Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance

Rocco Bellanova (University of Amsterdam / ORCID iD: https://orcid.org/0000-0001-6222-6636) & Georgios Glouftsios (University of Trento / ORCID iD: https://orcid.org/0000-0003-2749-9828)
*
†

Abstract

This article focuses on the Schengen Information System (SIS II) – the largest data infrastructure supporting police cooperation and border controls in the European Union. Through the SIS II, national authorities exchange information about individuals and objects, and this across national and institutional boundaries. Yet, the SIS II does not always perform as anticipated in its design scripts. Following common threads about *infrastructural politics* across Science and Technology Studies, political geography and critical security studies, we explore *fragility* and *maintenance* as being intrinsic to the functioning of data infrastructures and crucial sites of governance. We show how the SIS II is kept under continuous control to operate as a controlling data infrastructure. This article contributes to a critical inquiry into the datafication of border controls by interrogating how data acquire the status of allegedly credible and accurate information. Ultimately, this approach pinpoints the inherent fragility of seemingly mighty data infrastructures and casts a light on those actors and processes that sustain, through maintenance, contemporary digital borders.

Keywords

Data Infrastructure, Fragility, Maintenance, Schengen Information System (SIS II), Science and Technology Studies

Introduction

A few hours after the 13 November 2015 terrorist attacks in Paris, French authorities closed their Schengen borders. Among the individuals stopped – but not arrested – at the border with Belgium was, as it transpired a few hours later, the person that will become a key suspect. Months later he was arrested in Brussels and is currently serving a prison sentence for events surrounding that arrest (Rankin 2018). He is still awaiting trial for the Paris attacks (Le Monde & AFP 2020). Information about this person was already stored in the Schengen Information System (SIS II) before he arrived at the border. This is a pan-European centralised database consulted by national

[*] Authors' note: Our names appear in alphabetical order: we have equally contributed to the writing of this article. The fieldwork was carried out by Georgios Glouftsios.

[†] Contact information: Rocco Bellanova, Department of Political Science, University of Amsterdam (UvA), Nieuwe Achtergracht 166, 1018WV Amsterdam, The Netherlands - email: r.bellanova@uva.nl. Georgios Glouftsios, School of International Studies, University of Trento, Via Tommaso Gar 14, 38122 Trento TN, Italy - email: georgios.glouftsios@unitn.it.

authorities, such as border guards, police, migration offices and visa-issuing administrations, as well as European Union (EU) agencies like Europol, Frontex and Eurojust. Depending on their access rights, national authorities and EU agencies can query the SIS II and consult its "alerts", meaning datasets about people and objects (e.g. vehicles) with whom/which specific actions (e.g. capture, arrest) should be taken. Considering that there was a SIS II alert on the suspected perpetrator of the terrorist attacks in Paris, it is puzzling that the French police failed to arrest him (de Bruycker et al. 2016). This example highlights the potential pitfalls and failures of European data infrastructures that are often represented in official policy discourse as supporting the control of cross-border mobilities in a seamless, totalised and increasingly "smart" fashion (Aradau this issue; Jeandesboz 2016).

For the SIS II to operate as a database that effectively supports the control of transnational mobility, its data infrastructure should also be kept under control. Data infrastructures are "the institutional, physical and digital means for storing, sharing and consuming data across networked technologies" (Kitchin, 2014: 32). They are both "things" – fairly complex material entities, storing an enormous amount of digitised information – "and also the relation between things", i.e. means of data-based cooperation across spatial and organizational boundaries (Larkin 2013: 329). Understood as a data infrastructure, the SIS II interlinks geographically dispersed sites and state authorities that are enmeshed in the control of international mobility across the EU. But setting up and maintaining a data infrastructure "is a non-trivial exercise," ridden with "issues [that] are not simply technical, but are also social and political" (Kitchin 2014: 37 & 40). Like virtually any infrastructure (Borgman et al. 2016, Graham & Thrift 2007), the SIS II materialises as a *fragile* entity which requires *maintenance* Approaching the SIS II from this perspective permits a better grasp of the diverse processes that sustain the digital borders of Europe – both the control processes that the SIS II mediates, and the maintenance processes that seek to deal with its fragility.

In line with the aims of this Special Issue (Leese et al. forthcoming), we show that these processes mostly revolve around the production and circulation of data, and how they come to matter for border control. We explain that maintenance processes that cater to data as "matters of concern" (Kaufmann et al. 2019) and "of care" (Puig de la Bellacasa 2011) are the ones that undergird SIS II alerts as "matters of fact" (Latour 2004). In other words, there is a whole register of maintenance processes and practices through which alerts acquire the status of allegedly credible and accurate information that becomes available to end-users through the SIS II. This means that there is much going on behind the scenes to produce and circulate actionable knowledge upon which frontline officers make sovereign decisions of exclusion and inclusion based on SIS II alerts. The central contribution of this article lies in the suggestion that a critical inquiry into the datafication of border controls should go beyond unpacking the significance of data for controlling international mobility (see Amoore 2013; Broeders & Hampshire 2013) to also interrogate the underpinning *infrastructural politics* of digital borders. Such an infrastructural politics is certainly epitomised in the modes of production and circulation of actionable knowledge as these are inscribed into the design of data infrastructures (see Aradau & Blanke 2016; O'Grady 2015; Leese 2014). In our empirical context, it is also about the often overlooked, but equally important, processes of maintenance through which inherently fragile data infrastructures are made to function according to their design scripts. Following common threads about infrastructural politics across STS (Borgman et al. 2016; Star & Ruhleder 1996), political geography (Kitchin & Dodge 2011; Graham and Marvin 2001) and critical security studies (Aradau 2010; Lisle 2018), we explore fragility and maintenance as being intrinsic to the functioning of data infrastructures and crucial sites of governance.

To find information relevant to the fragility and maintenance of the SIS II, we conducted twelve semi-structured interviews with two groups of experts between November 2016 and March 2017. First, we interviewed experts from the European Commission who acted as project managers for the design, development and deployment of the system, as well as those involved in the drafting of evaluation reports assessing its functioning and use. Second, we interviewed experts working at the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), which is entrusted with the maintenance of the SIS II. We have also consulted various official sources and documents, comprising: (i) technical-administrative reports published by the Commission and eu-LISA and concerning the SIS II, (ii) legal frameworks that govern its establishment, and (iii) studies commissioned by EU bodies that reveal problems and failings in relation to its operations. Altogether, these diverse sets of research materials provide us unique insights on the functioning of the SIS II, particularly regarding its fragility and maintenance.

The remainder of this article is organised as follows. In the next section, we situate the SIS II within the European landscape of data infrastructures used for mobility controls, highlighting its specificity and some of its functional characteristics. In the following section, we discuss how critical approaches to digital borders comprehend European data infrastructures. Then, in conversation with a growing, cross-disciplinary body of literature on infrastructures, we introduce our conceptual approach to the study of the SIS II. The following analytical sections explore the SIS II's fragility and maintenance. We first attend to the fragility of the SIS II by identifying what matters of concern emerge during its operations; in particular, problems related to the quality of SIS II data and the functioning of its technical components. We then investigate the efforts that go into addressing these problems as matters of care, by focusing specifically on how the SIS II is controlled through maintenance. Finally, in the concluding section, we synthesise our key findings and suggest some avenues for future research.

