 2024) 90–91; U-M Mylly, 'Trade

highly malleable tool is the wide leeway firms (including AI vendors in migration governance) are afforded to invoke the protection over informational assets in the first place. In a sense, it radically departs from the logic of state-made concession which characterises other IP standards, such as patents. It more closely resembles self-coronation: a corporate conglomerate confers it upon itself. The idea of a laissez-faire prerogative embedded in a private liberty sphere informs it.[146] Trade secret holders are entitled to carry the initial self-allocation without fearing public oversight. (Alleged) trade secret protection starts out as a *de facto*, self-enforced act of assertion over information (whether in the form of algorithms or data) that reflects the logic of possession in private law.[147]

Of course, corporate (over-)claiming does not necessarily amount to legal protection sanctioned by trade secret law. A court or a regulatory authority can always redefine the ambit of protection when asked to do so in a misappropriation case.[148] In fact, the Court of Justice has determined the boundaries of protection in the case *Dun & Bradstreet Austria*,[149] which concerned the balancing of trade secrecy against the right to access information on automated decision making under Article 15(1)(h) GDPR.[150] However, what matters is the sort of 'first mover advantage' that a firm can secure by asserting trade secrecy over AI systems to prevent access to begin with. When developing an AI system, firms put in place reasonable measures to implement secrecy inside and outside the organisation.[151] These bestow secret status on the results of their practices to prevent misappropriation and diffusion of the informational apparatus of AI systems.[152] At worst, a public agency or a judicial authority re-determines the correct purview of trade secrecy after the fact, when they have the opportunity to do so, and with the possibility of the AI system being deactivated or replaced in the meantime. Even though the CJEU case law concerning pharmaceuticals and access to documents[153] and more recently on credit scoring[154] by regulators opposes the practice of claiming broadly, the trend persists and may well stretch to migration governance. For example, contractors may well claim trade secrecy over informational assets that are not specifically addressed within the contractual arrangement with the public counterparty.[155]

Yet, trade secrecy is not unlimited. Some scope restrictions and exceptions to it move in the direction of countering trade secret claims over AI systems. Article 1(2)(b) and (c) of the Trade Secret Directive respectively provide that the directive does not affect the disclosure obligations for the public interest and for the exercise of supervisory powers by European and domestic public authorities. These provisions enable public bodies to request access to documents and the disclosure of information for transparency in administrative proceedings.[156] Yet, the unclear

Secrets and the Data Act' 55 (2024) IIC – International Review of Intellectual Property and Competition Law 368, 6; Villasenor (n 39).

[146]See, similarly, Kapczynski (n 132).

[147]H Zech, 'Data As a Tradeable Commodity' in Alberto De Franceschi (ed), European Contract Law and the Digital Single Market: The Implications of the Digital Revolution (Intersentia 2016) 63. On public authorities overseeing ex post in trade secrecy allocation in the context of the Data Act, see Aplin (n 145) 101.

[148]Villasenor (n 39) 512.

[149]Case C-203/22 *CK v Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien* [2025] EU:C:2025:117.

[150]See Para 4.D.

[151]T Aplin et al, 'The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis' 54 (2023) IIC – International Review of Intellectual Property and Competition Law 826, 845. See Para 4.1 above.

[152]Firms are in practice apt to claim trade secrets broadly, in line with an established trend in environmental information sharing for public interest purposes. See ML Lyndon, 'Trade Secrets and Information Access in Environmental Law' in RC Dreyfuss and KJ Strandburg (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research* (Edward Elgar 2011) 458ff.

[153]*Pari Pharma*, para 108.

[154]*Dun & Bradstreet Austria*.

[155]See Para 4.B.

[156]T Aplin, 'The Limits of EU Trade Secret Protection' in S K Sandeen et al (eds), *Research Handbook on Information Law and Governance* (Edward Elgar 2021) 186.

confines of the 'public interest' do not talk much about when this prevails over private interests.[157] This would typically include information covered by the Access Regulation and environmental information.[158] On paper, the broad formulation of Article 1(2)(b) and (c) serves as the ideal basis for national data protection authorities to request disclosure of trade secrets,[159] as well as for the competent authorities within the AIA.[160] However, its missing operationalisation affects its practical salience in other fields, such as migration governance and security more broadly.

Article 5(d) provides an exception to trade secrecy for disclosures 'for the purpose of protecting a legitimate interest recognised by Union or national law'. The perimeter of such exception is contested.[161] It is not clear what qualifies as a 'legitimate interest',[162] and therefore how to balance it against trade secrecy. The notion of legitimate interest may well include the transparency obligations that the AIA stipulates.[163] Ultimately, Article 5(d) holds the potential for tackling private secrecy, but its ultimate role is contested as it has yet to be seen in action.

