

Security-as-service in the Management of European Border Data Infrastructures

Maguire, Eileen Murphy

Document Version
Final published version

Published in:
Journal of Common Market Studies

DOI:
[10.1111/jcms.13543](https://doi.org/10.1111/jcms.13543)

Publication date:
2024

License
CC BY-NC-ND

Citation for published version (APA):
Maguire, E. M. (2024). Security-as-service in the Management of European Border Data Infrastructures. *Journal of Common Market Studies*, 62(5), 1379-1394. <https://doi.org/10.1111/jcms.13543>

[Link to publication in CBS Research Portal](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

If you believe that this document breaches copyright please contact us (research.lib@cbs.dk) providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. Nov. 2024



Security-as-Service in the Management of European Border Data Infrastructures

EILEEN MURPHY MAGUIRE 

Copenhagen Business School, Copenhagen

Abstract

Today, large-scale IT systems play a central role in the management of European borders. These systems not only support and enable the management of mobility but also require expert management as complex data infrastructures. Drawing on fieldwork carried out at the headquarters of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), this article engages with growing calls to explore the politics of data infrastructure management. Focusing on the expert discourses and practices of eu-LISA, I show that, in line with a logic of service, it seeks to establish its legitimacy and authority as the manager of data infrastructures by sharing its expertise with its stakeholders. By attending to a logic of service, I show that the management of data infrastructures is neither exclusively depoliticising nor politicising; rather, it is often simultaneously both.

Keywords: (de)politicisation; data infrastructures; eu-LISA; expertise; service

Introduction

The contemporary border strives towards virtualisation, speed and efficiency (Bigo, 2014; Murphy and Maguire, 2015). However, many border crossers experience it as a space of violence and exclusion. In Europe, as elsewhere, the rise of data-led border management is often captured in the language and ideals of ‘smart borders’ (Amoore et al., 2008), prompting critical investigations of the forms of knowledge shaping contemporary practices of bordering. Recent work has focused on the central role large-scale IT systems play in the management of international mobility (Bellanova and Glouftsiou, 2022; Glouftsiou, 2021a; Leese, 2016). As data infrastructures, these systems support and enable the capture, storage, processing and exchange of data, in addition to supporting ‘the knowledge regimes that inform and shape migration policies, border regimes and migration management’ (Scheel et al., 2019, p. 579).

Extracting and exploiting the maximum value promised by such systems, frequently couched in terms of improved efficiencies and effectiveness, has become a priority for policy professionals and security experts (Amoore, 2006; Besters and Brom, 2010; Broeders and Hampshire, 2013; Carrera and Hernanz, 2015). These systems do occasionally fail (Glouftsiou, 2021b). As a result, ensuring their proper management has emerged as a priority area in European Union governance (European Commission, 2016). Perhaps one of the most important governance interventions in recent years is the establishment of eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

Established in 2011 as a means to improve the operational management of several large-scale IT systems, eu-LISA is responsible for multiple systems in various stages of

development and deployment [second-generation Schengen Information System (SIS II), Visa Information System (VIS), European Asylum Dactyloscopy Database (Eurodac), Entry/Exit System (EES), European Travel Information and Authorization System (ETIAS), European Criminal Records Information System – Third Country Nationals (ECRIS-TCN) and soon e-Justice Communication via Online Data Exchange (e-CODEX)]. It is also responsible for related initiatives, such as interoperability and data quality. Specifically, eu-LISA is tasked with ensuring the systems are available 24/7 to meet operational requirements, allowing the exchange of data between approved actors on issues of border crossings, visas and asylum applications. On-demand access to data stored in these systems and shared between actors has been framed as central to the successful implementation of asylum, border management and migration policies in the EU. Within critical security research, eu-LISA has been analysed as emblematic of the entry of new actors and forms of expertise, such as data management and IT systems operation, into the field of (in)security (see Bigo, 2020). Whilst this is true, it is also important to note that eu-LISA is a decentralised EU agency under DG Home. And eu-LISA's status as an EU agency strongly influences their scope of action and interaction with its key stakeholders – Member States, EU institutions and other EU agencies. As an EU agency, one of its key functions is the provision of expert advice on matters relating to its mandate. Thus, engaging with the politics of technocratic expertise is central to understanding the politics of contemporary data infrastructure management.