Situating the SIS II in the landscape of European data infrastructures

Since the coming into force of the Convention implementing the Schengen Agreement (1993), Europe's data infrastructures have multiplied. Three have already been implemented – the SIS II, the Visa Information System (VIS), and the European Asylum Dactyloscopy Database (EURODAC) – while others are currently under development, such as the Entry-Exit System (EES). Altogether, these data infrastructures support efforts to address irregular migration and operate as compensatory measures to perceived security risks, such as transnational organised crime and terrorism, associated with the easing of controls at the common borders of the (Schengen)

Member States. While data infrastructures have been set up by state authorities across the world – especially in the global north but also in other regions (Frowd 2014) – their deployment in Europe stands out because of the ambition to create a supranational, controlled space: the Schengen Area. Indeed, European data infrastructures are crucial for the establishment of what William Walters and Jens Henrik Haahr (2005: 105) have described as the "Schengenland" – that is, "a model of networks and of transnational liberal policing." Data infrastructures create a thick, yet barely visible, fabric for data exchange and transnational knowledge generation. They facilitate the dissemination of information and intelligence across national authorities involved in the control of international mobility, and they do so in different ways.

For example, EURODAC allows for the registration of fingerprints of applicants for international protection and helps to determine which Member State is responsible for examining each application (Official Journal of the European Union (OJEU) 2013). The VIS enables officials working at the consulates of the Member States in third countries to create digital files on people applying for short-stay Schengen visas (OJEU 2008). These files are consulted to determine whether applicants intend to migrate irregularly in the Member States after the expiry of their visas, assess the security risks that they may embody, and determine the validity and authenticity of visas at border crossing points. Related to the VIS, the forthcoming EES will have the technical capacity to calculate the duration of the authorised stay of all third-country nationals in the Member States' territories, and to detect those who have no longer the right to stay (OJEU 2017). Besides border security and migration management, there are also other data infrastructures that are used specifically for law enforcement and the pan-European cooperation in criminal matters, e.g. decentralised systems for the collection and analysis of passenger information and the exchange of DNA profiles, and Europol's databases. According to EU regulations adopted in 2019, all these data infrastructures should eventually become interoperable, allowing national authorities to access multiple databases simultaneously through common interfaces (OJEU 2019a).

The SIS II occupies a special place within this landscape of European data infrastructures for several reasons. First, it hosts the oldest and – at present – largest and most frequently consulted database (eu-LISA, 2020: 14). In 2019, the SIS II contained more than 91 million datasets and "there were over on average of 18 million searches per day" (eu-LISA 2020: 8 & 13). Second, it is used both to control the mobilities of third-country nationals (TCNs) who are travelling to, or migrating in, the Schengen Area, and also TCNs and EU citizens who are suspected of serious crime or terrorism. Third, it was designed to store "alerts" – that is, discreet batches of information – on both people and objects (e.g. stolen passports, ID cards and vehicles), as well as to create links between them; for example, a link between a person about whom intelligence is gathered and a car used by an organised crime organisation; or a link between individuals to be refused entry to the territories of the Member States and the stolen identity documents that they carry (Council of the European Union 2004: 3). Alerts include several pieces of information (e.g. names, nationalities, number plates) and diverse data formats, from alphanumeric data to fingerprints and digitised facial images. Dedicated police units in each Member State feed the system with data collected at the national level, and they facilitate the sharing of supplementary information when a query produces a “hit” – that is, when the data used by the authorities of a given country to conduct searches in the SIS II match the data already stored in the database by police units either of the same or a different country.

To be more precise, when the SIS II is used for border security purposes (see OJEU 2018a), it contains alerts on TCNs who are considered as embodying risks “to public policy, to public security or to national security” of the Member States (Ibid.: 33). This applies to persons convicted of a criminal offence in one or more Member State, as well as suspects for whom there are grounds to believe that they have been involved (or will be involved) in criminal and terrorism-related activities. Since the revision of the Schengen Borders Code in 2016, the SIS II can also be queried on a non-systematic basis when EU nationals and other individuals who enjoy the right to free movement cross external borders (OJEU 2016: 11). Apart from the creation of crime- and terrorism-related alerts, the SIS II is used for the coordination of processes related to migration management. For example, it enables the creation of alerts and the registration of re-entry bans on individuals who have entered, or attempted to enter, the Schengen Area irregularly, and on those who are subject to deportation procedures. The information collected, stored and processed in relation to alerts consulted for border security includes alphanumeric data, such as names, aliases and nationalities, biometric information, such as dactyloscopic data (i.e. fingerprints and palm prints), and data algorithmically extracted from digital facial images. The end-users with access to these alerts are border guards conducting controls at the external ports of entry of the Member States, customs, police authorities, internal security agencies, consular authorities responsible for the examination of applications for Schengen visas, as well as those responsible for issuing residence permits. In some countries, direct access to the SIS II is also provided to asylum authorities (OJEU 2019b), while EU agencies, such as Europol and Frontex, may also consult alerts.

Conversely, when the SIS II is used for law enforcement (see OJEU 2018b), security authorities can access a wider set of data, including data on EU citizens. More specifically, they can store, process and consult alphanumeric information and biometrics of, among others, persons wanted for arrest for surrender or extradition purposes, as well as unidentified wanted individuals, such as persons whose fingerprints have been found in a crime scene (i.e. latent fingerprints), but whose identities are unknown. In addition to that, the SIS II allows for the creation of alerts on objects for seizure or to be used as evidence in criminal proceedings, such as stolen passports and firearms, and alerts on persons and objects to be put under discreet surveillance. Regarding this last category of alerts, individuals to be monitored are those for whom there are reasons to believe that they intend to commit a crime, and those considered as threats to the internal security of the Member States, such as suspected foreign terrorist fighters, i.e. EU nationals who join insurgencies abroad (see Council of the European Union 2015: 4; Vavoula 2018: 10-13). Objects to be put under surveillance are vehicles, boats and aircrafts. Among the information shared in relation to these alerts is the place where and time when an individual, vehicle, boat or aircraft was located, and the route across which the relevant authorities have followed them. The end-users with access to the alerts stored in the SIS II for law enforcement are police and judicial authorities, border guards, authorities issuing registration certificates for vehicles and firearms, as well as Europol and Eurojust.

Despite these sophisticated functionalities, the SIS II offers a compelling case to study the fragility of European data infrastructures. The operative and political life of the SIS II bears the marks of failures and ongoing (re)adjustments (Parkin 2011). Indeed, the development of the SIS II was justified in official policy discourse as necessary to address the technical and functional limitations of its first-generation Schengen system (SIS I), e.g. the inability to process biometric data and create links between different categories of alerts (see Council of the European Union 2001)[1]. As regards the current version (SIS II), official evaluation reports signal various problems and malfunctions, such as issues of bad data quality and technical failures in the network connection between the Member States (e.g. European Commission 2016; European Court of Auditors 2019). Such problems undermine the supposedly frictionless security checks enacted on the basis of data gathered and shared by the SIS II. As we will discuss in subsequent sections, these data-related problems are major concerns for European institutions and national authorities. SIS II alerts – their data quality and composition – and the operation of the infrastructure that allows for data gathering, further processing and sharing are under regular control and maintenance to ensure that they effectively support pan-European cooperation in the fields of border security, migration management and law enforcement. As these problems are not uncommon in the context of other data infrastructures, a closer analysis of the SIS II's fragility and maintenance can provide novel insights about Europe's digital borders.