B. Building secrecy in procurement contracts on migration AI technology

Firms are inclined to utilise contractual measures (such as confidentiality or non-disclosure agreements) to protect confidentiality of information that they hold.[164] Interestingly, the role of contracts in erecting factual exclusivity is even more salient in the eyes of companies. Empirical evidence flips the frequently presumed order of importance between the two protection forms. Trade secrecy is often considered as an 'additional safety net' on top of contractual measures to avoid data and information misappropriation.[165] Hence the extensive practice (frequently informed by skilful lawyers and spanning manifold industries)[166] of relying upon contractual arrangements to prop up factual secrecy in data and algorithms.

In contracts, parties are furnished with extensive leeway to regulate their own affairs. One may submit that the trade-off for such extensive flexibility is that only parties to such contracts are legally bound by its clauses. AI providers, in fact, cannot seek relief against infringing or misappropriating third parties as per the Trade Secret Directive.[167] However, this does not mean that contractual arrangements to keep factual secrecy are ineffective in practice. For one thing, claiming secrecy broadly through contracts has become the 'preferred approach' to keep AI systems away from the public, or even to employees.[168] On the other hand, if the trade secrecy regime does not apply, the related exceptions and limitations to trade secrecy (including those for the public interest) are not applicable either.[169] This ends up reinforcing the private interests and needs *vis-à-vis* public accessibility.

[157]Foss-Solbrekk (n 17) 5.

[158]See also Trade Secret Directive, recitals 11 and 21.

[159]K Foss-Solbrekk and A Kristin Glenster, 'The Intersection of Data Protection Rights and Trade Secret Privileges in "Algorithmic Transparency"' in Eleni Kosta et al (eds), Research Handbook on EU Data Protection Law (Edward Elgar 2022) 181–2.

[160]Mylly (n 16) 1035.

[161]See J Schovsbo, 'The Directive on Trade Secrets and Its Background' in Jens Schovsbo et al (eds), *The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive* (Edward Elgar 2020) 18; Aplin (n 156) 188.

[162]Fia (n 135) 942.

[163]Mylly (n 16) 1035.

[164]A Radauer et al, *Study on the Legal Protection of Trade Secrets in the Context of the Data Economy* (Publications Office of the European Union 2022) 58–60 <https://data.europa.eu/doi/10.2826/021443> accessed 14 March 2024. See also Sandeen and Aplin (n 16); Aplin et al (n 151); Mylly (n 16); Marco Ricolfi, 'Dealing with de Facto Powers in an Algorithmic Environment' in Florent Thouvenin et al (eds), *Kreation Innovation Märkte – Creation Innovation Markets: Festschrift Reto M. Hilty* (Springer 2024).

[165]Radauer et al (n 164) 67–9.

[166]Sandeen and Aplin (n 16) 459.

[167]Ibid; Aplin et al (n 151) 848.

[168]Sandeen and Aplin (n 16) 459.

[169]Ibid; Aplin et al (n 151) 849.

Factual secrecy features prominently in AI procurement networks in migration governance. The preceding section has cautioned against the fact that firms can leverage trade secrecy overclaiming to eschew oversight from public authorities. There are reasons to be a bit more optimistic in this respect if one looks at contractual practice in EU migration governance. The agreements between contracting authorities and contractors concerning AI migration technology raise a high bar of confidentiality that binds both parties. For example, the framework service contracts on the use of drones by Frontex,[170] on the provision of services for business content development related to the data management and analytics software used by Frontex[171] and on the implementation and maintenance of the biometric systems by eu-LISA[172] all feature a confidentiality clause that concerns 'any information or documents, in any format, disclosed in writing or orally, relating to the implementation of the FWC and identified in writing as confidential'. The former also puts Frontex in control of the data processed by drones,[173] and bars the contractor from processing any data using its systems unless Frontex approved the technical design of the solution.[174] Moreover, the contractor must sign a non-disclosure agreement of information,[175] which binds all its duly authorised personnel.

Not only does confidentiality characterise public contracts, but it also captures the entire procurement procedure. Contractors enjoy a secrecy harbour based on the concept of 'business secrets', which partially overlaps with trade secrecy and antedates 'trade secrecy' in the EU *acquis* (the Trade Secret Directive).[176] Business secrets are a plethora of confidential information that firms may (be required to) provide to public administrations. Article 41(2)(b) of the CFREU associates them with the right of good administration.[177] Thus conceptualised, they form a corporate sphere of interest that public authorities are required to preserve while fulfilling tasks involving access to privately held information. A secondary law incarnation in migration governance is Regulation 2024/2509, which adapts procurement rules applicable to EU agencies and institutions to the general framework of the Public Procurement Directive. In particular, Annex I of Regulation 2024/2509 extends the confidentiality rules of the directive[178] to various phases of migration procurement.[179] Confidentiality covers information that is not necessarily a

[170] <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/acc779af-00e9-4487-a475-2578220559ab-CN?order=DESC&pageNumber=4&pageSize=10&sortBy=startDate&isExactMatch=true&cftPartyLegalEntityId=47352434> accessed 27 December 2025 (see Annex III – 'Draft FWC service contract').

[171] Ibid (see Annex III – 'Draft contract').