Over the last decade of critical security scholarship, a central question has emerged: how do expert technocratic discourses depoliticise matters such as migration and security, rendering them as mere technical matters of efficiency (see Amoore and de Goede, 2005)? In an effort to counter this official framing, researchers have sought to reveal the politics of security systems, and 'solutions', exploring the relationship between practices of expertise and power (Bigo, 2002; Leander, 2013; Walters, 2017). There is now a desire to expand analysis to include 'the mundane, but politically significant' (Glouftsiou, 2021b, p. 460) work of those involved in the management of data infrastructures. This requires that we ask larger questions. In this case, two pressing questions come to the fore: (1) if the management of data infrastructures is politically significant, what kind of politics does it signify, and (2) what does attending to the politics of managing data infrastructures mean for how processes of (in)security are performed and made sense of? I argue that the politics of data infrastructure management are located at the intersection of a logic of service and a logic of security, where matters of technocratic expertise, which are traditionally viewed as depoliticising under a logic of security, are highly politicised under a logic of service. Thus, this article explores a logic of service as the mode of managerial expertise informing the politics of data infrastructures.

Thus far, critical approaches to the study of security have paid little to no attention to the topic of service. The absence of critical research on service must be addressed, given that eu-LISA and similar actors define, understand and practise their work through a logic of service. Service is understood as political by these actors, but the political nature of service is not well understood in the social sciences. Under a logic of service value can only be co-created between the service provider and recipient. Central to this is the construction of value propositions or offerings that are evaluated by service beneficiaries in the context of their needs (Vargo and Lusch, 2008). For the co-creation of value to take place, the service offering must be accepted by the service recipient. As I will demonstrate,

eu-LISA seeks to establish the legitimacy and authority of its work and role through the construction of a particular value proposition: it is the actor best able to ensure the delivery of value from the use of IT systems to its stakeholders. In an effort to make concrete this proposition or claim, eu-LISA makes available its expertise in systems management to its stakeholders. This expertise is then evaluated by eu-LISA's stakeholders as part of ongoing negotiations and assessment of eu-LISA's claim that they are the actors best able to deliver value from the large-scale IT systems under their care.

In this sense, the sharing of expertise in systems management, practised through a logic of service, is neither simply politicising nor depoliticising but often simultaneously both. It is clear, then, that we must grapple with the logic of service as a key form of expertise in relation to which security practices are taking place. Today, then, the politics of security often presents itself in the form of service.

I. Note on Methodology

This article presents findings from a period of fieldwork carried out at the headquarters of eu-LISA, Tallinn Estonia, for 3 months in late 2018. Field site access was secured through a gatekeeper. During the fieldwork period, I took up the role of an eu-LISA intern, reviewing the Agency's then research and technology monitoring function. This unique position was key to how the research process unfolded, as I occupied the dual role of both an insider (as an eu-LISA intern) and an outsider (as a PhD researcher). This dual role strongly shaped my research relations, as my positionality moved along the continuum of insider/outsider (see Mikecz, 2012).

Positionality is an issue of not only how we situate ourselves during our research encounters and relations but also how we situate our research in relation to the wider objectives of the discipline (Salter and Mutlu, 2013, p. 15). This issue has been taken up in relation to the challenges and benefits of collaboration and engagement (see De Goede, 2020). In the case of my own research, I have sought to take seriously the hesitations my counterparts have in making sense of eu-LISA's work and role as a security organisation, preferring instead to think of their work and role in terms of service. I argue that attending to this distinction, and the ways in which it is maintained, provides a means to better understand how the practices and relations of actors within the field of (in)security unfold and develop. Such a position reflects the productive tension Montesinos Coleman and Rosenow (2016, p. 205) identify between proximity and distance, where 'engagement with practice – being "in the field" – can force us to gain distance from the concepts, categories, and problems through which the field asks us to interpret practice'. It was only by engaging with the practices of my counterparts and by taking seriously their efforts to distinguish their sense of their work and role from that of the professionals of (in)security that I was able to identify the importance of a logic of service.

During fieldwork, online and in-person expert interviews (see Bogner and Menz, 2009) were carried out with eu-LISA members of staff. This included staff from the headquarters, liaison office and operational site. Interviews were recorded with consent. In addition, analysis of key documents was carried out (see Bowen, 2009), focusing primarily on eu-LISA annual activity reports, strategy reports and single programming documents. These reports offer insight into the formal priorities, strategies and practices of eu-LISA. In this sense, documents were analysed as supplementary research data, adding further

insights into the issue of service as it emerged in the interviews. Following fieldwork, and in line with best practice, transcripts of the interviews were returned to participants for review. Final transcripts were analysed using thematic analysis (see Braun and Clarke, 2006). This analysis revealed a consistent understanding that eu-LISA's role is determined in the context of its stakeholder relations and that such relations are best characterised in terms of a logic of service. However, the reality of how service is practised reveals differing understanding of what kind of value eu-LISA should offer, to whom and how, as different and differing stakeholder demands are addressed by different Agency departments and sites. In this sense, the co-creation and delivery of value is not a pre-set process but rather one that is constantly being debated, negotiated and redefined within the context of stakeholder relations and, in this specific case, the practice of providing expertise.

