AI and interoperability

Book Chapter

Author(s):
Leese, Matthias

Publication date:
2024-06-21

Permanent link:
https://doi.org/10.3929/ethz-b-000703800

Originally published in:
https://doi.org/10.4337/9781803922171.00018

11. AI and interoperability

Matthias Leese

INTRODUCTION

Interoperability has been framed as a key challenge for contemporary forms of governance and public administration. Notably, apart from practical drivers in domains that require a high level of coordination between different actors, it is also seen as a cross-cutting requirement with regard to possible applications of machine learning and other forms artificial intelligence (AI) (Paul, 2022). In the European Union (EU), for example, interoperability is considered paramount in making knowledge infrastructures within a multi-level political architecture future-proof. The *New European Interoperability Framework (EIF)*, published by the European Commission (EC) in 2017 as a guideline for public administrations across the EU, calls to "avoid digital fragmentation" (European Commission, 2017b) and to link up information silos in order to achieve an optimal knowledge base for government–citizen interfaces and the single market. This strategy has more recently been followed up by a proposal for an *Interoperable Europe Act* that defines "measures for a high level of public sector interoperability across the Union" (European Commission, 2022). And while the political push for interoperability might currently be particularly strong in the EU, there is no shortage of interoperability projects in other part of the world (DeNardis, 2011), be it in North America (Vannijnatten, 2004; Dittmer, 2018), South America (Jimenez, Criado et al., 2011, Manda and Backhouse, 2016), Africa (Adebesin, Kotze et al., 2013, Gumbo and Moyo, 2020), or Australia (Sprivulis, Walker et al., 2007).

At times it does, however, remain vague what interoperability means in practice and how it relates to other concepts (Trauttmansdorff, 2022). The basic rationale of interoperability is as old as it is simple and intuitive. Its Latin origin translates to "to work between", indicating that it is concerned with the ways in which two or more different entities can function together and work towards a common goal. It thus speaks to fundamental questions of communication and coordination in complex environments that are characterized by specialization and division of labour. Literature from engineering, computer science, or management tends to break down interoperability into more specific layers, for example technical interoperability, syntactic interoperability, semantic interoperability, or organizational interoperability (Kubicek and Cimander, 2009; Roßnagel, Engelbach et al., 2012). Concrete interoperability challenges can then be addressed in research and practice with regard to concrete use cases. The *EIF*, for example, defines interoperability in public administration as "the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems" (European Commission, 2017b: 5). And the proposal for the *Interoperable Europe Act* frames it as "common rules and a framework for coordination [in the] public sector" (European Commission, 2022: 21).

As these examples illustrate, interoperability, while intuitively resonating with almost any form of public administration and governance, refuses to be defined easily and in a uniform way. As a high-level concept, it remains abstract enough for it to be an attractive political imaginary for regulation and practical improvement of cooperation structures that are considered to be insufficient. But at the same time, it needs to be substantiated in the context of concrete use cases. Only then can it be assessed in its meaning and implications, both in terms of the transformations that it brings to governance and public administration, but also in terms of its wider societal implications.

To do so, this chapter reconstructs how interoperability has been framed and is put into practice in the context of the European Area of Freedom, Security and Justice (AFSJ). In 2019, the EU adopted an interoperability framework for all major centralized databases that contain information regarding law enforcement, border control, and judicial cooperation (European Union, 2019a; European Union, 2019b: 28). This policy framework defines interoperability for EU internal security as the capacity to "facilitate the correct identification of persons" and "streamline access for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offenses" (European Union, 2019a). As will be argued, the case of AFSJ interoperability is illustrative of the politically perceived need to overhaul today's digital knowledge infrastructures and to render them ready for further technical advances such as AI applications. At the same time, as will be subsequently discussed, such an approach has sparked concerns regarding data protection infringements and disproportionate state surveillance and control capacities.

The chapter proceeds as follows. First, it engages the political imaginary that drives interoperability in the AFSJ. It then explores classification and standards as key considerations in interoperability efforts and discusses the related concept of data friction in the context of the costs that are required to overcome classification and standardization challenges. Finally, the chapter engages critique of the idea of interoperability and its practical implementations for research on public policy and AI technologies.

