ABSTRACT
In this article, we explore the security politics of EU database interoperability, inquiring how knowledge infrastructures underpin European security integration. Sitting at the intersection of Science and Technology Studies (STS) and critical approaches to European security, we unpack the co-constitutive relation between database anxieties and interoperability mechanisms. By database anxieties, we refer to what European institutions identify as the main epistemic and operational concerns that emerge from the current use of databases by security authorities across Europe. These anxieties are expected to be resolved by mechanisms that foster interoperability. We argue that the relation between database anxieties and interoperability mechanisms shapes the novel conditions of possibility for European security integration in a datafied world. While far-reaching in technological terms, interoperability is not about introducing a new overarching system, but about the management, re-organisation and re-purposing of datasets. Such formatting matters politically because it eventually informs sovereign acts of policing and mobility control.

ARTICLE HISTORY
Received 1 December 2021
Accepted 12 July 2022

KEYWORDS
Area of Freedom; Security and Justice (AFSJ); databases; interoperability; database anxieties; interoperability mechanisms

Introduction
Databases form the infrastructural skeleton of European security cooperation across the Area of Freedom, Security and Justice (AFSJ). State authorities across the EU rely on several databases for counter-terrorism, migration management and border controls (Brouwer 2006, Jeandesboz 2022). Depending on their tasks, national police, border guard and migration administrations, as well as Europol and Frontex, can consult information stored in different IT systems managed at the EU level, which – to date – remain unconnected. These systems are characterised by various data structures, access rules and purposes. This scattered landscape is both the by-product of each system’s socio-technical and political history (Geyer 2008) and a design choice rooted in the EU data protection principle of purpose limitation (De Hert and Gutwirth 2006b).
Security actors cannot automatically access all information stored across all AFSJ databases. This facet of European security integration has gained policy saliency following the 2015 attacks in Paris. Since then, the European Commission has insisted that such an architecture of differently designed and governed databases runs against the ambition of creating a high-tech Security Union (EC 2020).

In collaboration with the EU agency for large scale-IT systems (eu-LISA), European legislators and policy-makers are thus busy building up database interoperability. From a computer science perspective, database interoperability can be understood as the response to “[users’ needs for] shared access across these multiple autonomous databases” (Litwin et al. 1990: 268). In EU policy terms, this means that separate, EU-wide IT systems should become interconnected. In 2019, EU institutions adopted two regulations for achieving interoperability.1 As EU law scholars have already emphasised, database interoperability is not a mere technical fix but an inherently political process (De Hert and Gutwirth 2006a, Bastos and Curtin 2020). If we are to grasp AFSJ database interoperability, we should consider that it is also about what we can call – paraphrasing Leese (2022, p. 113) – the EU security “vision”. Streamlining data access and computational processing impacts what security analysts know about individuals moving across borders, what public authorities perceive as potential threats and how they cooperate in classical sovereign domains, such as law enforcement and border security. Interoperability directly affects European security integration: it touches upon sensitive domains of state sovereignty, requires the technical re-organisation of existing EU-wide databases, and entails the institutionalisation of common standards and security priorities.

This article explores the security politics of EU database interoperability. Unlike more orthodox EU studies, we do not focus here on security politics understood as “explor[ing] the ‘who gets what, when, and how’ of internal security cooperation” (Bossong and Rhinard 2016, p. 9). Our approach to studying technology’s role in security politics is de-descriptive (Akrich 1992; see also Bellanova and Duez 2012, Glouftsios 2021, Chapter 3). This entails, first, unpacking the governmental rationalities associated with the perceived necessity for EU database interoperability and, second, exploring how these rationalities materialise in design scripts based on which database interoperability will be constructed. Design scripts, in this context, refer to various documents (e.g. legislation, feasibility studies, impact assessments, product catalogues) that “heterogeneous engineers” (Law 1987, p. 230, see also Glouftsios 2021, p. 7) – including policy-makers, legislators and IT experts – draft, negotiate and circulate in the process of building interoperability. Examining such design scripts is important because it allows us to de-scribe some of interoperability’s core discursive, socio-political and technical elements.

We bring this de-descriptive analytical ethos to the conversation launched by this Special Issue with the aim to foreground how knowledge infrastructures reconfigure European security integration. While Justice and Home Affairs remains largely absent in institutional discourses concerning European digital sovereignty (cf. Roberts et al. 2021), the AFSJ and its databases are a pioneering domain in which the digital and sovereignty have been, and still are, entangled and redefined (Walters and Haahr 2005). Moreover, interoperability is a major hurdle for many institutions across Europe and beyond (Pelizza 2016), ranging from a domain of security such as warfare (Harris 2006) to relations with market actors (Alvarez León 2018). As such, interoperability can be considered an
important element in the continuous redefinition of the relation between sovereignty and the digital.

Sitting at the intersection of Science and Technology Studies (STS) and critical approaches to European security, we study the presumed challenges that generate the need for database interoperability and how the latter will be implemented in practice. The encounter between STS and critical approaches to security has resulted in analyses of the role of data practices in counter-terrorism, migration and border management, as well as warfare (Suchman et al. 2017, de Goede 2018, Scheel et al. 2019). Drawing on the emerging STS field of Critical Data Studies (Kitchin and Lauriault 2018), we emphasise the importance of databases along with algorithms (Gillespie 2014) in the making of European security (Bellanova and Glouftsios 2022), and explore the relation between database anxieties and interoperability mechanisms. By database anxieties, we refer to what European institutions identify as the main epistemic and operational concerns emerging from their appreciation of the current use of databases by authorities across Europe. These anxieties are expected to be resolved by mechanisms that foster interoperability, while inscribing specific ways of doing security through data into old and new data infrastructures. The relation between database anxieties and interoperability mechanisms is more than mere problem-solving. The design of new mechanisms does not just fix specific problems to appease epistemic or operational anxieties at their source. The relation between the two is also about defining the novel conditions of possibility for European security integration in a datafied world.