[172] <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/4802?order=DESC&pageNumber=4&pageSize=10&sortBy=startDate&isExactMatch=true&cftPartyLegalEntityId=47352456> accessed 27 December 2025 (see Annex III – 'Draft framework contract').

[173] '[ToR-120] Frontex is the owner and Controller of all data, including all the video records, images, metadata and logs captured by the aircraft during the flights as well of the resulting product after any alteration required necessary for data integration or any other product resulting of necessary data manipulation. [. . .] [ToR-122] The Contractor shall not keep any other copy of the data apart from the one recorded by the aircraft ' (<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/acc779af-00e9-4487-a475-2578220559ab-CN?order=DESC&pageNumber=4&pageSize=10&sortBy=startDate&isExactMatch=true&cftPartyLegalEntityId=47352434> accessed 27 December 2025, see Annex II – Terms of Reference, clause 12.2).

[174] Ibid., clause 12.7.

[175] Ibid., clause 12.1.

[176] See the thorough analysis in Commission, 'Commission Staff Working Document – Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' SWD (2013) 471 final, 107ff.

[177] Emphasis added.

[178] See in particular Public Procurement Directive, Arts 21, 50(4) and 55(3).

[179] Regulation (EU, Euratom) 2024/2509, annex I, para 7(3)(2), 10(2)(29) and 25(1)(2)–(3). See also Regulation (EU, Euratom) 2024/2509, Art 173(3), which also contemplates information withholding if its release 'prejudice the legitimate commercial interests of economic operators or might distort fair competition between them'.

trade secret,[180] but is considered confidential upon the unilateral decision of the firm.[181] In the *Antea Polska* judgement, the CJEU has espoused a broad interpretation of confidential information in procurement. Confidentiality rules in procurement do not only cover trade secrets, but also other business-related information whose disclosure might thwart competition and the mutual trust between tenderers and the contracting authority.[182] It goes without saying that information qualifying as a business secret has the potential to encompass various components of AI systems (data, algorithms) provided by vendors in procurement and deployed by migration and security authorities. The relevant case law has in fact espoused quite an expansive approach. The CJEU has embraced the following definition: 'information of which not only disclosure to the public but also mere transmission to a person other than the one that provided the information may seriously harm the latter's interest'.[183] The Court has also emphasised the three conditions to be met: (a) the information should only be restricted to a limited group of individuals; (b) its revelation could seriously harm either its provider or third parties; and (c) the interests that could suffer from its disclosure must be objectively worthy of protection.[184]

C. Commercial interests, public detriments

At this juncture, one may well wonder if affected persons, civil society groups and NGOs can rely on transparency points *vis-à-vis* private secrecy. The most evident one is the Access Regulation, which informs citizens' access to documents held by public bodies. In materialising Article 42 CFREU and Article 15 TFEU, Article 2 of the Access Regulation establishes a citizens' right of access to documents held by EU institutions,[185] and a corresponding obligation for the latter to grant access to such documents.[186] On paper, this provides the basis for access by private citizens to algorithmic systems employed by public authorities on public interest grounds. The notion of 'document',[187] in fact, is broad enough to encompass AI systems (more specifically, AI algorithms).[188]

Yet, citizens' or researchers' demands can be frustrated if the imperatives of private secrecy end up prevailing as much as political secrecy.[189] Article 4(2) of the Access Regulation restricts access to public documents if the disclosure undermines the 'commercial interests of a natural or legal person, including intellectual property'. However, the exception can be resisted in case of 'an overriding public interest in disclosure' (the 'counter-exception'). The case law on Article 4(2) has cast light on how the access rule under Article 2(1) and the corresponding exception and counter-exception function.

The CJEU has limited the potential for an overly sweeping scope of private interests. Since the latter form exceptions to the 'widest possible' access to public documents, they must be interpreted strictly.[190] Courts must carry out a balancing test between opposing public and private interests,[191] and the interest prevailing in the practice of the case determines whether the document is to be

[180] A Sanchez-Graells, 'Art 21: Confidentiality' in Roberto Caranta and Albert Sanchez-Graells (eds), *European Public Procurement: Commentary on Directive 2014/24/EU* (Edward Elgar 2021) 230.

[181] Ibid., 229.

[182] Case C-54/21 *Antea Polska S.A., 'Pectore-Eco" sp. z o.o., Instytut Ochrony Środowiska – Państwowy Instytut Badawczy v Państwowe Gospodarstwo Wodne Wody Polski* [2022] EU:C:2022:888, paras 54 and 63.

[183] Case T-353/94 *Postbank v Commission* [1996] ECR II-921, para 87.

[184] Case T-198/03 *Bank Austria Creditanstalt v Commission* [2006] ECR II-1429, para 71.

[185] Access Regulation, Art 2(1).

[186] Access Regulation, Art 2(2).

[187] Access Regulation, Art 3(a).

[188] Foss-Solbrekk (n 17) 5.

[189] See Paragraphs 3.A and 3.B above.