THE INTEROPERABILITY IMAGINARY

From a conceptual point of view, interoperability almost always indicates a policy aim in the form of a desirable future, i.e. it is presented as an imaginary that illustrates how things are supposed to work in contrast to current shortcomings (Hilgartner, 2015). In this sense, the interoperability agenda in the AFSJ speaks to alleged structural flaws in the information architecture that underpins law enforcement, border control, and judicial cooperation in the EU. In a largely digitized information environment, databases have come to be key tools for the execution of sovereign tasks (Ruppert, 2012) as they provide the information that is relevant for the (dis-)approval of border crossings, the production of intelligence about possible threats, and the intervention into potential illegal activities. However, as has been argued by the EC, AFSJ databases currently stand largely isolated from each other in a silo structure that prevents the connection of available information, thus leading to a suboptimal knowledge infrastructure that is riddled with "blind spots" (European Commission, 2017a: 33) and resulting intelligence that is "not always complete, accurate and reliable" (European Commission, 2017a: 9).

This perceived lack of knowledge production capacities stands in a sharp contrast to the increasing amount of AFSJ information systems and the data stored in them. There are currently three major systems that support information gathering and exchange in internal security matters in the EU: the Schengen Information System (SIS II) for law enforcement, border control, and judicial cooperation between the member states; the Visa Information System (VIS) for the exchange of data on visa applications and processes; and the European Asylum Dactyloscopy Database (EURODAC) for biometric data of asylum seekers and irregular border-crossers. In the future, these systems will be complemented by three additional ones that have been adopted but not yet implemented: the Entry-Exit System (EES) for the systematic recording of all border crossings into and out of the territory of the EU; the European Criminal Records System for third-country nationals (ECRIS-TCN) for information on individual criminal histories; and the European Travel Information Authorisation System (ETIAS) for the pretravel approval of entry criteria into the EU (analogous to similar systems in the US, Canada, and other parts of the world). As has been highlighted by the EC multiple times over the past decade, these systems are considered key in regard to the timely availability of accurate information, underpinning the regulation of mobility and the fight against terrorism and transnational crime (e.g. European Commission, 2014; European Commission, 2016b; European Commission, 2016a).

To make the most of the data and analytical capacities of these systems, interoperability is regarded as central to ensuring the accuracy and timely availability of information for national and supranational agencies involved in law enforcement, border control, and judicial cooperation in the EU. In its *Strategy Towards a Fully Functioning and Resilient Schengen Area*, the EC claims that "interoperability will connect all European systems for borders, migration, security and justice, and will ensure that all these systems 'talk' to each other, that no check gets missed because of disconnected information, and that national authorities have the complete, reliable and accurate information needed" (European Commission, 2021: 8). The political imaginary of interoperability in the AFSJ is thus one of uninterrupted information flow that addresses knowledge and awareness gaps and enables involved national and supranational actors to base their tasks on reliable and trustworthy data.

The way to achieve such a seamless information landscape is thereby presented in reductionist terms as a primarily technical challenge that deliberately brackets wider institutional, political, economic, and normative questions (also see on "trustworthiness": Gillis, Laux and Mittelstadt, Chapter 14; on "bias" discourses: Hong, Chapter 8; on "ethics": Rönnblom, Carlsson and Padden, Chapter 9, all in this volume). Practical interoperability between AFSJ databases is, in this perspective, supposed to be established through a cross-cutting layer that connects all systems without dissolving their actual structure, instead using biometric data to cross-match existing records, identify and merge multiple records tied to the same biometric identifiers, and facilitate searches and identification queries in a one-stop-shop fashion. To do so, the interoperability framework puts forward multiple technical components: a "Common Identity Repository" is in the future supposed to store biometric templates extracted from all AFSJ databases, whereas a "Multiple Identity Detector" is supposed to merge previously unconnected official records that pertain to the same person and detect fraudulent identities (European Union, 2019a; European Union, 2019b). These are to be complemented with a "European Search Portal", i.e. a unified query interface that can trigger simultaneous searches in all systems based on biometric or alphanumeric data (European Union, 2019a; European Union, 2019b). According to this rationale, implementing these features would raise informational awareness as involved authorities could obtain information on the availability of data in any of the six databases, whereas otherwise individual search queries would need to be run on each of the systems, with the additional hurdle of fragmented access rights.