As the focus of the fieldwork was on exploring how eu-LISA understands its work and role in relation to the field of European border security and migration management, service was not a pre-established category. Rather, it emerged inductively from the analysis of the data, as participants simultaneously countered a characterisation of their work in terms of security and focused instead on both their expertise in managing IT systems and the support they provide to their stakeholders by leveraging the role of IT systems. The identification of a logic of service as central to how my expert counterparts make sense of their work focused my attention on the relationship between security and service, with a particular focus on the tensions it brought to the fore, in this case, the simultaneously depoliticising and repoliticising function of providing expertise on the management of data infrastructures.

II. A Critical Theory of Service

Critical Security Studies literature has highlighted the central role technology and data-driven solutions play in border security and migration management (see Andersson, 2016; Guittet and Jeandesboz, 2010; Salter, 2004). At the same time, this research has also warned of the risks of technological determinism (Davidshofer et al., 2016), arguing for the need to explore how digital technologies intersect with social, political and economic forces to 'reconfigure the rationales, techniques and practices of border security and migration management' (Glouftsiou and Scheel, 2021, p. 124). More specifically, Bellanova and Glouftsiou (2022, p. 179) have argued that 'the pressing question 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'. Whilst research has highlighted the need to better understand the practices of managing data infrastructures, empirical accounts of the logics and rationales that support and enable this work are lacking (Glouftsiou and Scheel, 2021). I argue that service is a key rationale through which data infrastructures are managed and governed. To do so, I start by critically evaluating Service Science as a body of expert knowledge central to the management of IT systems.

Service Science is a transdisciplinary body of knowledge dedicated to the study of service systems and systematic service innovation. Service systems are 'value-co-creation configurations of people, technology, value propositions connecting internal and external

service systems, and shared information' (Maglio and Spohrer, 2008, p. 18). Such service systems include IT systems and their management. Indeed, the development of Service Science, in its current disciplinary form, is intimately linked to developments in ICT (Chesbrough and Spohrer, 2006). For example, on a page titled the 'invention of service science', the well-known multinational corporation IBM (International Business Machines) reflects on the beginning of Service Science as a response to their need for staff knowledgeable across computer science, engineering, management and social science to support the growing role of service in IBM's business model.¹ With the support of IBM, Service Science has, over the last two decades, been established as a recognised field of study across universities worldwide. In this sense, the expert literature on service has developed in relation to wider efforts to establish professional practices of service.

Drawing on Vargo and Lusch's (2004) theory of service dominant logic, Service Science defines service as 'the application of specialized competences (knowledge and skills) through deeds, processes and performances for the benefit of another entity or the entity itself' (p. 2). Under a logic of service value is co-created between the service provider and beneficiary. Co-creation take place within the context of the specific needs and objectives of the service beneficiary (value-in-use). Reflecting on the intimacy between data and predictive security practices, Bigo and Bonelli (2019, p. 103) have argued that this relationship is not inherent to the nature of data enabling technologies but rather 'depends on power struggles between actors who determine the use and exchange value of digital data. ... Moreover, the symbolic value of intelligence data depends less on its content – despite the ideology of secrecy that sanctifies this content – than it does on who produced it, in what context, and for what reason'. As service providers cannot create value alone, understanding these matters – the how and why data are produced, by whom and under what circumstances – is at the centre of managing data infrastructures under a logic of service.

Attending to a logic of service provides a means to engage with how service providers seek to co-create value within the process of managing data infrastructures. As value is argued to be determined in the context of service users' needs, service providers seek to construct value propositions, that is, value offerings, which they believe users will assess favourably. However, constructing and communicating value propositions is complex, as they are often subject to negotiation, amendment and refusal by service beneficiaries (see Ballantyne and Varey, 2006). Value propositions not only detail value offerings to service beneficiaries but also reflect how service providers want their own work to be valued (see Corvellec and Hultman, 2014). I argue that eu-LISA is engaged in the process of constructing and communicating a particular value proposition: it is the actor best able to ensure the delivery of value from the use of IT systems to its stakeholders. The acceptance of this, by its stakeholders, aids in establishing the legitimacy and authority of its role as a 'trusted' service provider (see Hudson, 2006). In an effort to make concrete this proposition or claim, eu-LISA makes available its expertise in systems management to its stakeholders.

Critiques of service research have highlighted its apolitical account of value, arguing that it fails to grapple with the inequalities of exchange relations in a capitalist market (see Hietanen et al., 2018). Indeed, today, there is much discussion of value co-destruction as a corrective to the optimism of earlier accounts of value co-creation

¹<https://www.ibm.com/ibm/history/ibm100/us/en/icons/servicescience/>.