Critical perspectives on (European) digital borders

Critical scholars – notably in the fields of security, border and surveillance studies – increasingly question EU data infrastructures and their deployment. This scholarly interest is linked to the broader turn towards the investigation of how social, political and technological elements become entangled in the construction of borders. Huub Dijstelbloem and Dennis Broeders (2015: 26) frame this point nicely, by inviting us to study the "material context of border control and migration policies" as emerging out of an "active interplay" between technologies, human actors and social groups. In this vein, some scholars investigate how databases and big data analytics affect the routine work of state authorities that enact controls on mobile subjects. For example, Alexandra Hall (2017: 489) explores how decisions about the capture and exclusion of travellers are made "at the interface of embodied humans," who analyse and consult security alerts, and of "algorithmic processes," which identify subjects that purportedly embody risks. In this context, collecting data is a crucial step for controlling mobilities. As Polly Pallister-Wilkins (2016: 158) eloquently shows, traditional border mechanisms like walls may become "devices of data capture"; they "produce the data that are often used, at a later time or in another place, to govern movement and wider (in)securities." Focusing on another decisive step, data analysis, Louise Amoore (2011) has demonstrated how intuitively constructed data association rules that indicate who should be treated as risky or bona fide travellers are coded into the software supporting the functioning of databases used by border guards. Her argument is important because it implies that controls based on risk flags are shaped by the "antecedent" work (see Bourne et al. 2015:

308) of programmers and mathematicians who have developed the software that allows for the processing of travellers' data.

Critical scholars also foreground and question how digital borders sift international mobility and inform transnational cooperation among state authorities that control subjects on the move. For example, Philippe Bonditti (2004: 472 & 475) has shown that biometric databases allow for the emergence of a "multileveled dispositive of control" which brings together state authorities and EU agencies that, by continuously gathering and sharing data, "trace patterns of mobility" to deal with threats related to terrorism. Such tracing is only possible through the digitally mediated coordination of controls that are conducted at varying sites and temporal registers – controls that result in the performative multiplication (see Glouftsios 2018) of borders before, at and beyond the ports of entry to the territories of the Member States (e.g. Bigo and Guild 2005; Vaughan-Williams 2010). As Walters (2006: 197) notes, contemporary digital borders "operate like filters", in the sense that they sort out and block the mobilities of those subjects that are considered as threatening or suspected of irregular migration. This observation is important to understand that data infrastructures do not only transform the socio-technical "morphology" (Dijstelboem and Walters 2019) of Europe's borders, but also support the biopolitical control of the populations crossing them (Adey 2009; Vaughan-Williams 2010). This means that arresting, hampering or blocking mobilities is not the main *raison d'être* of digital borders. As Amoore (2009: 62) puts it, their primary purpose is to regulate circulation, while at the same time maintaining the impression of securitability. This twofold promise of targeting controls without hampering travellers' (and goods') circulation offers national authorities a shared and seemingly depoliticized vision of border controls (Broeders 2007). When these authorities materially embrace such a common vision – through the set up and use of data infrastructures – they also create new political spaces across national and organizational boundaries (Pelizza 2019). Through their socio-technical instantiation, digital borders "hardwir[e] cooperation" (Andersson 2016: 25) among actors that would otherwise head into complex political conflicts.

We contribute to this vibrant body of research by engaging in a conversation about how digital data come to matter for the control of mobilities. As we further elaborate in the next section, this requires a focus on the SIS II's infrastructural politics, especially as they manifest in its fragility and those janitorial processes that keep data infrastructures alive (Plantin 2019). Our understanding of infrastructural politics is linked to, but departs from, recent studies that explore the "technopolitics" of border security: the controversies and power struggles that shape the design and development of new data infrastructures (e.g. Glouftsios 2019; Jeandesboz 2016; Sontowski 2018). These technopolitics bring together many negotiating actors (e.g. EU bureaucrats, national experts, IT companies and consultancies) who, in one way or another, affect the implementation of digital borders. We certainly recognise the analytical value of looking at such controversies and power struggles, as a way to unearth the politics energised in the process of designing, developing and deploying data infrastructures. Yet, this approach risks obliterating other important "things" and "relations" (Larkin 2013: 329) at play in infrastructural politics. For this, we need to focus on data infrastructures' fragility and maintenance, and how - through their infrastructural politics – digital data come to matter.

Infrastructural politics and the mattering of digital data

The notion of data infrastructure permits us to operationalise our understanding of infrastructural politics with regards to the SIS II's fragility and maintenance. Data infrastructures are "relational entities" (Kitchin 2014: 23). As Jonathan Gray et al. (2018: 3) explain, they "are comprised of shifting relations of databases, software, standards, classification systems, procedures, committees, processes, coordinates, user interface components and many other elements which are involved in the making and use of data." Recognising the fragility of these relations, and the maintenance efforts that go into addressing these fragilities, allows for an understanding of infrastructural politics that foregrounds and questions the diverse processes that ultimately make data matter in different contexts (Anwar 2020, Bellanova and González Fuster 2019).

To begin with, an analytical curiosity towards fragility and maintenance allows a better grasp of how political spaces, which are built upon data infrastructures, are sustained. There are several studies that explore how infrastructures produce political space. For example, in the context of European integration, historians of technology Frank Schipper and Johan Schot have introduced the notion of "infrastructural Europeanism" (2011: 246), which directs attention to the ways that Europe, understood as a political space, has been historically built upon transportation networks, supply chains, energy infrastructures, etc. (see Badenoch and Fickers 2010; see also Opitz and Tellmann 2015). Furthermore, geographers have analysed how infrastructures like telecommunications systems "bind cities, regions and nations into functioning geographical or political wholes" (Graham and Marvin 2001: 8), and how they allow space and social processes to be controlled at a distance (Graham 2010: 98-99). As Bruce Braun and Sarah Whatmore (2010: xiii) further explain, telecommunications infrastructures and related objects (e.g. mobile phones) spatialise not only in the sense that they change the topologies of everyday life, by redefining the capacity to communicate at a distance, but also by supporting the constitution of expanding political associations and collectivities.

In the context of international mobility controls, the infrastructural making of political spaces, such as the Schengen Area, manifests in the design, development and, crucially, maintenance of data infrastructures. These, like the SIS II, enable the flow of data across spatial and temporal registers where/when mobile subjects become targets of control practices (see Pelizza 2019: 266-268). Maintenance is crucial in that respect because infrastructures – and especially knowledge infrastructures – "are much more fragile than they appear […and] they have many points of potential failure […a] single point of failure, such as a network router or a central data archive, can disrupt an entire infrastructure" (Borgman et al. 2016: 1-2). Such fragility may hamper their designed relationality; for example, the capacity of data infrastructures to interconnect spaces (e.g. airports, land borders), end-users (e.g. border guards, police) and the technologies that they use to perform their work (e.g. biometric scanners, local databases). Importantly, as we will show in subsequent sections, fragility can also be related to the quality of the data processed, and thus ultimately the very possibility of making them matter for a border check or a security investigation. Focusing on the maintenance processes through which a fragile data infrastructure is made functional permits an exploration of the problems that emerge during its operations, and how its operations are monitored and controlled to ensure that it performs according to its design scripts. This is important because, to fully appreciate and unpack how international mobility is controlled through digital means – and how the Schengen Area is sustained as a controlled space – one should understand not only how data infrastructures operate, but also attend to their failures, and the maintenance processes through which they are rendered functional.