[190] Case C–350/12 P *Council of the European Union v Sophie in 't Veld* [2014] EU:C:2014:2039, para 48.

[191] Mylly (n 16) 1038.

disclosed.[192] Moreover, the recipient of the access request has the burden of explaining (even by means of general presumptions applying to several categories of documents, as seen above) the extent to which access to documents would jeopardise the (commercial) interest protected by the exception relied on.[193] More fundamentally, they must prove that the risk of compromising such interest is reasonably foreseeable and not merely hypothetical.[194] The individual invoking the overriding public interest must conversely prove that the latter gains more salience given the specific circumstances of the case.[195]

As 'commercial interests' are not defined anywhere in the legislation nor in the CJEU's judgements,[196] this concept has the potential to conjure a larger pool of private entitlements and interests than just trade secrecy. The notion of 'commercial interests' seems to align with that of 'business secrets' that we have encountered in the previous paragraph. This does not mean nonetheless that the corporate inclinations to (over-)claim trade secrecy or use contractual measures are to be blindly ratified in all instances. For their part, however, some EU agencies (such as the European Medicines Agency, 'EMA') have proven to be quite permissive in letting firms define themselves the ambit of documental access,[197] even though applying confidentiality presumptions to prevent access to commercially valuable information 'is always optional for the EU institution, body, office or agency to which such a request is addressed'.[198] By the same token, firms need to 'specifically and precisely' single out what information, once disclosed, would effectively undermine the commercial interests.[199] Information should thus be treated as confidential if the business priorities are tangible enough to call for secrecy.[200]

The Court of Justice has also taken on various approaches to construe the 'overriding public interest'. *Turco* has in fundamental terms opened the way to a broad understanding of the public interest as a product of 'increased openness'.[201] Later, the Court has raised the bar for assessing how the individual can demonstrate the overriding public interest in disclosure. *LPN* stressed that the need for transparency that is invoked must be 'pressing'.[202] The CJEU has recently provided further guidance on the 'overriding public interest' in data-driven applications. Although it has endorsed quite an extensive interpretation of the notion of 'overriding public interest' in *Bayer CropScience*,[203] it has later adopted a more restrictive perspective in the *Breyer* judgement. The decision concerns access to an AI system that detects lies in the context of border control. For the court, the applicant claimed too broad an overriding public interest to be relevant.[204] The automated system was developed for the EU Horizon 2020-funded iBorderCtrl pilot project, which employs AI lie-detector technology for automated border control security. The activist and politician Patrick Breyer requested access to the documentation of the Horizon project to the

[192]Joined Cases C-514/11 P and C-605/11 P *LPN and Finland v Commission* [2013] EU:C:2013:738, para 40.

[193]Case C-477/10 P *Commission v Agrofert Holding* [2012] EU:C:2012:394, para 57; Case C-404/10 P *Commission v Éditions Odile Jacob* [2012] EU:C:2012:393, para 116; Case C-280/11 P *Council v Access Info Europe* [2013] EU:C:2013:671, para 72; Case C-365/12 P *Commission v EnBW Energie Baden-Württemberg* [2014] EU:C:2014:112, para 64 and 65; *Pari Pharma*, para 71; *PTC Therapeutics*, para 63.

[194]Case C-280/11 P *Council of the European Union v Access Info Europe* [2013] EU:C:2013:671, para 54.

[195]*LPN*, para 94.

[196]Foss-Solbrekk (n 17) 6.

[197]Mylly (n 16) 1036.

[198]Case C-175/18 P *PTC Therapeutics International Ltd v European Medicines Agency* [2020] EU:C:2020:23, para 62. See also para 82.

[199]*PTC Therapeutics*, paras 82–3.

[200]Mylly (n 16) 1038.

[201]Joined cases C-39/05 P and C-52/05 P *Kingdom of Sweden and Maurizio Turco v Council of the European Union* [2008] ECR I-04723, para 75.

[202]Case T-851/16 *Access Info Europe v European Commission* [2018] EU:T:2018:69, para 112.

[203]Case C-442/14 *Bayer CropScience SA-NV and Stichting De Bijenstichting v College voor de toelating van gewasbeschermingsmiddelen en biociden* [2016] EU:C:2016:890.

[204]Case C-135/22 P *Patrick Breyer v European Research Executive Agency* [2023] EU:C:2023:640.

European Research Executive Agency ('REA'). In early 2019, the REA granted access to some documentation related to the project, while denying access to other information. The refusal was based on the commercial interests' exception to the right of access to public documents under Article 4(2) of the Access Regulation. On appeal the CJEU found that the applicant's reliance on a general ground of public interest to access documents developed for an EU-funded research project 'is not sufficient to establish that that interest must necessarily prevail over the reasons justifying the refusal to disclose those documents'.[205] Therefore, although an applicant may well rely on such grounds, these need to be aptly confined to proving their concrete relevance to the case. Moreover, the court clarified that, while the legal framework on the dissemination of research outcomes from Horizon 2020 Projects[206] ensures a high level of protection for fundamental rights, it does not imply that these rights have not been violated, and that there is no overriding public interest in disclosing the documents.[207] In the specific case, the fact that the iBorderCtrl project was 'merely a research project under development, the sole purpose of which was to test technologies'[208] has tipped the scales against mandating broader opening of the technical documentation about the algorithmic system. The court might well have pursued a different course had the implementation setting been less experimental.