Ultimately, our contribution broadens the taxonomy drawn in the introduction to this Special Issue (Bellanova et al., 2022). We suggest supplementing traditional, post-sovereign and post-traditional approaches to sovereignty with an infrastructural one (see Musiani 2022). As Badenoch and Fickers (2010, p. 2, italics in original) note, “it seems obvious that technological infrastructures are related to projects of European unification, but it is far from clear how”. Focusing on AFSJ database interoperability, we argue that the ongoing re-organisation of these knowledge infrastructures is about formatting European security. As STS literatures highlight, adopting specific formats has far-reaching consequences for how given digital technologies can be used (Bowker and Star 1999, Sterne 2012). These consequences are not deterministic but affect, in the case of databases, both the lives of those who are governed (i.e. subjects whose data are recorded), and the sovereign acts of those who are authorised to govern risk through security (i.e. state authorities whose capacity to process data is partially defined by computational formats) (Koopman 2019). Regarding our case, formatting casts a light on how, instead of integrating existing security practices under a unified command and control, European institutions leverage interoperability to set the conditions within which security actors make what is considered to be a “better” and more “effective” use of databases (see European Commission 2016c). Interoperability is represented as aiming at data’s effective management, accessibility and intelligibility. Formatting is not a lesser, but rather a different “political work” and “exercise of power” (Koopman 2019, p. 155) than those commonly studied by European security literatures focusing on digitalisation or algorithmic security.

The paper is structured as follows. The first section provides a brief overview of the role of databases in European security integration and sketches the context in which interoperability intervenes. The second section situates our contribution to ongoing
conversations across European security literatures and presents our understanding of the co-constitutive relation between database anxieties and interoperability mechanisms. In the third and fourth sections, we analyse the main institutional debates and choices currently informing EU database interoperability. Our discussion is based on various interoperability “design scripts” (Gloftsios 2021) that we analysed thematically: impact assessments, feasibility studies, policy and legislative proposals, as well as the adopted legislation that accompanied the interoperability project from its inception in 2016 until 2019 when the relevant EU Regulations were adopted.

The role of databases in EU security cooperation

Interoperability influences authorities’ power to govern perceived risks and their cooperation across international, institutional and legal boundaries. Currently, various European projects facilitate diverse forms of interoperability – for example, through the integration of Europol’s data silos or the networking of national databases with air passenger information. In this article, we focus on the EU flagship programme, which does not directly involve Member States’ databases but concerns those managed at the EU level. Several EU-wide databases have been built in the field of Justice and Home Affairs – the Schengen Information System (now SIS2), Eurodac and the Visa Information System (VIS) – and more are currently being set up, such as the European Travel Information and Authorization System (ETIAS), the Entry-Exit System (EES) and the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN) (Broeders 2007, Brouwer 2008, Jeandesboz 2016). This “complexity and fragmentation of information systems at European level” poses major challenges to European security integration (General Secretariat of the Council 2017, p. 6) that are expected to be addressed through interoperability. As former Commissioner for Migration, Citizenship and Home Affairs Avramopoulos stated, interoperability will “close gaps and remove blind spots in our information systems for security, borders and migration” (EC 2017d, np). And as a report from the Presidency of the Council highlights (2021, p. 6), “[t]he new architecture for EU information systems […] will completely change [how] border control, and other related activities will be carried out”.

Interoperability impacts the very political dimension of European security integration. Databases are crucial mechanisms for exercising sovereignty (Ruppert 2012), especially in law enforcement, border security and migration management. The European ambition to achieve interoperability reaffirms the crucial role of databases in governing societies. In this regard, Leese (2022, p. 127) explains how interoperability is linked to one of the most fundamental operations of the modern bureaucratic state, namely the production and management of individual identities, and notes that “[t]oday, the idea of identity as a governmental tool is predicated upon large-scale digital datafication and algorithmic analytics”. As Critical Data Studies’ literature highlights (Loukissas 2019), the fact that the data collected and used by authorities are increasingly digital does not mean they automatically become available to other actors or for any other purpose without proper formatting. Besides centring (anew) the political relevance of databases, interoperability also raises questions about how a novel, interconnected architecture of EU databases may foster new forms of European governance (Galli 2020). As Bastos and Curtin (2020, p. 65) argue, interoperability not only “combines in such an intense manner many of
the familiar problems of EU governance” but also “generates constitutional and political dilemmas that are arguably quite unique in terms of their intensity”. Such dilemmas are related, for example, to “the divisions of power within the EU” and the relation “between the use of information technologies and the normative standards that EU governance is expected to observe” (Bastos and Curtin 2020, p. 65).

The ambition of making databases interoperable has been recurrently presented as a necessary development to further European security integration. For instance, in 2005, the European Commission introduced the idea of improving the “effectiveness” of existing databases by making them interoperable (European Commission 2005, p. 2). Back then, the Commission’s suggestion was met with resistance and criticism, and no legislative instrument was adopted (De Hert and Gutwirth 2006a). As Bigo et al. (2020) show, the introduction of database interoperability has also been controversial among European institutions. For instance, during this first struggle around interoperability, the European Data Protection Supervisor (EDPS 2006, p. 2) voiced concerns about the relation between interoperability and fundamental rights, and about the Commission’s framing of interoperability as a mere technical question. Furthermore, the EDPS (2016, p. 2) argued that “making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data,” thus fostering a data-driven approach to security.