Scholars have interpreted the interoperability imaginary in the domain of EU internal security as expressive of a deep-rooted sense of governmental failure and fear. Leese (2022) has argued that the political desire for interoperability refers to fundamental questions of (re-) establishing a proper interface between public agencies and the population – particularly with regard to third-country nationals about which by default less information is available and thus needs to be consolidated across different domains that relate to the administrative management of foreigners (e.g. tourism and business travel, asylum, customs, policing, border control). Similarly, Bellanova and Glouftsios (2022) have diagnosed the interoperability imaginary in EU internal security as being foundational to a politics that seeks to reform European knowledge infrastructures, notably in regard to the issue as to "what societal phenomena and subjects should be known and recorded" (Bellanova and Glouftsios, 2022: 460). For them, the interoperability imaginary in the AFSJ is the expression of political anxieties as to the governability of fleeting and elusive phenomena such as migration, crime, or terrorism. In this context, interoperability is considered to present a practical policy path that promises to remedy inadequate state actor capacities vis-à-vis these phenomena by reformatting the digital foundations of knowledge and intervention. Finally, Trauttmansdorff and Felt (2021) have retraced how interoperability aspirations tie in with a larger vision of digital transformation that is framed as an inevitable and unidirectional response to current and future crises. Overall, these accounts tie in with Carmel's (2017) diagnosis that the idea of interoperability is constitutive to the idea of Europe as a social (and governable) space in the first place.

CLASSIFICATION AND STANDARDIZATION

While, as the previous section has shown, from a policy perspective the establishment of interoperability in the AFSJ is framed as a logical and straightforward technical operation that, even in complicated cases, can be achieved if only sufficient resources and innovative engineering are applied, in practice things tend to be slightly more complicated. While purely technical issues might in fact be resolved comparatively easily, literature from Science and Technology Studies (STS) has shown that technology must not be understood as isolated from the larger societal contexts within which it is embedded (Latour and Woolgar, 1979; Pinch and Bijker, 1984). If interoperability in the AFSJ is about making knowledge infrastructures work together, attention must accordingly be paid to how both "knowledge" and "infrastructures" in EU internal security are shaped and come into being in different ways that may or may not render them compatible with others. Valuable conceptual hints regarding the social construction of knowledge infrastructures can be found in the literature on classification systems and standards.

Classification and standardization are closely related concepts, with the former usually preceding the latter. In other words, classification systems tend to become formalized in the form of standards that can be universally referred to in order to ensure the compatibility of material and non-material stuff across time and space. Bowker and Star (1999: 5), in their seminal work on the social ordering functions of classification, have highlighted the "work that classification does in ordering human interaction" by structuring the ways in which individuals and organizations make sense of the world. In its essence, classification refers to an agreed upon way of using the same categories and measurements for the description and quantification of empirical phenomena. As such, classification is an integral part of how humans perceive the world, allowing them to “sort things out” through a system of “spatial, temporal, or spatio-temporal segmentation” (Bowker and Star, 1999: 10). As an epistemic practice, for Bowker and Star (1999: 10) classification thus provides a “set of boxes (metaphorical or literal) into which things can be put to then do some kind of work – bureaucratic or knowledge production”.

In regard to interoperability, the obvious issue with classification systems is that many different ones can exist alongside each other. Depending on choices regarding how to measure and quantify empirical phenomena, different forms of classification may lead to multiple different representations of the same phenomenon – and these might not be compatible (Stone, 2020). This is especially the case with regard to social phenomena such as mobility, crime, or terrorism – key categories in the field of EU internal security – that only come into being as governable phenomena through definition work and the subsequent operationalization of such definitions via data points (Law and Urry, 2004). Adam and Jeandesboz (2022) have shown, for example, how competing definitions of migration in EU external border control on the national level in the 1990s have hampered both operational awareness and the production of aggregate statistics, and how different classification systems were only resolved through the work of intergovernmental expert group meetings that harmonized definitions and corresponding data production. In the current landscape of EU AFSJ databases, legacy effects of their origins in legally separated domains have resulted in only partially compatible classification systems that currently present a major challenge.

The ways in which such epistemic incompatibilities are resolved is usually to formalize classification systems through standardization. Standards provide a common consensus as to how things should be categorized, counted, and measured that actors can refer to across different domains, cultures, and epochs (Lampland and Star, 2009). Arguably, the most well-known body for the establishment and distribution of standards today is the International Organization for Standardization (ISO) which aggregates national perspectives on standards to the global level, but there are many more specialized institutions for standard setting in almost any conceivable area or domain (Higgins and Larner, 2010). What they have in common is that if their work is successful, it tends to become invisible and, as Thévenot (2009) has argued, forms black boxes that govern life from the background where they are hardly noticed any longer. The common lack of visibility as well as the often technical appearance of standards do, however, conceal the work that goes into their construction and maintenance. Standardization work is in most cases by no means a smooth and straightforward operation but is, on the contrary, coined by the interest and power positions of multiple actors, rendering standardization processes fruitful sites for study of the socio-technical nature of politics and regulation (cf. Mügge, Chapter 19; Omotubora and Basu, Chapter 17; and Paul, Chapter 20, all in this volume). Leese (2018) has, for example, shown how in the EU the standardization of biometric modalities for border control largely revolves around business case considerations that prioritize cost-effectiveness over maximum accuracy. And Rommetveit (2016) has retraced how the introduction of biometric travel documents in the EU was largely preconfigured by industrial standards, notably the regulations provided by the International Civil Aviation Organization (ICAO).