Yet, the restrictive approach that the Court of Justice adopted in *Breyer* runs the risk of leaving crucial AI-related technical information about the algorithmic system out of scope. More specifically, information about its technical configuration, such as its design, its accuracy (including false positives/negatives), its potential for discrimination and the steps taken to address these risks, have all been kept under wraps.[209] Taken together with *LPN*, the message that the Court hammers home is that applicants need to go to great lengths to demonstrate that transparency reasons are 'pressing'. But this probably means that the bar really is set too high for applicants to access some informational components of AI systems.

D. Recouping transparency or paying lip service to it? Back to the GDPR and the AIA

In several recent cases involving algorithmic decision making, the CJEU has balanced trade secrecy against the right to obtain an explanation on automated decisions under Article 15(1)(h) GDPR, read in conjunction with Article 22 GDPR.[210] The result is that applicants may find their access requests granted when shallow secrets held by private contractors are involved. For example, in *SCHUFA*,[211] the court found that a credit agency which provides credit scoring reports to other parties (such as credit institutions and banks) must put data subjects in the position of accessing the 'specific information'[212] on the existence of automated decision-making, on the logic involved and the significance and consequences of the data processing for the data subject.[213] In fact, the agency SCHUFA had refused to provide detailed information on the various components

[205] *Breyer*, para 77.

[206] Regulation (EU) 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020)' and repealing Regulation (EC) No 1906/2006, OJ L 347/81.

[207] *Breyer*, para 105.

[208] *Breyer*, para 110.

[209] Foss-Solbrekk (n 17) 8.

[210] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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 (General Data Protection Regulation), OJ L 119/1 (GDPR). On the functions and rationales underpinning Article 22 GDPR and how the provision applies to fully automated decisions in migration control (in particular to the context of ETIAS and VIS), see F Palmiotto, 'When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis' 25 (2024) German Law Journal 210, 213ff.

[211] Case C-634/21 *OQ v Land Hessen* [2023] EU:C:2023:957. For a commentary, see Ibid., 215.

[212] *SCHUFA*, para 63.

[213] GDPR, Art 15(1)(h).

utilised to calculate the score based on (alleged) trade secret protection.[214] In his Opinion, AG Pikamäe stressed that trade secrecy 'cannot under any circumstances justify an absolute refusal to provide information, a fortiori where there are appropriate means of communication which aid understanding while guaranteeing a degree of confidentiality'.[215] Moreover, even though Article 15(1)(h) GDPR 'exclude[s] any obligation to disclose the algorithm, given its complexity',[216]

> the obligation to provide 'meaningful information about the *logic involved*' must be understood to include sufficiently detailed explanations of the method used to calculate the score and the reasons for a certain result. In general, the controller should provide the data subject with general information, notably on factors taken into account for the decision-making process and on their respective weight on an aggregate level, which is also useful for him or her to challenge any 'decision' within the meaning of Article 22(1) of the GDPR.[217]

The CJEU has more recently confirmed its view in *Dun & Bradstreet Austria*.[218] In particular, controllers are mandated to provide supervisory authorities or courts with information 'allegedly protected' by trade secrecy, in order for the latter to assess the extent of the information to be disclosed under Article 15(1)(h) GDPR.[219] This puts public authorities back in control in deciding the boundaries of trade secret protection, limiting the possibility for contractors to (over-)claim. Affected individuals (as long as they qualify as data subjects) may thus obtain meaningful information on the logic of the AI systems involved. According to the data processing agreements and clauses attached to the contracts reviewed for present purposes, contracting authorities usually act as controllers, whereas the contractors act as processors under data protection law.[220] Therefore, applicants would need to submit data access request to the contracting authorities, which will then rely upon the contractors to obtain the relevant information (unless they are able to fulfil them on their own). Having said that, legal persons such as NGOs and pressure groups are left out, since they would not qualify as data subjects.

One may wonder whether the transparency obligations under the AIA may help legal persons access secret AI-related data and information held or controlled by a contractor. The AIA imposes transparency requirements on high-risk AI providers that might well open up public access to informational components of AI systems. The providers[221] in this context would be the contractors. Under the AIA, they are primarily responsible for specifying the technical properties of a given AI system.[222] In light of its concise definition provided in recital 27,[223] transparency is understood as in relation primarily to the deployer (which would typically be the migration agency),[224] who can then instil systems of traceability and possess enough information to

[214] *SCHUFA*, para 16.

[215] Case C-634/21 *OQ v Land Hessen* [2023] EU:C:2023:957, Opinion of AG Pikamäe, para 56.