In response to the terrorist attacks in 2015–2016, database interoperability became a key priority of European policy-makers (Council 2015, Council 2016). In 2016, the Commission released two policy initiatives to promote interoperability in law enforcement, and border and migration management (EC 2016a, EC 2016c). At the same time, it created an ad hoc “high-level expert group on information systems and interoperability,” which delivered its final report in 2017 (General Secretariat of the Council 2017). The group was composed of experts from European institutions and national authorities of Member States and associated Schengen countries. Notably, the European Union Agency for Fundamental Rights (FRA) and the EDPS participated in the expert group, insisting on the risks for individuals brought about by interoperability (FRA 2017, p. 41–44) and the lack of clarity about the “policy objectives” of such a project (EDPS 2017, p. 2).

In 2019, the Commission’s policy initiative was legally backed by the adoption of two Regulations concerning the interoperability of all existing and future EU-wide databases. Together, the two Interoperability Regulations encompass most of the policy areas at the core of European security integration, from border controls and migration management to police cooperation and counter-terrorism. Their adoption seems to have settled the main institutional battles that had accompanied their proposal and negotiation. This does not mean that database interoperability will not prove problematic. As Blasi Casagran (2021, p. 434) notes, “these Regulations may be infringing the right to data protection and other fundamental rights”. The emphasis that both academics and institutions have put on the need to grasp interoperability as more than a technical fix invites us to unpack its security politics.

**Studying EU database interoperability**

Our paper aims to unpack how database interoperability is expected to support European security integration. The latter is typically approached in the relevant literature as
resulting from the inter-institutional, multi-level cooperation of security practitioners and related policy experts (Cross 2011, Bigo 2013, 2014, Trauner and Ripoll Servent 2015, Cross 2019). Recent studies have explored how the deployment of specific technologies conditions the authority different actors have in shaping European security. This approach permits, for example, to grasp how actors like the military (Csernatoni 2018), companies (de Goede 2012) and EU agencies (Jeandesboz 2016) participate in redefining security and the technological instruments through which it is practiced (Balzacq 2008), and how technological innovation shapes strategic visions and policy priorities that drive European security integration (Calcara et al. 2020).

Our paper partakes in the conversation between critical approaches to European security and STS. Most of these works are inspired by STS insights and concepts which foreground the productive role of technologies, from the low-tech, basic devices such as forms and templates (Walters 2002, Bonelli and Ragazzi 2014) to the deployment of advanced analytics (Dijstelbloem et al. 2011, Amoore and Raley 2017 Leese, 2014). While this literature does not systematically engage with EU studies (cf. Bossong and Carrapico 2016, Jeandesboz 2017), it often provides detailed analyses of the power dynamics brought about by EU-led security programmes and emphasises how digital infrastructures play as much an important role as institutions and norms in integration processes. Works at the intersection of STS and critical approaches to European security have opened two important research avenues.

First, researchers draw on STS literature to explore the socio-technical imaginaries of European security and better grasp how “our understanding of societal issues, including migration or security, is strictly connected to the existing modes of imagining (technological) solutions” (Oliveira Martins and Jumbert 2022, p. 1443). Bringing the focus to “the innovation-security-industry interface,” Oliveira Martins and Mawdsley (2021, p. 1459) further push the EU studies’ research agenda on innovation, retracing the progressive “institutionalization” of actors’ “beliefs” about the values and promises of security technologies. In the same vein, recent research on the intersection between digital sovereignty and European security builds on and enriches STS scholar Jasanoﬀ’s work on imaginaries (Jasanoﬀ and Kim 2015). For example, Csernatoni (this issue) unpacks EU rhetoric touching upon digital technologies and the defence sector by focusing on the “hegemonic interventions” through which EU “high politics” attempts to establish a shared imaginary of European strategic autonomy. Conversely, Lambach and Monsees (this issue) insist on the heuristic value of retracing how “geopolitical imaginaries […] contribute to the construction of a distinct EU identity”.

Second, there is fast-growing literature on the political role of infrastructures in the organization of European security. Some researchers investigate how security practices are carried out and maintained through infrastructures – especially digital ones (Dijstelbloem, 2021 Pollozek and Passoth 2019, Nolte and Westermeier 2020). This strand of research increasingly focuses on “the material practices and data infrastructures […] that can eventually shape institutional orders and polities” (Pelizza 2021, p. 488–489). Other scholars explain how infrastructures embody and underpin specific political visions despite their low public visibility (Aradau 2010, Leese 2022). A further strand of research focuses on (data) infrastructures as sites of security politics, foregrounding how decisions about their design and maintenance inform how security can and shall
be practised, and by whom (Glouftsios 2021, Bellanova and de Goede 2022, Bellanova and Glouftsios 2022).

We contribute to these research avenues by focusing specifically on what we describe as database anxieties and interoperability mechanisms. Anxieties refer to the various concerns emerging in debates surrounding database interoperability, which “haunt” sovereign actors in their attempts to assert their sovereignty (Dillon 2017, Gordon 2008). Borrowing from the work of the anthropologist and historian Stoler (2009), we suggest focusing on what institutions characterise – in the official and technical documents presenting or justifying their rationalities, and the design scripts of the technological solutions to be developed – as the phenomena that disturb their supposed ability to maintain and impose a given order. From this perspective, focusing on anxieties permits to challenge the idea of a rational, objective vision at the core of security politics. Without excusing institutions, it helps to foreground specific perceptions of what threatens their capacity to govern and opens a discussion on how given anxieties inform their worldview.

In our case, anxieties are often about what societal phenomena and subjects should be known and recorded, i.e. epistemic anxieties. They are also about what operational procedures are needed to produce knowledge informing sovereign decisions about, for example, inclusion, exclusion and detection of potential threats, i.e. operational anxieties. Our understanding of database anxieties is related to what Critical Data Studies describe as database imaginaries (Nadim 2021), rather than socio-technical imaginaries. This is about acknowledging the productive, and not merely symbolic, role of databases concerning what happens in the world and how actors act upon it. It is thus about understanding how “the database compels and entails specific imaginaries that help organize [security] practices in certain ways (and not others),” and about “take[ing] seriously the co-constitutive dynamics between databasing and worlding” (Nadim 2021, p. 126, 127). As we explain below, multiple operational and epistemic anxieties shape how interoperability comes to be imagined as a solution to various challenges, e.g. the limited access of police authorities to databases used primarily for migration management purposes and the inability of these authorities to detect individuals registered with different names in distinct databases.