As these considerations illustrate, interoperability is contingent on a number of seemingly unrelated and disparate issues in concrete use cases, and is moreover impacted by the legacies of choices made much earlier. In regard to the AFSJ, the significance of classification and standardization can, for example, be witnessed through the struggles for biometric matching capacities across multiple databases. As discussed earlier, such capacities are fundamental for the interoperability imaginary in EU internal security due to the role of biometrics as centralized link between administrative records located in multiple systems. The Joint Research Centre (JRC) of the EC has, for instance, in a study on fingerprint identification technology for the SIS II, explicated the socio-technical formations that determine whether biometric templates from fingerprints can be subjected to algorithmic matching processes. As the report outlines, such capacities are contingent, among other things, on the definition of standardized use cases, standardized performance requirements and indicators, database integrity, as well as the types and quality of biometric data that are to be processed (Joint Research Centre, 2015: 46).

Although there are already standards in place as to the specifications, formats, and minimum quality requirements of fingerprints for storage in the SIS II, the JRC highlights how these standards might in practice be undercut by messy conditions during the capture of biometrics with mobile devices (e.g. at refugee camps or at smaller border crossings points), the lack of quality-control processes to ensure that fingerprint images have a sufficient resolution for the capture of biometric templates, different practices of enrolment (e.g. when not all ten fingerprints are being captured), the non-compliance of ground personnel with best practice guidelines, or the lack of a common exchange standard for biometric data (Joint Research Centre, 2015: iii). As a consequence, the JRC (2015: ii) has called for further harmonization of the "selection of appropriate formats to collect, exchange and process data; production of statistics; identification of appropriate architecture options; application of rigorous procedures for biometric enrolment; selection of measures to foster quality; [and the] definition of use-case scenarios and introduction of regular performance evaluation actions". These recommendations highlight some of the epistemic stakes for interoperability projects in regard to the (digital) knowledge infrastructures that they usually target today. Interoperability processes, in this sense, must already start at the epistemic foundations that precede data and knowledge. Notably, these must not be reduced to technical questions, but instead comprise a wide variety of social, cultural, and organizational issues that must be excavated from "beneath layers of obscure representation" (Bowker and Star, 1999: 47).

In summary, interoperability considerations, while at the surface often presented as primarily technical challenges, are in fact rooted in more fundamental and long-standing ways of knowing and doing. Enabling public agencies and infrastructures to work together thus means harmonizing their ways of counting and measuring the phenomena that they are concerned with, as well as their ways of organizing and processing information. Analytically, accounting for the ordering capacities of classification systems and standards thus requires a broader understanding of interoperability as a socio-technical issue that relates to a multiplicity of organizational, institutional, political, economic, and normative considerations.

DATA FRICTIONS

Another concept that has particular relevance for interoperability questions is what Edwards (2010) has called "data frictions". In his work on climate data, he builds on the resistances that occur between poorly fitting parts in complex technical systems and "[reduce] the amount of work they can do with a given input" (Edwards, 2010: 83f.). Frictions are, however, not limited to the mechanical world, but also occur in computation. Such computational friction, according to Edwards, resists the transformation of data into knowledge and must thus from a practical perspective be reduced as best as possible. One particular form of friction that can frequently be experienced in computer systems relates to the intractability of data. As data moves from one place to another, it requires, as Edwards (2010: 84) frames it, "costs in time, energy, and attention" to ensure that it fits in with data from other sources, to convert its format, to check for consistency and integrity, and so on.