This approach foregrounds what we may call the *flickering* foundations of the Schengen Area as a controlled space. Here, flickering means that data infrastructures have far-reaching effects while being constantly subject to errors and malfunctioning with equally far-reaching effects (Hayles 1993). Contrary to other media, Katherine Hayles (1993: 77) argues, "information technologies operate within a realm in which the signifier [...] exists as a flexible chain of markers bound together by the arbitrary relations specified by the relevant codes." This means that "even very small changes" in this chain can have major consequences: with a few (voluntary or not) commands, information can be widely circulated, altered, miscommunicated or made unavailable (Hayles 1993: 77). Flickering data infrastructures that bring together hardware, software and users both power and threaten those "sequences of interpretation and movement" that bring discrete datasets up to the "frontline of security practice" (de Goede 2018: 27-28). As it is its reliance on modern computing that makes the SIS II foundational for the Schengen Area, the flip side of its flickering nature cannot be fixed once for all. It rather requires regular control, maintenance and (re)adjustment.

By casting a light on the flickering nature of the SIS II, and by paying attention to its fragility and maintenance, we can retrace the diverse ways in which its data come to matter. More specifically, we propose an understanding of the SIS II data and technical characteristics as *matters of concern* and *care* for those actors entrusted with the monitoring, evaluation and daily running of this data infrastructure. Within STS, the notions of matters of concern and care foreground the mobilizations at play in the traffic between knowledge and socio-political practices (Puig de la Bellacasa 2011; Latour 2004; Stengers 2015). From this perspective, what is generally presented as a matter of fact – in our case data turned into SIS II alerts and actionable knowledge – can work as such because related concerns (e.g. technical failures, bad quality data) have been settled through practices of care (i.e. maintenance).

Our point, then, is that critically studying data infrastructures, like the SIS II, requires attention for the diverse problems emerging during their operation. Such a focus complements research focusing on the political rationalities inscribed into their designs (see also Bellanova & de Goede 2020), and the political controversies generated in the process of their development and deployment – themes that have concerned scholars who examine the "smartening" (Jeandesboz, 2016) of border security for quite some time now (see previous section). In fact, as Andrew Barry (2001: 15) notes, "to view technical connections as if they were something like a smoothly running railway network would be a mistake [...] creating and maintaining a network requires work and repair". We will explain that the SIS II is a fragile data infrastructure that does not always function as expected. Problems do occur in its operation, and weaknesses are acknowledged by EU institutions and agencies. This means that "hardwiring cooperation" (Andersson 2016: 25) in the fields of border security, migration management and law enforcement requires constant maintenance of data infrastructures: not only designing and developing them properly, but also controlling and repairing their fragilities to keep them working more or less as expected. We thus attend to how the SIS II's functional problems – especially those related to the continuity of its operations and data quality standards – are dealt with. This permits us to explore the labour that goes into the stabilisation of the all-too-flickering status of Schengen's infrastructural moorings; labour not only related to technical maintenance processes and (re)adjustments, but also the training of the SIS II end-users, or what Christopher Henke describes as "people repair" (1999: 56).

SIS II's fragility

A concern for the SIS II's fragility can be read in its overall architecture, and how this already foresees solutions to keep binding diverse actors and sites across the Schengen Area. The SIS II consists of a Central System (CS-SIS) which was built in Strasbourg (France), a backup CS-SIS located in St Johann im Pongau (Austria), national Copies of the SIS II database, and national systems. All the data shared by the SIS II are stored centrally in CS-SIS in a highly secured datacentre where data processing facilities, servers and cabling configurations are installed underground (fieldwork observation, March 2017). The backup datacentre in St Johann im Pongau ensures the continuity of all services provided by the central system in the case of a major incident that would render it dysfunctional. In addition, the CS-SIS and backup CS-SIS are connected through a network that allows for data mirroring. A mechanism that enables the switchover of operations from the French site to the Austrian one was also established. These centralised infrastructures are connected to the SIS II's national components through a fully encrypted communications network (s-TESTA) managed by the Commission's Directorate General for Informatics. Also, the Member States have their own national databases that are connected through the communications network to the CS-SIS. End-users consult SIS II alerts through their national databases that, in turn, query the CS-SIS automatically. Furthermore, what are known as national Copies are also established in the premises of most Member States. These are continuously updated databases containing all the information stored in the CS-SIS. In this case, instead of querying the CS-SIS, national databases query the Copies, which provide an additional layer of robustness to the SIS II. In the unlikely event of a cascading incident that could potentially disrupt the operations of the CS-SIS and Backup CS-SIS, end-users will still have access to the information stored in the Copies, which means that their work processes (i.e. storing, processing and sharing of data) will not be affected.

These infrastructural moorings interconnect the different actors involved in border management, hardwiring their cooperation by supporting the dissemination of information and intelligence on suspect mobilities. Data infrastructures like the SIS II function as the material conditions of possibility supporting the practical implementation of border management policies, and the establishment of the Schengen Area as a controlled space. As one of our interviewees explained to us:

> People have often the impression that the Commission together with other EU institutions does policy. That we set a policy, rules and so on. This is true, but all these are based on real-world technological developments. There is a process going on underneath what people see, which enables the implementation of certain policies. Policies are driven by necessities, but when you design information systems [SIS II, VIS, EURODAC], you introduce certain ways of cooperating that the policy alone would never be able to do in that detail.
>
> (Interview 1, 2016)

Despite its robust infrastructural design characteristics, and the sophisticated functionalities discussed in previous sections, the SIS II does fail. Problems do emerge in its operations, which are generated both by the work practices of its end-users, and the functioning of its technical operating parts. Functional anomalies and disruptions can be generated, for example, by technical failures of the hardware, like disks, network switches and cabling (Interview 11 2017), as well as errors in the configuration of its software applications, like missing data fields that may prevent end-users from entering complete alert information (Interview 2 2016). Such problems render the SIS II a fragile data infrastructure, emerging as matters of concern that can destabilise its functioning and the provision of related services (i.e. data gathering, processing and sharing) to the authorities that consult it. Two actors are chiefly tasked with handling SIS II's matters of concern. eu-LISA is entrusted with its routine maintenance, while the European Commission's Directorate General for Migration and Home Affairs (DG HOME) regularly publishes evaluation reports on the effectiveness of the SIS II operations.

One of DG HOME's evaluation reports of the SIS II identifies several technical and functional deficiencies (see European Commission 2016). For instance, it emphasises the need to guarantee further resiliency in SIS II operations. The problem is that some Member States have not established national Copies of the database, and thus they face "the serious risk that if the network connection breaks down or Central SIS II [CS-SIS] becomes unavailable, they do not have a fall-back option and so access to SIS II alerts would be completely interrupted" (Ibid.: 9). This means that the border security, migration management and law enforcement processes mediated by the SIS II are not always as smooth as they are portrayed to be. The mobility controls that it supports can be disrupted by infrastructural failures. Even in the case of Member States that have established national Copies, studies commissioned by EU bodies indicate that there are synchronisation problems that result in data discrepancies between the alerts stored centrally and those that appear at the national level (European Court of Auditors 2019: 16). Furthermore, keeping the SIS II continuously available is challenging. Despite the SIS II being, up to a certain extent, resilient by design because of the backup database in Austria, the DG HOME's report clarifies that, in situations where the CS-SIS is unavailable due to technical failures, the switchover from the CS-SIS to the backup site is not instantaneous. This is why technical solutions should be explored to decrease the switchover time, argues the report, "as the current technical possibilities and procedures are not considered to meet the expected standards on system availability" (European Commission 2016: 10).