(Echeverri and Skålen, 2011; Laamanen and Skålén, 2015; Plé and Chumpitaz Cáceres, 2010). Within the expert literature on service, then, we see a need to develop a critical perspective, which I aim to begin here, as I explore how a logic of service brings with it its own form of politics, countering a depoliticised view of technocratic expertise.

Eu-LISA's efforts to communicate how they want their work and role to be valued, through the making available of their expertise, must be situated within the wider context in which eu-LISA's work takes place, that of an EU agency. The public administration literature has noted the rise of the agency model of governance, often described in terms of 'agencification' (Moynihan, 2006). This research has sought to understand where agencies sit in the administrative space, exploring the levels of governance they are accountable to, that is, Member State and/or EU level (Egeberg and Trondal, 2017; Lord, 2011). Further work has explored the expanding power and role of agencies as they take on 'quasi-rule making' roles through drafting and setting standards (Moloney, 2016; Trondal, 2010). Central to this is the role of technocratic expertise. Scipioni (2018, p. 769) has described the tasks EU agencies should perform as those 'related to gathering information and providing technical expertise'. Similarly, Schneider and Nieswandt (2018, p. 13) have argued that EU agency staff are 'united in a shared belief in disinterested, apolitical bureaucratic rules of procedure, based on a notion of "expertise" that transcends national boundaries and supersedes national concerns'. Thus, the provision of depoliticised expertise is a defining feature of the work and role of an EU agency and is central to how EU agencies seek to establish and maintain their authority and legitimacy (see Boswell, 2008; Fjørtoft, 2022; Parkin, 2012). However, the field of (in)security is marked by a reluctance to yield power to European Union institutions (Busuioc, 2016). The contested relations of Member States and European institutions, under the principle of subsidiarity, are mirrored in the dynamics of service provider and service recipient competitions. For example, Sampson (2010, p. 127) has reflected on the tensions of service relationships in what he describes as the 'customer-as-competitor' issue:

Customers are themselves the chief competitors for many services. Service providers sometimes need to convince do-it-yourself customers that they would be better off using the service provider. ... Customers have the advantage of owning and controlling their inputs, and may have the advantage of increased levels of customization (getting it exactly how they want it). Service providers, on the other hand, usually have advantages of economies of scale and expertise.

It is within this competitive and political landscape that eu-LISA must operate and persuade its stakeholders to trust in its expertise, legitimising its work and role as Europe's foremost IT service provider (Perkowski, 2019).

Extant research has explored the role of technocratic expertise in policy-making (Weingart, 1999). This work has highlighted the central role technical expertise play in defining and legitimising the problems policies are intended to address (Radaelli, 1999). In doing so, it has demonstrated the challenges of drawing firm distinctions between technical and political work (Winzen, 2011). Critical Security Studies research has argued that the prioritisation of technocratic expertise results in the depoliticisation of security practices. The C.A.S.E. Collective (2006, p. 476) describes depoliticisation as 'naturalized correspondences between things and words, between processes framed as problems and

ready-made solutions'. Thus, to think of issues in terms of depoliticisation is to think in terms of agreement and consensus concerning the role of technical solutions for security problems, as technocratic expertise forecloses or reduces the space to discuss the societal impacts of security measures and technical solutions (Bigo, 2020). For example, Trauttmansdorff (2022) has analysed the role technical authority and expertise play in developing consensus on migration policies, such as interoperability. In order to counter this effect, critical research has sought to foreground the politics of security technologies and data practices (see Jeandesboz, 2016; Leese et al., 2022; Scheel et al., 2019). This work has brought with it a growing concern with where we focus our analytical attentions in order to locate the politics of European security and border management (see Jeandesboz, 2017). One proposed solution is to think in terms of the politics of infrastructures, as the structures through which the regulation of data practices is increasingly taking place (Bellanova and de Goede, 2021).

Reflecting on the implicit politics of infrastructure networks, Folkers (2017, p. 856, emphasis in original) has argued for the importance of attending to 'the historically specific ways in which these matters *become* politicized and depoliticized'. Similarly, Hagmann et al. (2018, p. 5) have argued that 'instead of looking at security as closure, we propose an understanding of security as a field of political activity occupied by diverse actors mobilised in different kinds of struggles, and in which political conflicts can shift across arenas. Seen this way, political closure might be one possible outcome, but it should not simply be presumed and taken for granted'. Such an approach requires that we attend to 'the varied forms and modes of politics that increasingly emerge in and around security' (Hagmann et al., 2018, p. 5). Thus, EU agencies are a key arena in which the politics of infrastructures are taking place, under a mode of service.