The EC offers a practical example of data friction in its Staff Working Document accompanying the legislative proposal for the interoperability framework for the AFSJ. Without interoperability between databases, so the argument goes, duplicates of the same information would need to be created individually for each system, leading to a multiplicity of records and potential error sources, for example concerning visa regulation where each "visa application contains application data valid at a given moment and data identifying the applicant that are mainly constant over time but which can undergo lawful changes under some circumstances. When not handling identification data distinctly, they are created again for each system" (European Commission, 2017a: 10). The branching off of one piece of master information (i.e. the issuing of a visa) into multiple separately handled records in unconnected systems would in this sense require additional workload to keep all records accurate and up-to-date if the master information changes (e.g. the issued visa has been extended). Moreover, data frictions can occur when data from different sources must be rendered compatible by re-formatting or re-coding it (Ruppert, Law et al., 2013), or when data from one domain/use case must be repurposed for another domain/use case (Glouftsios and Leese, 2023).

To reduce potential data frictions and the resources it would require to resolve them, actors in the AFSJ have attempted to harmonize infrastructures and data. As early as in 2003, during the design phase of the second-generation SIS II, the feasibility study conducted by private consultancy Deloitte contained a specific part on potential synergies between the SIS II and the VIS. The corresponding report made a number of recommendations as to the potential future interoperability of the two systems, including the use of the same formats and standards for alphanumeric and biometric data, the use of the same network for transmission and storage, the use of the same hardware and platforms for central system components, and not least the use of an identical high-level system architecture for both databases (Deloitte, 2003: 17f.). These considerations were, notably, made under the assumption that SIS II and VIS could be connected in the future, for example through the *ex post* implementation of a common Automated Fingerprint Identification Service (AFIS) as specified by the eventual legal regulation for the SIS II (European Union, 2006; European Union, 2007).

CRITIQUE

As the previous sections have outlined, interoperability is a complex socio-technical concept that has governmental as well as societal repercussions as it restructures knowledge infrastructures and intervention capacities. The case of EU internal security is a particularly pertinent one in this regard, as information stored in AFSJ systems could potentially affect the lives of the entire EU population and millions of third-country citizens. Making databases work together and linking up data on individuals is politically framed as a move towards increased accuracy and more effectiveness in security governance, but it also bears the risk of enabling unprecedented surveillance and control capacities for state authorities (Bigo, 2021). In regard to AFSJ interoperability, scholars have paid specific attention to the effects of interoperable databases for political and social ordering. As Bastos and Curtin (2020) have argued, the full realization of interoperability in EU internal security would have profound societal and political repercussions, for example in regard to new power constellations within the EU, in regard to the scope of data protection and fundamental rights, and not least in regard to the relations between the EU and third parties. Throughout this section, some of the most pertinent themes of critique throughout the literature will be discussed.

Firstly, as discussed earlier, in politics and policy-making, interoperability is often presented as a self-evident concept that addresses shortcomings in public administration and the knowledge infrastructures that underpin governance and regulation. Moreover, despite its genuinely socio-technical make-up, it is usually framed as a purely technical challenge that can be overcome if only sufficient resources are mobilized. As the EC has argued as early as in 2005, interoperability should be considered "a technical rather than a legal or political concept. This is disconnected from the question of whether the data exchange is legally or politically possible or required" (European Commission, 2005: 3). For Bigo, Ewert et al. (2020), such a technical framing is part of a larger strategy of the EC to depoliticize regulatory decisions, i.e. to conceal the impact on new technological tools for fundamental rights of both EU citizens and third-country nationals. As they argue, interoperability in the AFSJ is "entrenched in the paradox on freedom, technology, and surveillance" (Bigo, Ewert et al., 2020: 109) that goes back to the founding principle of the Schengen area and its underpinning rationale that free movement can only be safeguarded by enhanced surveillance and control capacities.

Such enhanced surveillance and control capacities tend to interfere with some of the fundamental legal and human rights principles that the EU is predicated upon. Vavoula (2020) has, for instance, pointed out that interoperability potentially interferes with the principle of purpose limitation, i.e. the fact that data generated for a particular use case must not without explicit permission be used in other contexts – an argument that, also in terms of access rights to data across different systems, resonates well with concerns put forward by the European Data Protection Supervisor (2018) and the EU Agency for Fundamental Rights (2018). For Vavoula (2020), fully interoperable AFSJ databases, in undermining purpose limitation, would contribute to what she deems a "Panopticon lens", or, in other words, the repurposing of existing data for as many different cross-domain use cases as possible, for example mobilizing asylum data for border control or visa data for law enforcement. From the perspective of EU citizens and third-country nationals, others have put forward concerns about individual privacy rights (Aden, 2020; Electronic Frontier Foundation, 2021) and have voiced concerns about interoperability further contributing to the pre-emptive regulation of crime and mobility (Giannakoula, Lima et al., 2020).