**Interoperability mechanisms** refer to the practical ways that operational and epistemic anxieties are expected to be addressed. Not all database interoperability projects rely on the same mechanisms. The choice and design of these mechanisms are eminent examples of what Flyverbom and Murray (2018) describe as datastructuring. As with database imaginaries, datastructuring recognises the productivity of databases, e.g. the ways databases produce the sovereign power of states to manage population and control their borders. But it also emphasises the need “to analyze data settings rather than data sets” (Loukissas 2019, p. 2, italics in original), that is, to de-scribe how databases are managed, organised and re-purposed.

From this perspective, a focus on interoperability mechanisms feeds into research that attends to infrastructural politics. It invites us to pay further attention to how seemingly mundane decisions about data curation, circulation and integration have far-reaching political effects (see also Bellanova and de Goede 2022, Glouftsios 2018). Interoperability mechanisms mediate precisely such processes of datastructuring through which operational and epistemic anxieties related to law enforcement, border security and migration...
management are supposed to be addressed. Interoperability mechanisms are not just technical: they shape European security integration by conditioning how public authorities across the EU coordinate their work through data gathering and sharing. Ultimately, focusing on database anxieties and interoperability mechanisms caters to the power of formatting (Koopman 2019). This is a power that goes beyond solving specific problems; it paves the way – through the (re)organization of seemingly minor infrastructural elements – to novel relations between sovereignty and the digital.

**Database anxieties**

From its first stages, interoperability between existing and forthcoming information systems was framed as necessary to address threats associated with international mobility and migration. The 2015 *European Agenda on Security* emphasised, among other things, that threats “are becoming more varied and more international, as well as increasingly cross-border and cross-sectorial in nature” (EC 2015, p. 2). While cross-border threats refer to transnational organised crime and terrorism, their cross-sectorial nature implies that they can also impact other policy areas, such as border and migration management. Emphasis on this “double cross” fosters existing governmental anxieties about mobilities as unruly and thus potential sources of still unknown threats (Bigo 2002), to which only interoperability seems to be the response.

Indeed, according to the 2016 European Commission’s Communication on *Stronger and Smarter Information Systems for Borders and Security*, which was the Communication that advanced the interoperability project, “border management, law enforcement, and migration control are dynamically interconnected” (EC 2016c, p. 2). The Communication discursively associates international mobility, migration and internal security by emphasising that “Europe is a mobile society”; by referring to the Syrian crisis and the “1.8 million irregular border crossings” that it “triggered”; by reminding us how the 2015 terrorist attacks in Paris “bitterly demonstrated the threat to Europe’s internal security”; and by claiming that there is “evidence” – without making public any such evidence – “that terrorists have used routes of irregular migration to enter the EU and then moved within the Schengen area undetected” (EC 2016c, p. 2). Similarly, the 2016 Commission’s Communication on *Enhancing Security in a World of Mobility* emphasises the need to reconcile “the benefits of increased mobility with the imperative of security”, which implies the facilitation of travels of “bona fide” EU and third-country nationals, and the parallel management of “irregular arrivals” through the establishment of “appropriate identification and screening procedures” (EC 2016b, p. 3).

Besides being exemplary of the ongoing securitisation of international mobility and migration (Huysmans 2000), such framings justify the interoperability between databases originally developed for different purposes. Indeed, framing international mobility, and specifically migration, as a phenomenon generating security risks justifies the need for law enforcement authorities to access information systems that have been established and are being used primarily for border and migration management. The cross-border, cross-sectorial and mobile nature of perceived threats requires transnational “responsibility-sharing, mutual trust, and effective cooperation” (EC 2015, p. 2) among state authorities (police, border guards, migration administrations) and EU agencies (Frontex, Europol). Such transnational, inter-agency cooperation is to be “hardwired” (Andersson
through interoperable databases that support information sharing at the national and EU levels. At the core of the interoperability project is the aim to facilitate, streamline and intensify information sharing and at the same time deal with operational and epistemic anxieties related to: (1) frictions in policing work; and (2) blind spots that prevent state authorities from establishing links between data stored in different information systems. We will now discuss these anxieties in more detail, before explaining how they feed into the interoperability framework.

Frictions in policing work

Interoperability is said to address frictions in the work of police authorities when accessing third-country nationals’ data collected for border and migration management purposes. The operational anxiety at stake here is twofold. First, it is related to the incapacity to consult distinct information systems swiftly, simultaneously and seamlessly. Second, it is about difficulties in verifying the identities of third-country nationals in Member States’ territories.

According to the Commission’s (EC 2017c, p. 11) impact assessment accompanying the legislative proposal on interoperability, “inadequate” access to data is caused by the “complex landscape” of differently governed databases. This is also linked to the principle of purpose limitation, which foresees that data collected for one specific purpose (e.g. migration management) should not be used for other purposes (e.g. law enforcement) that have not been previously specified in relevant legislations (Brouwer 2011). While in the case of some databases (SIS II, forthcoming ECRIS-TCN) law enforcement is set as a primary objective, in others (Eurodac, VIS, forthcoming EES and ETIAS) it is a secondary one. This means that police authorities can query the databases that have been established for border and migration management only under certain conditions and only if the consultation of data is necessary for the prevention, detection or investigation of terrorism or serious crime. In practice, police officers should first lodge requests to access data, which are then assessed by dedicated authorities in the Member States to determine whether the conditions of access are compatible with the purpose limitation principle. This process is, however, resource-intensive. Moreover, it can create delays “because of a lack of technical and practical means at national level”, and it may “hinder the efficiency of the legitimate use” of information systems for policing purposes (EC 2017c, p. 9 and 11).