Where issues of technocratic expertise and styles of management have often been analysed as depoliticising, I argue that the specific mode of management at play brings to the fore a politics of its own kind, a politics of service. Whilst the role of digital technologies presented as solutions to security challenges may no longer subject to meaningful political disagreement, the delivery of value from these technologies very much is. In this sense, a logic of service is increasingly emerging as the language through which matters of security are being debated and contested and defined. But as of yet, critical security research has not developed a critical stance on service. Hereafter, I will delve into the work of eu-LISA in greater detail to appreciate the significance of the logic of service for one of Europe's key border management agencies. In doing so, I demonstrate that practices of providing expertise, under a logic of service, are neither exclusively depoliticising nor politicising; indeed, they are often simultaneously both.

III. A Management Authority for Large-Scale IT Systems

[T]he primary objective of eu-LISA is 24/7 service to the Member States, that's our mission. ... The point is that to fulfil our mission you need to have people that are committed, that they work hard 24 hours a day, seven days a week and they try to keep the situation under control and make sure the systems work. (Interview No. 5, with senior eu-LISA staff member, 2018)

Prior to the establishment of eu-LISA, the operational management of large-scale IT systems was carried out directly by the European Commission in combination with

France and Austria. In the process of adopting the SIS II and the VIS, the Council and the Parliament invited the Commission to submit proposals for the setting up of a long-term management authority for large-scale IT systems. An impact assessment compared five options against operational, governance, legal and financial criteria. From these options, the choice of a new regulatory agency was deemed favourable. The need to set up a management authority for large-scale IT systems was framed in terms of the challenges of expert systems management and governance, focusing in particular on the practical requirements and demands of maintaining the systems, as it was argued that ‘the systems cannot function without a long-term central Management Authority to ensure continuity and operational management of the systems, and the permanent flow of data’ (European Commission, 2009, p. 10). The impact assessment goes on to state that ‘a dedicated, specialised organisation would also ensure the highest level of efficiency and responsiveness to the requirements of Member States and other stakeholders’ (European Commission, 2009, p. 14). Thus, matters of efficiency and effectiveness were prioritised in the impact assessment, framing the setting up of a management authority, and the choice of a regulatory agency, as a depoliticised, technical matter. This depoliticised framing of the management of the systems is further reflected in the following description distinguishing between the impacts of the systems and the impact of the authority responsible for their management:

It is the existence of the systems themselves that may have economic, environmental and, most of all, social impacts. The establishment of the Authority that would manage the systems is not likely to produce any additional significant impacts under these categories. All the systems have an impact on problems such as crime, terrorism, security, and fundamental rights. However, their mode of management will not be a differentiating factor between the scales of these impacts. (European Commission, 2009, p. 19)

However, as extant critical security research has shown, the ‘mode of management’ and forms of managerial expertise at play in data infrastructures is a profoundly political matter. For example, Tsianos and Kuster (2016, p. 239) have argued in relation to the potential for systems interoperability that ‘it is only the set-up of the legal and institutional form of EU-LISA [sic] as an agency that provided the possibility to build a common open and flexible database architecture’. I argue that the mode of management eu-LISA employs is one of service, and it is within a logic of service that the politics of data infrastructure management can be found.

In the years since its formal establishment, eu-LISA has worked hard to communicate to its stakeholders its role in the field. Through their website, social media posts, official documents and publications, along with various presentations at conferences and events, they are engaged in near-constant communication of their work and the role they play in European (in)security and border management. For example, their biannual newsletter, ‘The eu-LISA Bits & Bytes’,² provides updates on the progress of their work. A new ‘awareness package’ has been launched, which serves as a ‘one-stop shop’ containing ‘everything you need to know about the various activities of eu-LISA’.³ And, most recently, they received ‘a Forbes Social Award for its innovative and inspirational initiatives in the

²Available at <https://eulisa.europa.eu/SiteAssets/Bits-and-Bytes/toc.aspx> (accessed 17 July 2022).

³Available at <https://www.eulisa.europa.eu/our-publications/information-material?RID=28&LID={9b47a889-222a-49cc-9a04-7ecc81cf4ab9}.https://www.eulisa.europa.eu/SiteAssets/Discover/default.aspx#/> (accessed 17 July 2022).

field of public communication'.⁴ Within these communication practices, descriptions of eu-LISA's mission, such as the one below, are commonplace across their website and official publications and reports:

The Agency's mission is based on its legal mandate and focuses on *continuously adding value for Member States by supporting through technology their efforts for a safer Europe*. This mission is delivered through the Agency's vision, which is to *provide high-quality and efficient services and solutions to stakeholders, to earn their trust through continuously aligning technology capabilities with the evolving needs of Member States and to grow the Agency as a centre of excellence* in the Justice and Home Affairs (JHA) domain. (eu-LISA, 2018, p. 11, emphasis in original)

Such statements are reflective of a logic of service (Vargo and Lusch, 2004), as eu-LISA applies its skills and knowledge to 'continuously add value for Member States'. In addition, this description reflects one of eu-LISA's core value propositions; that is, it is the actor best able to deliver value from the systems under its care. This proposition is further reflected in the Agency's strategic vision, where it has explicitly set out the goal to earn the trust of their stakeholders by making available their expertise.