The latter argument ties in with the analysis of critical border scholars who see interoperability as yet another step towards a high-tech apparatus for surveillance and population control (cf. Antenucci and Meissner, Chapter 31 in this volume; Molnar, Chapter 23 in this volume). Dijstelbloem and Broeders (2015: 22) have in this sense advanced the argument that the EU border framework today is largely predicated on "monitors, computers, scans, cable networks, radars, [and] communication technology" that serve to "prevent the arrival of unwelcome migrants by tracking, tracing and blocking them, and facilitate their return". AFSJ interoperability, for them, thus speaks to larger trajectories of European migration policy and constitutes a political project that is geared towards the drawing together of "biometrics, information storage systems, risk profiles, migrant categories, and travel data […] to a network in which references circulate" (Dijstelbloem and Meijer, 2011: 28). Notably, such a network could be accessed and mobilized at any given point in time and at any given location – at the border, inside the territory of the EU, and even outside of it.

CONCLUSIONS

In summary, this chapter has outlined how and why interoperability has become a key concept in public administration and governance that resonates closely with the continuing rise and importance of digital knowledge infrastructures and related questions of databases, information exchange, and analytical capacities, including AI applications. The first section argues that, as a high-level concept, interoperability has sufficient appeal to serve as a political imaginary that informs policy-making in many different domains. At the same time, however, the chapter has challenged the ways in which interoperability is commonly framed in the political arena. It is, as has been shown, not an exclusively technical matter, but rather connects to fundamental epistemic questions as well as social, cultural, and organizational aspects of knowledge and action.

The study of interoperability must then investigate its socio-technical composition within particular contexts. Only then can it be filled with meaning and assessed in its potentially transformative effects on public administration and governance. To do so, this chapter has engaged in more detail with the interoperability project in the EU AFSJ where it is supposed to make multiple large-scale databases for law enforcement, border control, and judicial cooperation work together through the biometrically mediated cross-matching of official records that pertain to different legal domains – without dissolving the actual silo structure of these databases. Understanding interoperability as a situated socio-technical phenomenon, as this chapter has argued, has significant repercussions for our understanding of governance and public administration. Rather than automatically being turned into more efficient and effective forms of cooperation, analytical attention must be paid to the wider epistemic and institutional surroundings within which interoperability is supposed to take place. As such, it challenges, among other things, techno-solutionist conceptualizations of AI as a means to address and resolve current challenges in the public domain. Instead, understanding interoperability as a relational and situated phenomenon foregrounds its entanglement with larger regulatory and societal issues.

Building on such an understanding, the chapter has discussed some of the most pertinent critiques of interoperability. While appearing intuitive and logical on the surface, as has been shown, the unrestricted availability of information can abet governmental aspirations that are predicated upon surveillance and control, undercutting both individual and collective normative and legal principles and, most importantly, serving to sort and discriminate populations and mobility flows almost independent of temporal and spatial constraints. Clearly, more empirical research on interoperability – in the EU AFSJ and elsewhere – is required to fully understand its (long-term) implications. As of the time of writing, interoperability of EU internal security databases remains a work in progress and even after eventual implementation, practical deviations from high-level policy can be expected. Nonetheless, interoperability can be expected to become real in one form or another in the near future. Therefore, the need to critically assess what such interoperability will look like and what effects it will have, both in the EU and beyond, is all the more pressing.

REFERENCES

Adam, P. and J. Jeandesboz (2022). ‘Before Datafication: Quantification and Information Sharing on Migration and External Borders in the European Union’, Paper presented at the EISA Pan-European Conference, 1–4 September, Athens.

Adebesin, F., et al. (2013). ‘A Review of Interoperability Standards in e-Health and Imperatives for their Adoption in Africa’, *South African Computer Journal*, **50** (1), 55–72.

Aden, H. (2020). ‘Interoperability between EU Policing and Migration Databases: Risks for Privacy’, *European Public Law*, **26** (1), 93–108.

Bastos, F. B. and D. M. Curtin (2020). ‘Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue’, *European Public Law*, **26** (1), 59–70.

Bellanova, R. and G. Glouftsios (2022). ‘Formatting European Security Integration Through Database Interoperability’, *European Security*, **31** (3), 454–474.

Bigo, D. (2021). ‘Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?’, in D. Bigo, T. Diez, E. Fanoulis, B. Rosamond and Y. A. Stivachtis (eds), *The Routledge Handbook of Critical European Studies*, London/New York: Routledge, pp. 400–417.