This operational anxiety has far-reaching consequences in redefining what counts as a legitimate sovereign act. Indeed, it re-signifies the principle of purpose limitation. This is no longer understood as a crucial safeguard that governs the lawful access of police authorities to data collected for border and migration management. Rather, it is seen as something that creates friction in policing work. Information on third-country nationals is stored in distinct databases, and thus public authorities – depending on their access rights and the purpose limitation principle – must conduct searches separately across different databases based on biographic or biometric data. According to a 2017 feasibility study on interoperability prepared by PricewaterhouseCoopers for the Commission, conducting such separate searches – which is a pre-requisite to guarantee the application of the purpose limitation principle – is “time consuming” and “brings additional challenges as regards the in-land identification of TCNs [third-country nationals] on the Schengen
territory, especially when a TCN is not carrying any identity document or has changed names/nationalities/travel documents” (EC 2017a, p. 10).

Such difficulties in identifying third-country nationals refer to the proclaimed lack of regular identity checks in the Member States. These checks are neither strictly related to migration management nor the prevention, detection and investigation of terrorism or serious crime. For migration management procedures, border control and the countering of serious crime and terrorism, competent public authorities can consult digitised information stored in relevant databases. However, besides the SIS II, which primarily contains alerts on convicted persons and individuals who are subject to deportation procedures, no use of other border- and migration-related information systems is foreseen for identity checks in the Member States’ territories (European Commission, 2017a, p. 10).

The operational anxiety about this absence of identity checks works in tandem with the epistemic anxiety concerning third-country nationals – often migrants and asylum seekers – who come to be treated as deviant subjects that should be made knowable and identifiable swiftly and accurately. Again, the interoperability project shows how these anxieties have a generative force, to be leveraged to promote a positive vision of European security for European citizens. For instance, according to the European Commission (2017a, p. 29), rendering third-country nationals knowable and identifiable through digital technologies built upon the interoperability framework will have a positive “impact on many EU citizens, as [it] will help reassure citizens that any third-country national on the European territory has a known genuine identity and a valid reason to be there”. In other words, there is the expectation that checking the identities of third-country nationals inside the Member States – not just at borders – will somehow address EU citizens’ presumed fear of the Other. As Blasi Casagran (2021, p. 452–454) argues, regular identity checks facilitated by interoperability are inherently discriminatory – they imply differential treatment of EU citizens and third-country nationals and the assumption that the latter are more likely to engage in activities threatening the public.

In short, the anxiety at stake here concerns frictions in consulting distinct information systems. This highlights the crucial role European institutions expect databases to play in overcoming operational difficulties on the ground. By redirecting the object of governmental anxieties to what the databases already record and what security actors should access, the question of whether third-country nationals should be considered prima facie as a source of insecurity somewhat fades away.

**Multiple identities and blind spots**

The second anxiety is rooted in the fact that European security largely relies on digital infrastructures. In this case, the source of anxiety does not lie in the world out there, what is happening beyond the borders of Europe, or what may have slipped through them. Specifically, it concerns the incapacity to see what is already present in the databases and thus the risk of not mastering or fully exploiting the digital infrastructures already at the disposal of public authorities. This anxiety – with the accent being on epistemic concerns – is framed by the European Commission (2017c, p. 10) in terms of “blind spots” or “incomplete pictures” in knowledge production, caused by the difficulty “to identify connections between different pieces of registered information”. This is due to the fragmented landscape of databases used for policing, border controls and migration
management. Blind spots in knowledge production are directly related to authorities’ incapacity to detect “multiple identities” – that is, the same person is registered in several distinct information systems but under different identities.

Besides identity fraud (e.g. an individual provided fictitious identity documents to authorities inserting information in a database) multiple identities and blind spots may result from people being registered under different identities for legitimate reasons (e.g. name change after marriage) and cases where inaccurate data are recorded by public authorities. This is about the undependability of already stored data. The Commission’s High Level Expert Group (HLEG) on Interoperability identified bad quality, inaccurate and undependable data as a “cross-cutting” problem relevant to all existing information systems. Bad quality data hinder the investigatory and administrative work of public authorities because their processing may produce false negatives – that is, the non-identification of a wanted person – and false positives, meaning situations where individuals are wrongfully identified, arrested or denied access in the territory of a Member State. Spelling errors, the recording of the wrong sex or nationality, and the insertion of birth dates in databases when the precise date is unknown are only some practices that result in bad quality biographic data (FRA 2018, p. 84, European Court of Auditors 2019). But even in the case of biometric data, quality problems do emerge when, for example, police authorities physically collect and then digitise “latent fingerprints” from crime scenes (Science Hub 2015, p. 26). Latent fingerprints are less reliable and accurate than live scans and, as with inaccurate alphanumeric data, they may cause false alerts.

These problems and data inaccuracies can result in the registration of different identity data that refer to the same person in unconnected information systems. Combined with the phenomenon of identity fraud, this feeds into epistemic anxieties that revolve around blind spots in the production of knowledge mobilised to govern threats, borders and migration in the EU.

The interoperability mechanisms

Having unpacked the database anxieties underpin the interoperability framework, we now turn to its four mechanisms. The two Interoperability Regulations foresee the introduction of interfaces to broaden and facilitate public authorities’ and EU agencies’ access to information stored in both legacy and new databases. The Regulations provide for the creation of four “interoperability components: (a) a European search portal (ESP); (b) a shared biometric matching service (shared BMS); (c) a common identity repository (CIR); (d) a multiple-identity detector (MID)” (Art. 1(2) of Regulation (EU) 2019/817). Our aim here is to explain how these four mechanisms are expected to advance European security integration, specifically in law enforcement, border controls and migration management.