[216] Ibid., para 57.

[217] Ibid., para 58.

[218] See Para 4.A.

[219] *Dun & Bradstreet Austria*, para 76.

[220] <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/docs/805d2211-bb20-406e-966b-d4ba24e0fca0-CN/Annex%20III-%20Draft%20FWC_V1.pdf; https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/acc779af-00e9-4487-a475-2578220559ab-CN?order=DESC&pageNumber=4&pageSize=10&sortBy=startDate&isExactMatch=true&cftPartyLegalEntityId=47352434> accessed 27 December 2025; <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/docs/etender/8422/8422_104876_EN-Annex%20III%20-%20FWC%20service%20contract_498_ENG_V1.pdf> accessed 27 December 2025.

[221] AIA, Art 3(3).

[222] See AIA, recitals 64, 71, and 72. See also Arts 53 and 55.

[223] 'Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights'.

[224] AIA, Art 3(4).

communicate explanations. Yet, the relevant requirements are underspecified in terms of detail, and it seems that the deployer will just have to install whatever systems of traceability they can based on the information they are given. Moreover, what 'enough information' is or will be to enable deployers to 'communicate explanations' remains an open question. It must in any event be enough to support 'informed decision making by them'. Providers are urged to communicate information to deployers 'in a clear and easily understandable way, free of misunderstandings or misleading statement'.[225] The very wording used to break the principle of transparency into operative, effective rules, however, implies that very different approaches may be taken by the provider in giving effect to it.

The rationale behind recital 27 radiates out through the transparency obligations of the AIA. Under Article 13(1), any high-risk AI system must be transparent enough to allow deployers to interpret its outputs and use them 'appropriately'. The implication is that transparency has to be ensured throughout the design and development of the AI system. How this is to be done is yet another open question, although necessarily implying that providers are required to adopt technical approaches and measures of one kind or another that can foster the requisite level of transparency to the provider.[226] Similarly, Article 13(2) AIA requires that any high-risk AI system be accompanied by instructions to deployers. Yet, the caveats 'when appropriate' and 'where applicable' suggest that the provider is required to disclose rather little information to the deployer about the inner workings of the system.[227] The provider thus potentially retains full control over the information they release about the crucial technical aspects of the AI system.[228]

In sum, the transparency requirements under the AIA ends up favouring deploying competent authorities in migration. They effectively reinforce the secrecy practices mandated by procurement contracts, which put public authorities in control of the informational components of AI technology.[229] However, actors other than the deployer, such as affected persons, NGOs and watchdogs, are left out of the picture.

5. Public transparency and accountability under challenge from AI secrecy

A. (Re-)conceptualising AI secrecy: main takeaways from EU migration law and governance

For different reasons and motivations, both migration authorities and AI vendors leverage legal regimes of AI secrecy, which grant them broad leeway to keep the public (including citizens and researchers) in the dark, either about the very existence and operation of an AI system (deep secrecy) or about how it functions (shallow secrecy). In this guise, AI secrecy in migration governance dovetails nicely with what Deeks has recently described as the 'double black box': the exacerbation of already opaque government decision-making with even more layers of concealment due to the corporate-designed features of AI systems.

AI secrecy stretches well beyond the conventional notion of hiding information or algorithms, as it has been frequently framed in the literature. It begins much earlier: with the decision to keep its development under wraps. Embedded in law and migration practice, that deliberate choice alone can make it nearly impossible for large parts of the public (individuals, civil society) to even imagine that such systems exist or are being used. This has been referred to as deep AI secrecy. This kind of secrecy is engrained in the way migration authorities (do not) address public access requests,[230] and is further reinforced by the broad protections granted to commercial interests

[225]AIA, recital 74.

[226]For a discussion on 'explainable AI' and its limitations, see Busuioc et al (n 120).

[227]See Para 4.B

[228]On the absence of a clear-cut disclosure obligation in the AIA, see B Kuźniacki et al, 'Towards EXplainable Artificial Intelligence (XAI) in Tax Law: The Need for a Minimum Legal Standard' (2022) 14 World Tax Journal 573, s 4.1.2.

[229]See Para 4.B.

[230]See Paras 3.A and 3.B.

and confidentiality in procurement processes.[231] Frontex and eu-LISA exist in a largely public access-free zone, also after the entry into force of the AIA. For instance, the deployment of AI in ETIAS remains hidden, despite public indications and reports suggesting AI tools will be employed in the future.[232] By the same token, eu-LISA is able to keep details about the system's design, including the profiling algorithms, secret under the guise of public security concerns.[233]