Bigo, D., et al. (2020). ‘The Interoperability Controversy or How to Fail Successfully: Lessons from Europe’, *International Journal of Migration and Border Studies*, **6** (1–2), 93–114.

Bowker, G. C. and S. L. Star (1999). *Sorting Things Out: Classification and Its Consequences*, Cambridge, MA: MIT Press.

Carmel, E. (2017). ‘Re-Interpreting Knowledge, Expertise and EU Governance: The Cases of Social Policy and Security Research Policy’, *Comparative European Politics*, **15** (5), 771–793.

Deloitte (2003). *SIS II Feasibility Study. Additional Study: SIS-VIS Synergies*, 23 May.

DeNardis, L. (2011). *Opening Standards: The Global Politics of Interoperability*, Cambridge, MA/London: MIT Press.

Dijstelbloem, H. and D. Broeders (2015). ‘Border Surveillance, Mobility Management and the Shaping of Non-Publics in Europe’, *European Journal of Social Theory*, **18** (1), 21–38.

Dijstelbloem, H. and A. Meijer (2011). *Migration and the New Technological Borders of Europe*, Basingstoke, UK: Palgrave Macmillan.

Dittmer, J. (2018). ‘The State, All at Sea: Interoperability and the Global Network of Navies’, *Environment and Planning C: Politics and Space*, **39** (7), 1389–1406.

Edwards, P. N. (2010). *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*, Cambridge, MA: MIT Press.

Electronic Frontier Foundation (2021). *Privacy Without Monopoly: Data Protection and Interoperability*, San Francisco.

European Commission (2005). *Communication from the Commission to the Council and the European Parliament on Improved Effectiveness, Enhanced Interoperability and Synergies Among European Databases in the Area of Justice and Home Affairs*, COM(2005) 597 final, 24 November, Brussels.

European Commission (2014). *An Open and Secure Europe: Making it Happen*, COM(2014) 154 final, Brussels.

European Commission (2016a). *Delivering on the European Agenda on Security to Fight Against Terrorism and Pave the Way Towards an Effective and Genuine Security Union*, COM(2016) 230 final, Brussels.

European Commission (2016b). *Stronger and Smarter Information Systems for Borders and Security*, COM(2016) 205 final, Brussels.

European Commission (2017a). *Commission Staff Working Document Part 1/2: Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability Between EU Information Systems (Borders and Visa) and Amending Council Decision 2004/512/EC, Regulation (ED) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and Proposal for a Regulation of the European Parliament and the Council on Establishing a Framework for Interoperability Between EU Information Systems (Police and Judicial Cooperation, Asylum and Migration)*, SWD(2017) 473 final, Brussels.

European Commission (2017b). *New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations*, Brussels: Publications Office of the European Union.

European Commission (2021). *Communication from the Commission to the European Parliament and the Council: "A Strategy Towards a Fully Functioning and Resilient Schengen Area"*, COM(2021) 277 final, Brussels.

European Commission (2022). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures for a High Level of Public Sector Interoperability Across the Union (Interoperable Europe Act)*, COM(2022) 720 final, Brussels.

European Data Protection Supervisor (2018). *Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-Scale Information Systems*, Brussels.

European Union (2006). *Regulation (EC) No 1987/2006 on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II)*, Brussels: Official Journal of the European Union.

European Union (2007). *Council Decision 2007/533/JHA on the Establishment, Operation and Use of the Second Generation Schengen Information System (SIS II)*, Brussels: Official Journal of the European Union.

European Union (2019a). *Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on Establishing a Framework for Interoperability Between EU Information Systems in the Field of Borders and Visa and Amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA*, Brussels: Official Journal of the European Union.

European Union (2019b). *Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on Establishing a Framework for Interoperability Between EU Information Systems in the Field of Police and Judicial Cooperation, Asylum and Migration and Amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816*, Brussels: Official Journal of the European Union.

European Union Agency for Fundamental Rights (2018). *Interoperability and Fundamental Rights Implications: Opinion of the European Union Agency for Fundamental Rights*, Vienna: European Union Agency for Fundamental Rights.

Giannakoula, A., et al. (2020). 'Combating Crime in the Digital Age: A Critical Review of EU Information Systems in the Area of Freedom, Security and Justice in the Post-Interoperability Era: Challenges for Criminal Law and Personal Data Protection', *Brill Research Perspectives in Transnational Crime*, **2** (4), 1–97.

Glouftsios, G. and M. Leese (2023). 'Epistemic Fusion: Passenger Information Units and the Making of International Security', *Review of International Studies*, **49** (1), 125–142.