Data quality is another critical matter of concern, which is even more pressing and problematic than the technical operations and availability of the SIS II. The DG Home's report reveals that there have been "major issues" with the quality of SIS II data (Ibid.: 11), while the reports of an expert group which was established to find solutions for interoperability between IT systems at EU level (including the SIS II) identified data quality as a pressing, cross-cutting issue that hampers the effectiveness of border controls (see European Commission 2017). For example, the national authorities responsible for creating and updating SIS II alerts may enter incomplete or incorrect data, such as false names and dates of birth, which may create cascade negative effects in the work of those actors who use the SIS II for mobility controls. The following extract from a report published by the European Court of Auditors is indicative:

> we found [SIS II] alerts where the first name of the person was inserted as a surname and missing or incomplete dates of birth making it difficult to identify the person. As a result of such issues, when border guards check a name in SIS II, they may receive hundreds of results (mostly false positives), which they have to check manually. This not only makes border control less efficient, but also increases the risk of real hits being overlooked.
>
> (European Court of Auditors 2019: 31)

The problem of bad data quality in the SIS II is so extensive that, according to official measurements, the number of warnings related to either inaccurate or incomplete alert data is approximately three million (Ibid.: 30). These numbers confirm scholarly critiques of the supposed capacity of digital surveillance to "find the needle in the haystack" (see Aradau and Blanke 2016). In the case of mobility controls this means, for example, finding a terrorist within a population of travellers. The problem of how to find the needle is often understood as relating to the sheer quantity of data that are stored and processed by state authorities in their attempts to address security risks. However, data quality is also important, since it is precisely because of the bad quality of alert data that queries in the SIS II can result in hundreds of false positives. This form of fragility seriously hampers the materialization of the SIS II's seamless vision of control, troubling the status of alerts as matters of fact.

Bad data quality is a problem generated not by the technical functioning of the SIS II per se, but by the work practices of its end-users. This means that the "proper" functioning of the SIS II depends both on the conduct of its human constitutive parts and the operations of its technical components. Here is another extract of an interview that we conducted with an expert from the European Commission on problems related to data quality:

> Data quality is a very complex issue. We are talking about thousands of end-users being able to insert data. When you book a ticket, you make sure that your personal information is correct [...]. You are the one who is going to be affected if you insert incorrect information in the [booking] system. In our systems [including the SIS II], this is very rarely the case. Someone who inserts information in the systems is rarely going to use that information again. It will be somebody else down the line.
>
> (Interview 3 2016)

The initial creation of alerts – which is done through the analysis of available information and the filling of relevant data fields by dedicated police units in each Member State – is of utmost importance in the control processes mediated by SIS II. It is precisely through the consultation of alerts after their initial creation that controls are conducted "down the line". The consequence of bad data quality is that frontline officers who consult SIS II alerts may not be able to identify individuals and objects of interest, what is often described as *false negatives* or *missed hits*. At the same time, bad quality data may have serious repercussions for individuals identified wrongly by the SIS II (i.e. *false positives*) and subsequently arrested, detained or denied entry to the Schengen Area.

The problem of bad data quality does not only emerge in the case of the SIS II. A report published by the EU's Fundamental Rights Agency (EU FRA) – which investigated the SIS II and several data infrastructures deployed for border and migration management – reveals that because of misidentifications "the police may arrest a person or border guards may not let a person cross the border" and, especially as regards applicants for international protection, misidentifications may result in individuals being "suspected of having intentionally tried to provide a false identity" (EU FRA 2018: 15). Indeed, the report demonstrates that in cases of incorrect alphanumeric data, inaccurate biometric identifications or the physical impossibility of individuals to provide fingerprints due to, for example, damaged fingers, there is a tendency among authorities to suspect that the individuals in question are trying to hide their identities, especially when it comes to visa applicants, migrants and asylum seekers. This is very problematic since frontline officers tend to relate to already stored data – especially biometrics – as matters of fact that reveal the "true" identity of the individuals in front of them (see Amoore and Hall 2009; Scheel 2019). It makes it difficult to contest (see Glouftsios and Scheel 2020) potential misidentifications and may render even those who are physically unable to register their fingerprints a priori suspects.

SIS II's maintenance

The SIS II's fragile data infrastructure requires continuous care. In practice, this means monitoring, control and maintenance to guarantee that it functions according to its design specifications, and that it is available to its end-users. Dealing with issues related to availability is not a straightforward matter but requires lots of maintenance work, which is necessary to keep the SIS II "up and running" (Interview 9 2017). More specifically, there is the "operational management" process through which the functioning of the SIS II is continuously monitored and, in the case of technical malfunctions and other emerging issues such as software updates and capacity limitations, the relevant maintenance procedures are initiated. eu-LISA is responsible for the operational management of the SIS II (see OJEU 2011). One of the experts working at the Agency describes the process of operational management thus:

> We are running the server infrastructure of the systems [including the SIS II] in our datacentres in Strasbourg and Austria; we are operating the communication infrastructure between the central systems and the Member States where the national parts of the

> applications and the systems are hosted; and we are taking care of the maintenance of the applications as such. This relates to correction of errors and adaptive maintenance. We keep the software up to date, we maintain the machines by replacing hardware components, and we do evolutions in the systems – functional and technical evolutions.
>
> (Interview 11 2017)

From interviews conducted with eu-LISA's experts, and from documents that detail the work of the Agency (e.g. eu-LISA 2015), we understand that actors in charge of caring for the SIS II data infrastructure deploy two main types of maintenance: *corrective* and *adaptive* (see also Glouftsios forthcoming). Corrective maintenance refers to all those activities that seek to react to functional anomalies and prevent potential disruptions of the services provided to end-users. Functional anomalies and service disruptions are either identified by eu-LISA through the monitoring of the central SIS II operations in Strasbourg, or reported by national authorities responsible for the management of the Member States' systems. As discussed in the previous section, such anomalies and disruptions can be generated, for example, by technical failures of the systems' hardware components (e.g. servers, network cables) and errors in the design of their software applications (e.g. missing data fields). Corrective maintenance signifies that the SIS II does not only support the control of international mobility by allowing for the gathering, further processing and sharing of data. It is also controlled through processes that seek to "reactively" correct any identified anomalies in its operations and "pro-actively" address potential disruptions of the services that it provides to end-users (Interview 2 2016). In other words, by monitoring how the SIS II operates, and by correcting any identified anomalies generated by technical failures and malfunctions, eu-LISA seeks to address future service disruptions that could generate frictions in the continuity of data-based controls that target cross-border mobilities.

As stated above, alongside corrective maintenance, the SIS II is subjected to adaptive maintenance, which aims to optimise the system's operations by adjusting it to technological advances, like new versions of software, and proactively addressing any problems that may arise from obsolete components (e.g. servers, network cables, power supply systems) that have been previously installed. Adaptive maintenance is also required to meet the emerging needs of end-users. An important example concerns the storage and processing capacity of the SIS II. The more data end-users insert in the database, and the more end-users consult it due to, for instance, its deployment in new Member States, the more storage and processing capacity should be built by eu-LISA (Interview 9 2017). For instance, according to a recent report, European institutions are aiming to further expand its storage capacity from 100 million to 130 million alerts (eu-LISA 2019: 8). This shows how much storage, data processing and computing power matter for European cooperation between state authorities enacting mobility controls. These seemingly technical issues have political effects because they condition the infrastructural power to control international mobility. It is through the continuous corrective and adaptive maintenance of the SIS II that eu-LISA tries to make it function and address any emerging issues identified through the routine monitoring of its operations.