Since its founding, eu-LISA has published three strategic documents (eu-LISA, 2014, 2017, 2021), outlining the Agency's goals. In these reports, they outline their intention to establish themselves as an acknowledged ICT centre of excellence and service provider (see eu-LISA, 2014, 2017, 2021), where 'as the principal ICT service provider in the Justice and Home Affairs domain and based on its expertise and capabilities, eu-LISA will continue its work on building and consolidating its role as a centre of excellence. The Agency will continue to provide its advice and assistance to the European Institutions, the Member States and other EU Agencies as needed' (eu-LISA, 2021, p. 10). Where the status of the strategic goals of the Agency have evolved over time, their focus has remained relatively consistent: delivering value and benefit to their stakeholders based on their expertise. This approach to the organisation of their work, or mode of management, aligns with a logic of service, as eu-LISA has worked hard to establish the legitimacy of its expertise in order to justify its role as the rightful manager of the systems. Reflecting on this issue, one interviewee explained the value of having a 'dedicated IT agency' thus:

[T]he Agency has, by now, a considerable experience in the management of large-scale IT systems, containing sensitive and personal data and ensuring the implementation of data protection and security regulations. The point is that you know the Commission was, of course, fine in the running of IT systems but we are, quality-wise, better because we are like a dedicated IT agency while Commission is not an IT body; Commission is an executive body implementing agency, institution, proposing institution. They are not – Commission cannot be an implementing agency in a very efficient form. So, I would say that there is a quality increase from bringing those officials, desk officers, managing contracts, you know, IT contracts, to bringing all this work to an agency who is then really dedicated. So, let's say that that is the point of this experience, that our agency has a very good experience by now and we have a good streamlined approach, how to manage IT systems. So that's a quality in itself. And the fact that we deal with a lot of sensitive data, that's a huge challenge and we are good, really we are good. (Interview No. 35, 2018)

⁴Available at <https://www.eulisa.europa.eu/Newsroom/News/Pages/eu-LISA-awarded-for-innovative-public-communication.aspx> (accessed 27 November 2022).

As my interviewee explains, the degree of expertise and experience that comes with a ‘dedicated IT agency’ is a ‘quality in itself’ that should be acknowledged. However, the value of this work must always be demonstrated and cannot be taken for granted. The value of eu-LISA’s expertise is contextually determined by its efforts to meet the needs of its stakeholders. The interviewee went on to note this dynamic as they compared the model of centralised IT systems management under the control of an EU agency with the current set-up for systems in customs:

For example, in the customs domain, that’s what we were explained on Tuesday, they are very afraid that if they go to a centralised IT systems model for, let’s say, most of the customs databases, then they lose control but our point was that they wouldn’t because the management board is very closely supervising the work of the agency, so they wouldn’t. Now, they are very much dependent on those voluntary Member States and, secondly, who are running their IT systems, and, secondly, they are very dependent on the Commission. And, you know, they feel that the Commission officials are making their decisions. ... Maybe it’s a perception but that’s what they feel and maybe there are some factual bases for that. ... So, we try to explain them the model that it is not taking away their power, in fact, it is doing everything together because we have to report all the time what we are doing. And in addition to that management boards and advisory groups, we have *ad hoc* groups and, you know, any topic basically that Member States want to – where they want to control us or steer our work, they can call an *ad hoc* group and they have done so and then we meet with them and we explain what we do. So, there is a lot of interaction and this I think the customs people just haven’t really understood and they’re afraid that somebody in the Commission will do the decisions but in the agency model, it’s not the agency staff does it; we do it jointly. (Interview No. 35, 2018)

Under the agency model, eu-LISA makes available its expertise to its stakeholders as part of joint efforts to plan the management of the systems. Thus, to think in terms of service is to reflect on the particular mode of management eu-LISA enacts in its role as the operational managers of large-scale IT systems. In this sense, service acts as a logic setting the conditions for the possibility of knowledge on both the systems and the use of the systems. It also draws our attention to how security emerges within the politics of service. Specifically, in the management of large-scale IT systems, service legitimises, values and provides the grounds upon which contestation takes place. It is on these grounds that contemporary security is debated, although it is not often named as such in those debates, as matters of security are translated into debates on how the value of IT systems is determined.