Gumbo, T. and T. Moyo (2020). 'Exploring the Interoperability of Public Transport Systems for Sustainable Mobility in Developing Cities: Lessons from Johannesburg Metropolitan City, South Africa', *Sustainability*, **12** (15), 1–16.

Higgins, V. and W. Larner (2010). *Calculating the Social: Standards and the Reconfiguration of Governing*, Basingstoke, UK: Palgrave Macmillan.

Hilgartner, S. (2015). 'Capturing the Imaginary: Vanguards, Visions and the Synthetic Biology Revolution', in S. Hilgartner, C. A. Miller and R. Hagendijk (eds), *Science and Democracy: Making Knowledge and Making Power in the Biosciences and Beyond*, London/New York: Routledge, pp. 33–55.

Jimenez, C. E., et al. (2011). 'Technological e-Government Interoperability: An Analysis of Ibero-American Countries', *IEEE Latin America Transactions*, **9** (7), 1112–1117.

Joint Research Centre (2015). *JRC Science for Policy Report: Fingerprint Identification Technology for Its Implementation in the Schengen Information System II (SIS-II)*, Brussels: European Commission.

Kubicek, H. and R. Cimander (2009). 'Three Dimensions of Organizational Interoperability: Insights from Recent Studies for Improving Interoperability Frame-Works', *European Journal of ePractice* **6**, 1–12.

Lampland, M. and S. L. Star (2009). *Standards and their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*, Ithaca, NY/London: Cornell University Press.

Latour, B. and S. Woolgar (1979). *Laboratory Life: The Social Construction of Scientific Facts*, Beverly Hills, CA: Sage.

Law, J. and J. Urry (2004). 'Enacting the Social', *Economy and Society*, **33** (3), 390–410.

Leese, M. (2018). 'Standardizing Security: The Business Case Politics of Borders', *Mobilities*, **13** (2), 261–275.

Leese, M. (2022). 'Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU', *Geopolitics*, **27** (1), 113–133.

Manda, M. I. and J. Backhouse (2016). 'Addressing Trust, Security and Privacy Concerns in e-Government Integration, Interoperability and Information Sharing Through Policy: A Case of South Africa', *CONF-IRM 2016 Proceedings* (67), n.p.

Paul, R. (2022). 'Can Critical Policy Studies Outsmart AI? Research Agenda on Artificial Intelligence Technologies and Public Policy', *Critical Policy Studies*, **16** (4), 497–509.

Pinch, T. J. and W. E. Bijker (1984). 'The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other', *Social Studies of Science*, **14** (3), 399–441.

Rommetveit, K. (2016). 'Introducing Biometrics in the European Union: Practice and Imagination', in A. Delgado (ed.), *Technoscience and Citizenship: Ethics and Governance in the Digital Society*, Cham, Switzerland: Springer, pp. 113–126.

Roßnagel, A., et al. (2012). *SECUR-ED Deliverable 22.1: Interoperability Concept*.

Ruppert, E. (2012). 'The Governmental Topologies of Database Devices', *Theory, Culture & Society*, **29** (4–5), 116–136.

Ruppert, E., et al. (2013). 'Reassembling Social Science Methods: The Challenge of Digital Devices', *Theory, Culture & Society*, **30** (4–5), 22–46.

Sprivulis, P., et al. (2007). 'The Economic Benefits of Health Information Exchange Interoperability for Australia', *Australian Health Review*, **31** (4), 531–539.

Stone, D. (2020). *Counting: How We Use Numbers to Decide What Matters*, New York: Liveright.

Thévenot, L. (2009). 'Governing Life by Standards: A View from Engagements', *Social Studies of Science*, **39** (5), 793–813.

Trauttmansdorff, P. (2022). 'The Fabrication of a Necessary Policy Fiction: The Interoperability "Solution" for Biometric Borders', *Critical Policy Studies*, online first: 10.1080/19460171.2022.2147851.

Trauttmansdorff, P. and U. Felt (2021). 'Between Infrastructural Experimentation and Collective Imagination: The Digital Transformation of the EU Border Regime', *Science, Technology, & Human Values*, online first: 10.1177/01622439211057523.

Vannijnatten, D. L. (2004). 'Canadian–American Environmental Relations: Interoperability and Politics', *American Review of Canadian Studies*, **34** (4), 649–664.

Vavoula, N. (2020). 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?', *European Public Law*, **26** (1), 131–156.