Apart from the correction of failures and malfunctions, as well the adaptation of the SIS II to emerging technologies and end-user needs, the problem of bad data quality is typically addressed through technical (re)adjustments and the training of SIS II end-users. eu-LISA is involved both in the implementation of technical (re)adjustments and (to some extent) the training of end-users, which are processes that can be thought of as contributing to the maintenance of the system's effective functioning since they seek to address problems concerning pre-defined data quality standards.

As regards technical (re)adjustments, one example is the introduction of fuzzy querying functionality in the SIS II (European Commission 2016: 11). Fuzzy querying allows for the identification of non-exact matches. This means that end-users may find results relevant to their search even if the information inserted (or already stored) in the database is incorrect or incomplete. Another example of technical (re)adjustments is the introduction of automatic fingerprint matching functionality (see JRC 2015). The capacity to store and process biometric data, specifically fingerprints, is considered as a solution to incomplete or inaccurate alphanumeric information. However, it is important to highlight that biometric identification is not a silver bullet. For example, Shoshana Amielle Magnet (2011: Chapter 1) has convincingly argued about the inherently biased nature of biometric registration schemes that do not take into account the situated nature of identity and instead construct it as a purely technical matter of algorithmic data matching. In addition, the accuracy of biometric identification depends a lot on the quality of registered and already stored fingerprints, which in turn depends on factors related to the ways that fingerprints are captured (JRC 2015: 26).

For example, it makes a difference if biometric data are extracted from a live-scanned or a latent fingerprint. With live scans, the quality of fingerprints, and thus the chance of accurate biometric matching, is (relatively) high. However, latent fingerprints – e.g. fingerprints that were collected physically from crime scenes and subsequently digitised – pose "huge challenges" (Ibid.), not only because it is impossible to reacquire a sample, but also because they present low quality features, which can in turn lead to inaccurate biometric matching. Even if we (wrongly) assume that biometric identification works, the option to "perform biometric searches on the basis of fingerprints stored in SIS is not yet available in all Schengen States' national systems, as some require more time than others to implement the necessary technical solutions" (European Court of Auditors 2019: 15). So while some Member States have implemented biometric matching functionality as a solution to problems relating to the quality of alphanumeric data, such problems persist not least because this functionality is not available to all end-users.

The training of the SIS II end-users is organised both centrally, meaning at the EU level, and nationally (Interview 8 2017). Centrally, those responsible for organising training courses are the European Commission (DG HOME), eu-LISA and CEPOL – the EU Agency for Law Enforcement Training. Training concerns not only data quality, but also the work processes related to the creation and consultation of SIS II alerts, as well as the exchange of "supplementary" information by the SIRENE (Supplementary Information Request at the National Entries) offices. To be clear, this information is characterised as supplementary because it is connected to alerts, but it is not directly accessible for frontline officers who perform controls by querying the database. Frontline officers only have access to alphanumeric and biometric data that are useful to identify an individual, while supplementary information is related to the more “investigative knowledge” (Interview 8 2017) which has been produced about the activities of that individual. The provision of training on data quality matters and the functionalities of the SIS II is viewed as crucial because the benefit that national authorities may derive from the SIS II depends on how well-trained they are to use it (European Court of Auditors 2019: 16). The training approach adopted is described as “train the trainer” (see eu-LISA 2013), which means that training is first provided to representatives of national authorities using the SIS II, who then design specialised training courses at the national level. Besides this, webinars are organised both centrally and at the national levels.

While training is certainly important to familiarise end-users with the functionalities of the SIS II, problems do emerge because in some Member States there are no “safe” virtual environments for end-users to practice different functionalities and rare scenarios – for example, the identification of a terrorism suspect or the misidentification of an individual due to the bad quality of data stored in the database. This specifically concerns border guards who only practice “live” on the SIS II. Indeed, the lack of a virtual training environment does not allow end-users “to experience features and scenarios that they do not encounter frequently”, which may render the use of such features and the dealing with rare scenarios difficult when encountered in the real world (European Court of Auditors 2019: 16). While the provision of training is not related to the very technical aspects of the SIS II, training activities are essential to the effective functioning of the system because they seek to modulate the conduct of its human operating parts. Data quality depends on the training of state authorities that create alerts and gather supplementary information, while the overall effectiveness of the SIS II as a controlling data infrastructure depends on the training of those actors who consult SIS II alerts to identify suspect and wanted individuals.

Conclusion

In this paper, we explored a key European data infrastructure, the SIS II. It operates as a flickering foundation, so to speak, of the Schengen Area – one that supports the establishment of a controlled space of “free” movement without functioning optimally and requiring constant maintenance work. Empirically, we explained how the SIS II and its data emerge as matters of concern and care. The SIS II does not enact control in a totalised, smooth and continuous fashion. Problems that are generated both by its technical functioning and end-users’ practices do emerge. For its data to be considered matters of fact, attention to data quality, connectivity and users’ behaviour is paramount. This is precisely why the European Commission, in cooperation with eu-LISA, seeks to control the SIS II by monitoring its operations, by producing evaluation reports that identify functional deficiencies, by organising training courses for end-users, and by implementing corrective and adaptive maintenance procedures. Indeed, the SIS II is a powerful but, at the same time, fragile data infrastructure whose constitutive elements require control, maintenance, (re)adjustments and training. These processes are important in the context of border controls because, by rendering the SIS II functional, they sustain the power to govern international mobility by digital means.

Our analysis contributes to a growing body of literature that focuses on (in)security data and their political technologies, be it expanding data infrastructures or devices, such as biometric scanners, automated border control gates, body scanners, and so on. It supplements this trans-disciplinary conversation by emphasising the potential of mobilizing ideas developed in STS to explore not only how digital borders are designed, developed and deployed – a well-documented theme in the relevant literature – but also how they are made durable through maintenance. Expanding upon these observations, we believe that scholars interested in the infrastructuring of border controls have much to gain by paying more attention to fragility and maintenance for two reasons.

First, it is through attention to the problems, limitations and overall fragility of infrastructures that we can develop counter-narratives challenging the supposed effectiveness of control measures aimed at capturing, filtering and sorting out the mobilities of (in)securitised subjects. As we have shown in our analysis, several institutional actors – especially at the European level – already consider these issues the de facto priorities of security cooperation and border controls. Critical literature's limited interest in security, border and migration data as matters of concern (besides questions of privacy and discrimination; Brouwer 2008, Leese 2014) risks leaving us unable to have a say on how to care about these digital data, and thus about the lives and subjectivities that are connected to them (Bellanova 2019). The second reason is that exploring the fragility and maintenance of infrastructures will allow us to think more expansively about the heterogeneous actors, practices and processes that sustain contemporary digital borders. Besides traditional actors, such as border guards, police, data analysts and migration authorities (Bigo 2014, de Goede 2018), we need to think about the role of maintainers and repairers in the making of borders. Considering the role of these actors may reveal emerging rationalities, knowledges and techniques of power that are related to the infrastructurally-mediated control of mobility. In that respect, the pressing question that we should address revolves around the extent to which the governing of subjects and populations on the move depends on the monitoring, control, correction, adaptation and (re)adjustment of those (data) infrastructures that make mobility governable in the first place.