One interviewee reflected on this issue, as they explained how they manage stakeholder relations and any potential challenges to the Agency’s authority during advisory groups:

First of all, I’m marketing eu-LISA, to demonstrate how we do things. So, I promote the methods and the work and what is therefore behind delivering a specific product, or a specific deliverable. So, in fact, I sell. I market the Agency itself. If I mess up, it has the opposite effect. At the same time, I defend the Agency, but I defend also the stakeholders because they have needs and they need me to properly pass the message internally on the business need and to convince other stakeholders on what is behind that need. ... What I try to do is again work on those three pillars. If you sell knowledge, you inspire trust. If you sell a vision comprising of those three pillars, you inspire

confidence. Also, I think a key element, when they trust you they are open to you. Of course, governments, they play their own cards, and delegates, stakeholders, they have their own agenda to follow. The key success factor here is indeed to, somehow, make them believe to the common goal. For sure, they will follow their agenda, I am not there to change it, but I am there to adapt it. So, it means I do comply with what they want, but they also comply with what I want. So, it's somewhere in between the whole thing. (Interview No. 4, 2018)

The process of establishing eu-LISA as the actor best able to deliver value from the management of IT systems is not spontaneous and without its challenges, expounded by what is at stake in their work. In this sense, as my interviewee goes on to note, 'stakeholder management is maybe the most challenging one in this respect, because what we have to do here will occur for the very first time in the European IT history and maybe globally' (Interview No. 4, 2018). In this sense, eu-LISA's ability to fulfil the proposition that it is the actor best able to deliver value from the management of the system is determined in the context of its stakeholders' needs. Thus, a logic of service not only shapes eu-LISA's understanding of its role and relations to its stakeholders but also provides a framework through which the Agency's stakeholders can make claims and demands to the Agency. For example, one interviewee discussed the challenges of finding solutions to accommodate the requests of Member States, whilst also ensuring that the Agency acts within its legal remit and mandate, as they explained, 'it's not that we don't want to do, it's quite the opposite, we really want to help the Member States, but on the other side, we have some legal constraints that we need to respect' (Interview No. 11, 2018). Thus, the co-creation of value plays out in the context of competing demands of accountability.

Central here is the notion of trust between eu-LISA and its stakeholders as a means of mediating the politics of different agendas. This trust, as my interviewee explains, is intimately linked to the knowledge and expertise of the Agency. In this sense, eu-LISA staff are keenly aware of the politics of their own expertise, as the role of trust is important not only in relation to the progress of delivering specific projects and deliverables but also in relation to the development of the Agency itself (see Busuioc and Groenleer, 2013). Another interviewee, further reflecting on the importance of trust in the Agency, noted that:

[L]ooking at the new mandate it seems like we've gained trust during those first five years. So, people have started to entrust us with even more interesting tasks, and that is what is very well reflected in the mandate. I don't see any, not even a single point, not even a hint of an idea of taking away from the Agency, saying 'well, this maybe you didn't do that well, so maybe we'll find somebody else to do that'. Quite to the contrary, it is clearly spelled out if you read the changes that everybody seems to be pretty happy with what we did with what we have. And, feels like if they give us the necessary resources that we can do even more and even better with the new tools that they defined in the new regulation. (Interview No. 3, 2018)

Establishing the legitimacy and authority of their role as the manager of the large-scale IT systems under their purview has been central to the way in which eu-LISA has carried out its responsibilities. In this sense, eu-LISA is intimately aware of the politics of their work. But rather than a politics of security, theirs is a politics of service.

Conclusions

This article has sought to address a notable gap in how we understand the (de)politicisation of security processes. In order to do so, I have highlighted the role played by a logic of service. Under a logic of service that which would typically be considered as depoliticising, the form of expertise supporting the management of large-scale IT systems, and the practice of providing this expertise, is in fact highly politicised. I argue that attention to and understanding of a logic of service is therefore important for the study of security for a number of reasons.

In the case of eu-LISA, service is the framework through which they make sense of their role in the wider field of border security and migration management. If we are to understand the ways in which actors make sense of security, we must consider the forms of practical knowledge that key actors draw on as both part of their day-to-day work and also how they organise their approach to this work.

Furthermore, attention to service offers a new relation in which to explore the boundaries of (in)security. Mapping out the lines along which the politicisation of service and (de)politicisation of security intersect and diverge adds further empirical depth and nuance to our effort to study (in)security. For example, in this article, I have demonstrated that rather than a clear-cut depoliticisation of security practices and a politicisation of services, what we find is a constant shifting back and forth between depoliticisation and politicisation, often occurring at the same time, as multiple logics (both security and service) are at play in how eu-LISA seeks to establish its legitimacy and authority. I argue that it is within a logic of service that the politics of many security practices and relations are now taking shape and being played out.