Although there exists at least a suspicion that AI systems are being used, information about them is being withheld from public access applicants.[234] Even if the public becomes aware that AI is being used and implemented in migration governance, layers of shallow secrecy obscure any understanding of its functioning. Shallow AI secrets characterise the tendency of migration authorities not to disclose technical information on the systems they use. Private conglomerates from which migration governance technology is procured enjoy various protection harbours thwarting access to the utilised AI systems. These regimes of shallow secrecy prevent affected persons and NGOs access to AI-related information (datasets and algorithms) that vendors build, even if public authorities managing migration governance technology are in agreement with opening up access to such information. Trade secrets[235] put (putative) secret holders in the position of invoking protection broadly considering the legal prerequisites to access trade secrecy.[236] Exceptions and limitations to trade secrecy are nevertheless poorly equipped to enable access.[237] However, recent case law has sought to place the defining of trade secrecy boundaries back in the hands of public authorities.[238] What is more, there is the business secrecy haven that companies invoke in procurement processes.[239] Whereas contracting authorities retain control over AI systems in procurement by means of procurement clauses that build confidentiality,[240] affected persons and civil society are both equally side-lined in access requests as vendors can readily invoke the commercial interest exception under Article 4(2) of the Access Regulation, as occurred in *Breyer* with regard to an AI system for migration control.[241]

While the recent case law on the GDPR's right to access to AI explanation holds promise for increased transparency for data subjects,[242] the AIA barely makes a dent in the secrecy apparatus informing access to information about AI (and its actual operation, in the case of deeper forms of secrecy). For one thing, the way transparency is formulated in the AIA means that it is mediated by the (private) providers involved, and is consonant with communication rather than public access as such.[243] Even more fundamentally, the AIA enables implementing AI technology in the context of border control and migration databases (which affect largely very vulnerable groups of people) to continue to be developed and applied in the dark, without subjecting such high-risk systems to the AIA's governance apparatus for a long buffer period (until 2030).[244] Secrecy moreover permeates the entire regulation due to Article 78, which embeds confidentiality into nearly every aspect of governance under the regulation.[245] In sum, public sector deployers and

[231]See Paras 4.A–4.C.
[232]See Para 3.A.
[233]See Para 3.B.
[234]See Para 3.A.
[235]See Para 4.A.
[236]See Para 4.A.
[237]See Para 4.A.
[238]See Para 4.D.
[239]See Para 4.C.
[240]See Para 4.B.
[241]See Para 4.C.
[242]See Para 4.D.
[243]See Para 4.D.
[244]See Para 3.C 'Public privilege through material and temporal exclusion'.
[245]See Para 3.C 'Ubiquitous secrecy: Article 78 AIA'.

private vendors of high-risk AI systems for migration and border control management can effectively maintain secrecy in a seemingly infinite variety of ways.

B. Breaking free of AI secrecy: tackling the public-private secrecy interstices

Broadly speaking, the picture that the paper has depicted is quite grim. Yet, it is worth considering several countervailing strategies and frameworks that can offer more promising avenues for tackling secrecy. Looking into each and every avenue lies outside the scope of this paper. A natural first impulse might be to call for sweeping, consistent reforms of a relatively new legal and regulatory framework. In light of the comprehensive approach to AI secrecy which we consider, however, it is worth focusing on the very operations that allow both political and private secrecy practices and decisions to shape up and flourish in migration governance, impacting affected persons and civil society actors the most.

A striking illustration is the context in which migration authorities operate. The working and operational environment in which Frontex operates is prone to a high level of opacity. Frontex's working methods in the context of its Consultative Forum in which many NGO's participate have also come under scrutiny.[246] In this context too it seems Frontex manages the narrative and by dint of a very strict confidentiality clause which entails risks of criminal liability if sensitive or non-public information is shared with even membership organisations, the working methods laid down by Frontex do not encourage meaningful input. For this reason, some membership organisations such as PICUM (representing more than 160 NGO's) have withdrawn from participation in the Consultative Forum.[247] A new working document was later published online in 2024 which contains extensive rules on confidentiality and secrecy, outlined in the terms objected to by PICUM.[248] The Consultative Forum of Frontex struggles as a result to function as a direct link to civil society, given the far-reaching duty of confidentiality to which its members are bound.[249] This exemplifies the nested structures of secrecy and confidentiality, and how they spread beyond core government to also include supervisors and civil society. Dismantling the secrecy-infused environment of the Consultative Forum would empower civil society and pressure groups to gain a (better) understanding of Frontex's policies.

Another driver of secrecy at operational level is the context in which contracting authorities and vendors interact and decisions are formed. Frontex organises 'Industry Days', limited-entry events during which high-up public officials and top executives from contractors come together to discuss technological solutions. Attendance to these events is restricted to selected industry players, private providers and representatives of Member State authorities. Although Frontex Industry Days may not always be solely 'closed-door',[250] demanding registration to participate online[251] and carefully vetting participants might indicate restricted public permeability. Frontex has admittedly sought to increase it by releasing informative materials about the events[252] and keeping a transparency register dedicated to lobbying. In their words,

[246]See, in general, <https://www.frontex.europa.eu/fundamental-rights/consultative-forum/general/> accessed 27 December 2025.

[247]PICUM's input into the European Ombudsman's strategic inquiry on the role of the European Border and Coast Guard Agency in SAR operations is essential.