Acknowledgements

We would like to thank Geopolitics' Editors, especially Professor Nancy Hiemstra, for taking care of the review process in the middle of a pandemic, as well as the three anonymous reviewers for their constructive comments. We would also like to thank this Special Issue's Guest Editors– Matthias Leese, Stephan Scheel and Simon Noori – as well as Beste İşleyen, Silvia Aru and Annalisa Pelizza (and the 'Processing Citizenship' project's team) for their feedback on previous versions of this article.

Funding

Rocco Bellanova's work was carried out in the framework of the research project 'FOLLOW: Following the Money from Transaction to Trial', funded by the European Research Council, Grant No. ERC-2015-CoG 682317. Georgios Glouftsios's research has been funded by the Leverhulme

Trust (grant number 2014-097) and the School of International Studies at the University of Trento (project STERI: Science, Technology and International Relations).

References

Adey, P. 2009. Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space* 27: 274-295.

Amoore, L. 2009. Algorithmic war: Everyday geographies of the war on terror. *Antipode* 41(1): 49–69.

Amoore, L. 2013. *The Politics of Possibility*. Durham: Duke University Press.

Amoore, L. and A. Hall 2009. Taking people apart: digitised dissection and the body at the border. *Environment and Planning D: Society and Space* 27: 444-464.

Amoore, L. 2011. Data derivatives. On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6): 24-43.

Andersson, R. 2016. Hardwiring the frontier: The politics of security technology in Europe's 'fight against illegal migration'. *Security Dialogue* 47(1): 22-39.

Anwar, T. 2020. Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases. *International Political Sociology* https://doi.org/10.1093/ips/olaa006.

Aradau, C. 2010. Security that matters. Critical infrastructure and objects of protection. *Security Dialogue* 41(5): 491-514.

Aradau, C. and T. Blanke 2016. Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*: 20(3) 373-391.

Badenoch, A. and A. Fickers 2010. *Materializing Europe. Transnational infrastructures and the project of Europe.* Hampshire: Palgrave Macmillan.

Barry, A. 2001. *Political machines.*. London and New York. The Athlone Press.

Bellanova, R. 2019. (In)security data as matters of care. In: Salter, M.B. (ed) Horizon Scan: Critical Security Studies for the next 50 years. *Security Dialogue* 50(s): 31-32.

Bellanova, R. and M. de Goede. 2020. The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, https://doi.org/10.1111/rego.12338

Bellanova, R. and G. González Fuster. 2019. Composting and computing: On digital security compositions. *European Journal of International Security*, 4(3): 345-65.

Bigo, D. 2014. The (in)securitization practices of the three universes of EU border control: Military/Navy - border guards/police - database analysts. *Security Dialogue* 45(3): 209-225.

Bigo, D. and E. Guild 2005. Policing at a distance: Schengen visa policies. In: *Controlling frontiers: free movement into and within Europe*, ed D. Bigo and E. Guild (pp. 233-263). Aldershot: Ashgate.

Bonditti, P. 2004. From territorial space to networks: A Foucaldian approach to the implementation of biometry. *Alternatives* 29(4): 465-482.

Borgman C.L., P.T. Darch, A.E. Sands and M.S. Golshan 2016. The durability and fragility of knowledge infrastructures. *Proceedings of the 79th ASIS&T Annual Meeting* 53: 1-10.

Bourne, M., H. Johnson and D. Lisle (2015) Laboratizing the border: the production, translation and anticipation of security technologies. *Security Dialogue* 46(4) 307-325.

Braun, B. and S. J. Whatmore 2010. The stuff of politics: An introduction. In B. Braun and S. J. Whatmore (eds.) Political matter. Technoscience, democracy, and public life. Minneapolis and London: University of Minnesota Press.

Broeders, D. 2007. The new digital borders of Europe: EU databases and the surveillance of irregular migrants *International Sociology* 22(1): 71-92.

Broeders, D. and J. Hampshire 2013. Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe. *Journal of Ethnic and Migration Studies* 39(8): 1201-1218.

Brouwer, E. 2008. *Digital borders and real rights: Effective remedies for third-country nationals in the Schengen Information System*. Leiden: Martinus Nijhoff.

Council of the European Union 2001. *Requirements for SIS II*. Document number 6164/3/01 REV 3. Brussels, 22 June 2001.

Council of the European Union 2004. *SIS II functions / Open issues.* Document number 12573/3/04. Brussels, 30 November 2004.

Council of the European Union 2015. *State of play on implementation of the statement of the Members of the European Council of 12 February 2015 on counter-terrorism*. Document number 14438/15. Brussels, 23 November 2015.

de Bruycker, P., D. Watt, H. Labayle, A. Weyembergh, and C. Brière. 2016. *The Paris Terrorist Attacks : Failure of the EU's Area of Freedom, Security and Justice?* Réseau Universitaire Européen Droit de l'Espace de Liberté, Sécurité & Justice. Available at: http://www.gdr-elsj.eu/2016/01/08/cooperation-judiciaire-penale/the-paris-terrorist-attacks-failure-of-the-eus-area-of-freedom-security-and-justice/ (last accessed on July 8, 2020).

de Goede, M. 2018. The chain of security. *Review of International Studies* 44(1): 24-42.

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 W. Walters 2019. Atmospheric Border Politics. *Geopolitics* OnlineFirst: 1-24.

European Commission 2016. *Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with art. 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and art. 59 (3) and 66 (5) of Decision 2007/533/JHA.* COM(2016) 880 final.

European Commission 2017. High-level expert group on information systems and interoperability. Final report. Ref. Ares(2017)2412067.

European Court of Auditors 2019. *Special Report. EU information systems supporting border control - a strong tool, but more focus needed on timely and complete data.*

EU FRA 2018. Under watchful eyes: biometrics, EU IT systems and fundamental rights. doi:10.2811/136698.

eu-LISA 2013. eu-LISA Training Strategy 2013-2016. Accessed December 1, 2019.

https://www.eulisa.europa.eu/AboutUs/MandateAndActivities/CoreActivities/Documents/eu-LISA%20Training%20Strategy%20and%20Training%20Plan.pdf.

eu-LISA 2015. *Report on the technical functioning of Central SIS II and the Communication Infrastructure, including the security thereof and the bilateral and multilateral exchange of supplementary information between Member States.* doi:10.2857/567010.

eu-LISA 2019. *SIS II – 2018 Statistics.* Tallin: eu-LISA.

eu-LISA 2020. *SIS II – 2019 Statistics.* Tallin: eu-LISA.

Frowd, P.M. 2014. The field of border control in Mauritania. *Security Dialogue* 45(3): 226-241.

Glouftsios, G. 2018. Governing circulation through technology within EU border security practice-networks. *Mobilities* 13 (2): 185-199.

Glouftsios, G. 2019. Designing digital borders: The EU Visa Information System. In: M. Leese and M. Hoijtnik (eds.) *Technology and Agency in International Relations*. London and New York: Routledge.

Glouftsios, G. and Scheel, S. 2020. An Inquiry into the Digitisation of Border and Migration Management: Performativity, Contestation and Heterogeneous Engineering. *Third World Quarterly*. DOI: 10.1080/01436597.2020.1807929.

Glouftsios, G. forthcoming. "Governing border security infrastructures: Maintaining large-scale information systems". *Security Dialogue*. DOI: 10.1177/0967010620957230.

Graham, S. and S. Marvin 2001. *Splintering urbanism. Networked infrastructures, technological mobilities and the urban condition.* London and New York: Routledge.

Graham, S. and N. Thrift 2007. Out of order: understanding repair and maintenance. *Theory, Culture & Society* 24(3): 1-25.