Interoperability brings about a form of European security through data structuring, rather than database integration. While far-reaching in technological terms, interoperability is not about introducing a radically new system, but the gradual re-orientation of routines and data structures. As such, interoperability is a form of mass surveillance where the mass at stake is primarily a mass of digital data (see also Bellanova and de Goede 2022, p. 103), rather than a centrally organised panoptical architecture. The panopticon
metaphor, because of its ocular-centric representation of surveillance (Lyon 2007), may be useful to explain how interoperability “fixes state vision” (Leese 2022) by directing the surveillant gaze of authorities to blind spots (Vavoula 2020, p. 142) and supporting them in resolving errors related to inaccurate data. However, the four components at the core of the interoperability project do not function as infrastructural integrators that create a panoptic whole. They are instead mechanisms for datastructuring – re-organising, linking and re-purposing data – deployed to appease anxieties concerning the functioning of existing and forthcoming EU-wide databases, whose “fragilities” (Bellanova and Glouftsios 2022, p. 170) are as significant as their strengths for European security.

**Addressing frictions: the interface and the match-flag**

To resolve frictions in policing work (1st anxiety), the mechanisms introduced as part of the interoperability framework are the ESP and the so-called match-flag functionality in the CIR. These mechanisms have two aims. First, they should facilitate and streamline police authorities’ access to data originally collected for border and migration management purposes. In terms of datastructuring, this means that interoperability seeks to re-purpose already available information. Second, the ESP and the match-flag should assist in the identification of third-country nationals in the Member States. Here, European security integration is about enabling police authorities across the EU to consult the data of all third-country nationals previously recorded by a transnational constellation of actors entrusted with the management of borders and mobilities: consular authorities processing requests for Schengen visas, visa-issuing administrations, asylum and migration authorities, and border control agents.

More specifically, the stated aim of the ESP is to facilitate “the fast, seamless, efficient, systematic and controlled access” (OJEU 2019, Art. 6) of state authorities, including police authorities, to the databases they deem necessary to perform their tasks. Police authorities responsible for countering terrorism and serious crime in different Member States do not know in advance where – that is, in which database – they can find information about a suspect individual, and so they conduct searches separately in each database. The ESP will provide simultaneous access to data stored in the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN databases managed by Europol and Interpol (OJEU 2019, Art. 9). The ESP is said to reduce the complexity resulting from the fragmented landscape of databases in the EU by enabling the consultation of the data they store and by combining the results of data queries “on one single screen” (European Commission, 2016a, p. 16). In this sense, the ESP functions as a “single window” (European Commission, 2017a, p. 17) for police officers to “see” data shared by information systems developed not only for law enforcement but also for border and migration management purposes. Practically, this means that a police officer in a Member State searching for information about an individual suspected of involvement in terrorism or serious crime will be able to match the biographic and biometric data of that person with information stored in distinct databases fed by a multiplicity of state authorities (not only police) across the EU.

Besides, the interoperability framework foresees that third-country nationals’ data will be consulted to “achieve the purpose of correct identification of persons within the Schengen area” (OJEU 2019, p. 30). This is about identity checks carried out within Member States’ territories. According to a report published by the Commission’s HLEG
on interoperability, “law enforcement access to the systems for identification purposes should not require prior authorisation or be subject to complicated procedures” (General Secretariat of the Council 2017, p. 15). Identification here refers to checks that involve either: (a) the querying of various systems to reveal the identity of an undocumented person (i.e. an individual who does not carry an identity document), using biometric data (fingerprints or facial images) as search keys; or (b) the confirmation of the identity claimed by a documented person by conducting searches based on biographic data and then matching the fingerprint or facial image of that person with the biometric data linked to the claimed identity. It is worth highlighting here that while the identities of third-country nationals are often checked at ports of entry – e.g. airports, seaports and land borders – identity checks in Member States’ territories through, for example, mobile biometric scanners connected to the ESP (see Council of the European Union, 2017), signify the extension of the border inwards to public spaces that come to function as checkpoints where non-EU nationals are targeted.

In this context, the main concern that emerges is about potential violations of the purpose limitation principle. This is especially the case with regard to the consultation of data stored in Eurodac, VIS and the forthcoming EES and ETIAS for law enforcement. To ensure the application of the purpose limitation principle, the so-called match-flag functionality will be developed in the CIR. The CIR is essentially a database that will store individual files containing a set of biographic and biometric data of all third-country nationals registered in the information systems that will become interoperable (excluding the SIS II). For each set of data, it will also indicate the system to which the data belong (OJEU 2019, Art. 17). The match-flag functionality introduces a two-step data consultation process (see EC 2018, p. 10). First, a police officer queries the CIR, through the ESP, by inserting the alphanumeric or biometric identity data of a suspect individual or a person subject to an identity check as search keys. If the inserted identity data matches the information already stored in the CIR, the officer will be notified through a match-flag that the person in question is registered to one or more databases. As a second step, the officer can request access to a database that stores additional personal information.

Take the fictional example of a police officer in Greece who searches for background information about Ms C, a citizen of third country X who is suspected of involvement in an organised crime network operating in Southern Europe. By using the identity data of Ms C, the police officer searches in the CIR, through the ESP, and receives a notification that Ms C’s data are registered. Ms C’s data belong to the VIS because she has applied in the past for a Schengen visa to the French consulate in third country X. The police officer will not have access to the VIS file of Ms C, but only her data stored in the CIR, such as name, nationality, photograph and fingerprints. To get access to additional information that is potentially useful for the investigation – for example, the purpose of travel, residence and occupation that Ms C declared when she applied for a visa – the officer will have to lodge a request to consult Ms C’s VIS file.