[248]Frontex Consultative Forum on Fundamental Rights Working Methods <https://www.frontex.europa.eu/assets/Partners/Consultative_Forum_files/Working_Methods_-_Frontex_Consultative_Forum_on_Fundamental_Rights.pdf> accessed 27 December 2025 (art 5).

[249]Gkliati and Kilpatrick (n 56) 68.

[250]<https://www.frontex.europa.eu/innovation/announcements/general-industry-days-all-innovation-for-borders-is-welcome-TnvSOi> accessed 27 December 2025.

[251]<https://www.frontex.europa.eu/innovation/announcements/industry-days-on-haps-high-altitude-platform-systems-for-border-surveillance-BOIwkW> accessed 27 December 2025.

[252]<https://www.frontex.europa.eu/innovation/announcements/general-industry-days-all-innovation-for-borders-is-welcome-TnvSOi> accessed 27 December 2025.

> [a]ll meetings and contacts of the Executive Director, Deputy Executive Directors and Heads of Divisions in matters concerning procurement procedures and tenders for services, equipment or outsourced projects and studies are registered in this tool.

However, the register does not display information on the content of the meetings. Injecting more public participation at the level of Industry Days has the potential to hold both private and public actors more accountable regarding the decisions made.

6. Conclusion

This paper has told a poignant story of how legal regimes, often originally intended for highly different technological contexts, impinge on access to, and transparency of today's AI technology in a very critical area of public governance such as migration control. Procured AI technology in this sensitive domain is based on pervasive regimes of secrecy that shield both the development and deployment of AI from public scrutiny. The double 'black box' that we have contributed to describing has revealed the intensity with which political secrecy is more generally being conjoined with private secrecy. Both public and private actors employ a certain amount of self-serving reasoning, and there is often little recourse for supervisory authorities to overturn these tendencies, given the specific derogations in existing legal regimes adapted in a different era.

This public–private double black box raises concerns not only about transparency and accountability in migration governance, but also about the much broader implications of private corporations holding influential roles in areas traditionally governed within the public sphere. This mirrors the recent developments concerning large chunks of US security infrastructure being controlled and managed by private actors and new moves at the European level to instigate far-reaching and novel forms of defence and security cooperation, seemingly with private actors and procurement processes at its core.[253] The time is ripe for a new conversation that moves beyond the status quo of allowing secrecy to dominate as if it were consonant with the public interest and the private interest, simply because aged legal regimes say so. Reclaiming the necessity for secrecy as well as for its limits will instead focus on ways to dominate secrecy itself in the wider public interest and for more ambient forms of accountability. Our aim is not to disallow real and adapted needs for AI secrecy, but to breathe new life and vigour into what more transparency can and should mean in our contemporary, ever-evolving democratic systems. As AI technology becomes more and more integrated, establishing meaningful countermeasures and practices that resist the secrecy inherent in private–public interactions becomes more critical than ever. One countervailing driver may be promoting AI literacy initiatives that would meaningfully (re-)equip the public(s) with the tools necessary to challenge opaque decisions and the prevailing narratives behind AI deployment.[254]

Acknowledgements. The authors gratefully acknowledge (in alphabetical order) Valerie Albus, Marco Almada, Maurizio Borghi, Mark Bovens, Evelien Brouwer, Gráinne de Búrca, Madalina Busuioc, Mateus Correia De Carvalho, Saverio Della Corte, Megan Donaldson, Michèle Finck, Martijn Hesselink, Margot Kaminski, Alexandra Karaiskou, Estela Maria Lopes, Albert Meijer, Lola Montero, Anna Morandini, Ludovica Paseri, Jennifer Raso, Marco Ricolfi, Ludivine Sarah Stewart and

[253]See, for example, European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'White Paper for European Defence – Readiness 2030' <–https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en?filename=White%20paper%20for%20European%20defence%20–%20Readiness%202030.pdf> accessed 24 April 2025.

[254]E Fernandes et al, 'Article 4: AI Literacy' in C Necati Pehlivan et al (eds), *The EU Artificial Intelligence (AI) Act: A Commentary* (Wolters Kluwer 2024) 86; T Fia, 'Article 4: AI Literacy', in G Malgieri et al, *The EU Artificial Intelligence Act: A Thematic Commentary* (Hart 2026) (forthcoming).

Thomas Streinz for their valuable comments and suggestions on earlier drafts of this paper. All remaining errors and omissions are the authors' sole responsibility. Tommaso Fia's research was carried out as part of the Machine Learning Cluster of Excellence, EXC number 2064/1 – Project number 390727645, funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation). The authors acknowledge support by the Open Access Publishing Fund of the University of Tübingen.

Competing interests. The authors have no conflicts of interest to declare.

Cite this article: D Curtin and T Fia, 'Cracking AI secrecy: (beyond) EU migration law and governance' (2026) *European Law Open* **5**, 305–334. https://doi.org/10.1017/elo.2025.10064