Graham, S. 2010. The end of geography or the explosion of place. In, P. K. Nayar (ed.) *The new media and cybercultures anthropology.* Sussex: Wiley-Blackwell.

Gray, J., Gerlitz, C. and L. Bounegru. 2018. Data infrastructure literacy. *Big Data & Society* 5(2): 1-13.

Hall, A. 2017. Decisions at the data border: Discretion, discernment and security. *Security Dialogue* 48(6): 488-504.

Hayles, N.K. 1993. Virtual Bodies and Flickering Signifiers. *October* 66: 69-91.

Henke, C.R. 1999. The mechanics of workplace order: toward a sociology of repair. *Berkeley Journal of Sociology* 44(3): 55-81.

Jeandesboz, J. 2016. Smartening border security in the European Union: An associational inquiry. *Security Dialogue* 47(4): 292-309.

JRC Science Hub 2015. *Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II).* Document Number EUR 27473 EN.

Kaufmann, M., Egbert, S. and M. Leese 2018. Predictive Policing and the Politics of Patterns. *The British Journal of Criminology* 59(3): 674-692.

Kitchin, R. 2014. *The Data Revolution*. London: Sage.

Kitchin, R. and M. Dodge. 2011. *Code/Space. Software and everyday life*. Cambridge, MA: MIT Press.

Larkin, B. 2013. The Politics and Poetics of Infrastructure. *Annual Review of Anthropology* 42(1): 327-343.

Latour, B. 2004. Why has critique run out of steam? From matters of fact to matters of concern. *Critical Inquiry* 30 (Winter 2004): 225-248.

Le Monde and AFP. March 17, 2020. *Attentats du 13-Novembre : vingt personnes renvoyées aux assises, dont Abdeslam*. Le Monde. Available at: https://www.lemonde.fr/police-justice/article/2020/03/17/attentats-du-13-novembre-vingt-personnes-renvoyees-aux-assises-dont-abdeslam_6033342_1653578.html (last accessed on July 8, 2020).

Leese, M. 2014. The new profiling: algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue* 45(5): 494–511.

Leese, M., S. Noori and S. Scheel. Forthcoming. Data Matters: Introduction to the special issue. *Geopolitics*.

Lisle, D. 2018. Failing worse? Science, security and the birth of a border technology. *European Journal of International Relations* 24(4): 887-910.

Magnet, S.A. 2011. *When biometrics fail. Gender, race, and the technology of identity.* Durham: Duke University Press.

O'Grady, N. 2015. Data, interface, security. Assembling technologies that govern the future *Geoforum* 64: 130–137.

Official Journal of the European Union (OJEU) 2008. *Regulation No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)*. L 218/60.

OJEU 2011. *Regualation No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*. L 286/1.

OJEU 2013. *Regulation No 603/2013 on the establishment of Eurodac*. L 180/1.

OJEU 2016. *Regulation 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)*. L 77/1.

OJEU 2017. *Regulation (EU) 2017/2226 establishing an Entry/Exit System (EES)*. L 327/20.

OJEU 2018a. *Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks*. L 312/14.

OJEU 2018b. *Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters*. L 312/56.

OJEU 2019a. Regulation (EU) 2019/818 *on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.* L 135/85.

OJEU 2019b. *List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System*. C 222/01.

Opitz, S. and U. Tellmann 2015. Europe as infrastructure: Networking the operative community. *South Atlantic Quarterly* 114(1): 171-190.

Pallister-Wilkins, P. 2016. How walls do work: security barriers as devices of interruption and data capture. *Security Dialogue* 47(2): 151-164.

Parkin, J. 2011. *The difficult road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law*. Brussels: Centre for European Policy Studies.

Pelizza, A. 2019. Processing alterity, enacting Europe. *Science, Technology, & Human Values* 45(2) 262-288.

Plantin, J-C. 2019. Data Cleaners for Pristine Datasets. *Science, Technology, & Human Values* 44(1): 52-73.

Puig de la Bellacasa, M. 2011. Matters of care in technoscience. *Social Studies of Science* 41(1):85-106.

Rankin, Jennifer. April 23, 2018. *Paris attacks suspect Salah Abdeslam gets 20-year sentence in Belgium*. The Guardian. Available at: https://www.theguardian.com/world/2018/apr/23/paris-attacks-suspect-salah-abdeslam-gets-20-year-sentence-in-belgium (last accessed on July 8, 2020).

Scheel, S. 2019. *Autonomy of Migration? Appropriating Mobility Within Biometric Border Regimes*. London and New York: Routledge.

Schipper, F. and J. Schot, 2011. Infrastructural Europeanism, or the Project of Building Europe on Infrastructures: An Introduction. *History and Technology* 27(3): 245–64.

Sontowski, S. 2018. Speed, timing and duration: Contested temporalities, techno-political controversies and the emergence of the EU's smart border. *Journal of Ethnic and Migration Studies* 44(16): 2730-2746.

Star, S. L. and K. Ruhleder 1996. Steps toward an ecology of infrastructure. *Information Systems Research* 7(1): 111-134.

Stengers, I. 2015. "Accepting the reality of Gaia. A fundamental shift?" In The Anthropocene and the Global Enrivonmental Crisis, edited by Clive Hamilton, Christophe Bonneuil and François Gemenne, 134-144. London: Routledge.

Tazzioli, M. 2018. Spy, track and archive: the temporality of visibility in Eurosur and Jora. *Security Dialogue* 49(4): 272–288.

Vaughan-Williams, N. 2010. The UK border security continuum. Virtual biopolitics and the simulation of the sovereign ban. *Environment and Planning D: Society and Space*. 28: 1071-1083.

Vavoula, N. (2018) Prevention, Surveillance, and the Transformation of Citizenship in the 'Security Union': The Case of Foreign Terrorist Fighters. *Queen Mary University of London, School of Law Legal Studies*. Research Paper No. 293/2018.

Vukov, T. and M. Sheller 2013. Border work: surveillant assemblages, virtual fences, and tactical counter-media. *Social Semiotics* (23)2: 225-241.

Walters, W. and J. H. Haahr 2005. *Governing Europe. Discourse, governmentality and European integration*. London and New York: Routledge.

Walters, W. 2006. Rethinking borders beyond the state. *Comparative European Politics* 4: 141–159.

Interviews cited

Interview 1 2016. European Commission DG HOME. Brussels 28 November 2016.
Interview 2 2016. eu-LISA. Brussels 28 November 2016.
Interview 3 2016. European Commission DG HOME. Brussels 30 November 2016.
Interview 8 2017. European Commission DG HOME. Brussels 17 January 2017.
Interview 9 2017. eu-LISA. Strasbourg 15 March 2017.
Interview 11 2017. eu-LISA. Strasbourg 16 March 2017.
Interview 12 2017. Greek Police. Athens 22 March 2017.

[1] The first generation SIS was introduced in 1995 as a compensatory measure for risks that were expected to emerge after the progressive abolition of controls at the common borders of the Member States (see Brouwer 2008). The transition from the SIS to the SIS II was characterized by major delays. Indeed, though the SIS II was expected to go live in 2006, it did not become operational until 2013. It is beyond the scope of the article to analyse this transition phase, but it is worth highlighting that the reasons for the multiple setbacks were not just technical in nature. As Joanna Parkin (2011) explains, the manifold complications in the development and deployment of the SIS II were also linked to budgetary issues, criticisms related to its

fundamental rights implications, and the enduring struggles between the European Commission and a multiplicity of actors over the ownership and scope of the project.