This two-step process – first querying the CIR through the ESP and then getting authorisation to access the VIS (or Eurodac and the forthcoming EES and ETIAS) – is said to safeguard the lawful use of border- and migration-related databases for law enforcement purposes. Yet, as the European Data Protection Supervisor noted, this process facilitates the routine access by police authorities to non-law enforcement databases, which entails
a violation of the purpose limitation principle and a “disproportionate intrusion in the privacy of for instance travellers who agreed to their data being processed […] to obtain a visa, and expect their data to be collected, consulted and transmitted for that purpose” (EDPS 2018, p. 17). The ESP and the match-flag functionality in the CIR, understood as interoperability mechanisms, reflect the desire to streamline the consultation of all third-country nationals’ data for purposes linked to the countering of serious crime and terrorism, as well as for regular identity checking. This is a desire informed by a wider epistemic anxiety that represents non-EU citizens as inherently risky subjects that should be rendered knowable.

**Knowing subjects: biometrics and the identity detector**

To detect multiple identities, the mechanisms introduced as part of the interoperability framework are the sBMS and the MID. These should not be understood as functioning independently from the ESP and the CIR. For example, identifying undocumented persons based on their biometrics through the ESP depends on services provided by the sBMS. At the same time, the MID allows links between identities stored in different databases and the CIR to be visualised and memorised. Despite the interrelatedness between the four interoperability mechanisms, we decided to focus on the sBMS and MID in a separate section for analytical and clarity reasons. While the ESP and CIR aim to streamline policing and mobility controls across the EU by resolving frictions in data access and consultation, the sBMS and MID are expected to advance European security integration by covering the aforementioned “blind spots” or “incomplete pictures” in the transnational production of security knowledge. Regarding datastructuring, the sBMS and MID are not so much about re-purposing existing data (as in the case of the ESP and the match-flag), but about establishing links between them to cover blind spots created by the incapacity of public authorities to associate the information stored in distinct databases.

The sBMS will allow for the consultation and comparison of biometric data from the SIS II, Eurodac, VIS, and the forthcoming EES and ECRIS-TCN (OJEU 2019, Art. 12). Since the ETIAS will not process any biometric data, it will not be linked to the sBMS. It is important to clarify here that the SIS II, Eurodac and VIS have their own systems that provide biometric matching for fingerprints (known as the Automated Fingerprint Identification Systems, or AFISs). The sBMS introduces matching functionalities for facial images too, providing a common platform that enables the simultaneous querying and comparison of biometric data across the existing and future databases that will become interoperable (see Eu-LISA 2018, p. 5). Technically, biometric data (samples) will be retained by each database separately. The sBMS will only store biometric templates (OJEU 2019, Art. 13), which are mathematical representations generated by the algorithmic processing of biometric samples. Importantly, each biometric template will include a reference to the database(s) in which the corresponding biometric samples are stored.

In practice, this means that when state authorities conduct searches through the ESP by enrolling an individual’s fingerprints, those fingerprints will be checked against biometric templates in the sBMS, which will allow a determination of whether the person in question is registered in one or more databases. The sBMS can therefore be thought of as an association tool enabling the establishment of links between data files and
different identities assumed by the same person (EC 2017b, p. 47). The sBMS is considered crucial because it will allow authorities to detect identity fraud, distinguish identity fraud from cases of people who are registered under multiple identities for legitimate reasons, and establish links between persons who happen to share the same or very similar identities (EC 2017b, p. 56–58). In short, the sBMS supports the transnational production of security knowledge by linking identities stored in distinct border, migration and law enforcement databases fed with information by multiple authorities across the EU. These links are divided into four visualised and memorised categories by the MID.

The first category is the yellow link (OJEU 2019, Art. 30). Yellow links are created, for example, when files in two or more databases share the same biometric data but a different biographic identity (or vice versa: same biographic identity, but different biometric data). Yellow links should be assessed and confirmed manually by data owners – that is, by national authorities responsible for creating and updating the files in each database (OJEU 2019, Art. 29). This is because automated biometric matching fails, especially in case of bad quality data. A yellow link denotes that manual assessment and verification have not yet occurred. It signifies the constitutive uncertainty and epistemic anxiety about who a person is – uncertainty that is expected to be fixed through the manual assessment of the link by, for example, fingerprint experts.

The second category of links memorised in the MID is the green link, which refers to a situation where different persons (different biometric data) share the same biographic identity (OJEU 2019, Art. 31). For example, Ms Y, a Schengen visa holder, is stopped and interrogated upon her arrival at an airport – for example, Amsterdam Schiphol – because there is an SIS II alert for extradition purposes (OJEU 2018, Art. 26) that refers to her biographic identity. Greek authorities previously created this alert. However, biometric verification at Schiphol through scanning Ms Y’s fingertips reveals that this is a false positive: Ms Y is not the person for whom the alert has been issued. In this case, a green link will be created, denoting that Ms Y shares the same or very similar biographic identity with a person registered in the SIS II. In this example, green links are expected to fix the problem of false positives that may result in an individual’s wrongful suspicion and arrest.

The third category is the red link, which means that the same person is registered in different databases with different biographic identities (OJEU 2019, Art. 32). Take the example of Mr B, a citizen of third country Z for whom French authorities issued an SIS II alert for discreet checks because they suspected him of involvement in a terrorist network (OJEU 2018, Art. 36). Mr B purchases a fake identity document under the name Mr C. With that document, Mr C applies and acquires a Schengen visa from the Italian embassy in third country Z. Through the sBMS, a link is detected between the identities B and C, and the authorities subsequently confirm that this is a case of identity fraud. When Mr C arrives at Milan’s Malpensa airport, the Italian authorities will stop and arrest him because of the red link in the MID. Contrary to green links, red links are expected to reduce false negatives: the non-identification of known suspects or wanted individuals.

Finally, the last category of links created in the MID is the white link, which means that the same person is registered with the same identity in two or more databases (OJEU 2019, Art. 33). For example, Ms D is registered in the VIS because she has previously applied for a Schengen visa. However, because her country of origin is now visa-exempt, she applied for a travel authorisation through the ETIAS. Upon her arrival in a
Member State, she is registered in the EES and, through the sBMS, the authorities detect a link to a VIS file. In this case, the MID will memorise a white link between Ms D’s files in the VIS and EES, which denotes that she is registered in different databases for legitimate reasons.

The functionalities of the sBMS and MID reflect a long-standing technique of producing security knowledge through biometrics. The establishment of biometric registration systems in the EU allows for the “traceability” (Bonditti 2004) of mobile subjects – that is, the tracking and reconstruction of their travels and bureaucratic trajectories (Scheel 2019, p. 63). Data files that contain information about individuals – their nationality, where they applied for a visa, under what names, where and when they entered the EU for the first time, etc. – can be unlocked through a (seemingly) simple biometric match. This could also be done before the introduction of the interoperability framework, by using existing, EU-wide databases deployed for policing and border security. However, the sBMS and MID are expected to add the capacity to establish, visualise and memorise links between previously disassociated data. Through such links, the goal is to allow authorities across the EU to produce more accurate and reliable information, reassuring that they know subjects with (biometric) certainty.

Conclusions

European institutions see interoperability as contributing to improving, accelerating and intensifying information sharing between state authorities across the EU. The interoperability of AFSJ databases, including those that were not set up for security purposes, is expected to resolve frictions in policing work, facilitate the identification of third-country nationals in the Member States’ territories, and shed light on blind spots by detecting multiple identities and related data-quality problems. Interoperability seeks to address the need to “collect, check and connect the right information at the right time in the right place to undertake effective action” (Council of the European Union 2016, p. 7). This is supposed to be achieved not by introducing a new system that integrate into a single database all existing data, but by designing, implementing and re-organising a series of infrastructural elements that store, match, associate and repurpose data sets stored in already existing systems.

Drawing on STS and critical approaches to European security, we proposed studying the security politics of interoperability by exploring the database anxieties that inform it, and then analysing the mechanisms adopted to respond to these anxieties. As such, we participate in the growing conversation about the role of digital technologies and knowledge infrastructures in the making of European security (Bossong and Carrapico 2016, Carrapico and Barrinha 2017, Calcara et al. 2020). Our contribution is three-fold.

First, we cast a light on a major dynamic at play in European security integration – EU database interoperability – which, despite its policy relevance, remains largely overlooked in European security literatures (cf. Curtin 2017, Leese 2022). A focus on database anxieties reminds us that European security visions are rooted in rationalities that see threats emerging not only beyond and within European borders but also, and crucially, from the world that has been already recorded – or that should have been recorded – in databases. In this context, attention to the interoperability mechanisms reveals that European security integration needs datastructuring, and that the latter affects the
former in practice. Our analysis shows that it is crucial to better understand how data-structuring and the (re)design of knowledge infrastructures – in this case, AFSJ databases and their interoperability mechanisms – inform the conditions of possibility for European security integration.

Second, we supplement the literature highlighting interoperability’s potential impact on European governance. More specifically, we explicate the formatting power of European institutions; that is, the power to influence through the choice and design of specific interoperability mechanisms how petty sovereigns (public authorities or EU agencies) can make novel use of existing and forthcoming databases. This formatting power affects the broader dynamics of European security integration. The interoperability mechanisms foreseen would add layers of formatting that promise efficiency while facilitating (and inviting) further connection across national and organisational boundaries. This is what Koopman (2019, p. 12) sees as formatting’s key “operation of power,” namely one that “both tie[s actors] down and speed[s them] up”.

Third, our work demonstrates how AFSJ remains a crucial site in which digital sovereignty is at play. While EU institutional discourses about digital sovereignty do not primarily touch upon Justice and Home Affairs (cf. Oliveira Martins et al., this issue), the introduction to this Special Issue argues that there is value in leveraging this policy momentum to better grasp the rearticulation of the digital and sovereignty, both understood as historically evolving and intertwined in specific ways (see Bratton 2015, p. 20–21). In this spirit, our article highlights how database interoperability becomes a crucial site of such rearticulation. By foregrounding the political role of infrastructures, this contribution also broadens the nascent digital sovereignty research agenda, thus echoing Musiani’s (2022, p. 786) invitation to approach “the study of digital sovereignty as a set of infrastructures and socio-material practices”.

Additional information

Authors are listed in alphabetical order. They have contributed equally to the article. They would like to thank Annalisa Pelizza, Helena Farrand Carrapico and Denis Duez for the comments provided to early versions of this article, as well as Jocelyn Mawdsley and two anonymous reviewers for their constructive feedback.

Note


Disclosure statement

No potential conflict of interest was reported by the author(s).
Funding

Rocco Bellanova’s research was supported by funding provided by the Université Saint-Louis – Bruxelles (Belgium) in the framework of the preparation of the ERC Starting Grant project “DATAUNION - The European Data Union: European security integration through database interoperability” (ERC-StG-2021, GAP-101043213). Georgios Glouftsios’ research was funded by Fondazione Caritro (Project “Digitised Borders”).

ORCID

Rocco Bellanova http://orcid.org/0000-0001-6222-6636
Georgios Glouftsios http://orcid.org/0000-0003-2749-9828

References

Council, 2015. Conclusions of the council of the EU and of the member states meeting within the council on counter-terrorism. Brussels: Council of the EU.


European Court of Auditors, 2019. EU information systems supporting border control – a strong tool, but more focus needed on timely and complete data. Luxembourg: European Court of Auditors.