Attending to service provides a way to reintroduce politics into analysis of power relations. Where matters of technical discussions can often appear as depoliticised, a focus on how value is defined, constructed, consumed and circulated can help to reveal where the tensions and frictions of these developments lie. The issue of value is increasingly central to how data infrastructures are conceptualised and operationalised; thus, service frameworks are constantly under evolution, structuring the working practices and professional bodies of knowledge and relations of key actors. The account I have developed here offers but one telling of how a logic of service intersects with a logic of security. However, the notion of service is manifold, as it is defined within the context of situated sociotechnical relations, which must be addressed within our studies of (in)security.

Acknowledgements

The author would like to specifically thank the EU agency eu-LISA for hosting me during the fulfilment of the work, and for granting permission to access the data used in the analysis. I am especially grateful to my counterparts for sharing their time and expertise with me.

Correspondence:

Eileen Murphy Maguire, Copenhagen Business School, Copenhagen, Denmark.
email: irisheileen@gmail.com

References

- Amoore, L. (2006) 'Biometric Borders: Governing Mobility in the War on Terror'. *Political Geography*, Vol. 25, No. 3, pp. 336–351.
- Amoore, L. and de Goede, M. (2005) 'Governance, Risk and Dataveillance in the War on Terror'. *Crime, Law & Social Change*, Vol. 43, No. 2–3, pp. 149–173.
- Amoore, L., Marmura, S. and Salter, M.B. (2008) 'Smart Borders and Mobilities: Spaces, Zones, Enclosures'. *Surveillance & Society*, Vol. 5, No. 2, pp. 96–101.
- Andersson, R. (2016) 'Hardwiring the Frontier? The Politics of Security Technology in Europe's 'Fight Against Illegal Migration''. *Security Dialogue*, Vol. 47, No. 1, pp. 22–39.
- Ballantyne, D. and Varey, R.J. (2006) 'Creating Value-in-Use Through Marketing Interaction: The Exchange Logic of Relating, Communicating and Knowing'. *Marketing Theory*, Vol. 6, No. 3, pp. 335–348.
- Bellanova, R. and de Goede, M. (2021) 'Co-producing Security: Platform Content Moderation and European Security Integration'. *Journal of Common Market Studies*, Vol. 60, No. 5, pp. 1316–1334.
- Bellanova, R. and Glouftsiou, G. (2022) 'Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance'. *Geopolitics*, Vol. 27, No. 1, pp. 160–184.
- Besters, M. and Brom, F.W.A. (2010) 'Greedy' Information Technology: The Digitalization of the European Migration Policy'. *European Journal of Migration and Law*, Vol. 12, No. 4, pp. 455–470.
- Bigo, D. (2002) 'Security and Immigration: Toward a Critique of the Governmentality of Unease'. *Alternatives: Global, Local, Political*, Vol. 27, No. February, pp. 63–92.
- Bigo, D. (2014) 'The (in)Securitization Practices of the Three Universes of EU Border Control: Military/Navy – Border Guards/Police – Database Analysts'. *Security Dialogue*, Vol. 45, No. 3, pp. 209–225.
- Bigo, D. (2020) 'The Socio-genesis of a Guild of 'Digital Technologies' Justifying Transnational Interoperable Databases in the Name of Security and Border Purposes: A Reframing of the Field of Security Professionals?' *International Journal Migration and Border Studies*, Vol. 6, No. 1/2, pp. 74–92.
- Bigo, D. and Bonelli, L. (2019) 'Digital Data and the Transnational Intelligence Space'. In Bigo, D., Isin, E. and Ruppert, E. (eds) *Data Politics Worlds, Subjects, Rights* (Abingdon: Routledge), pp. 100–122.
- Bogner, A. and Menz, W. (2009) 'The Theory-Generating Expert Interview: Epistemological Interest, Forms of Knowledge, Interaction'. In Bogner, A., Littig, B. and Menz, W. (eds) *Interviewing Experts* (London: Palgrave Macmillan), pp. 43–80.
- Boswell, C. (2008) 'The Political Functions of Expert Knowledge: Knowledge and Legitimation in European Union Immigration Policy'. *Journal of European Public Policy*, Vol. 15, No. 4, pp. 471–488.
- Bowen, G.A. (2009) 'Document Analysis as a Qualitative Research Method'. *Qualitative Research Journal*, Vol. 9, No. 2, pp. 27–40.
- Braun, V. and Clarke, V. (2006) 'Using Thematic Analysis in Psychology'. *Qualitative Research in Psychology*, Vol. 3, No. 2, pp. 77–101.
- Broeders, D. and Hampshire, J. (2013) 'Dreaming of Seamless Borders: ICTs and the Pre-emptive Governance of Mobility in Europe'. *Journal of Ethic and Migration Studies*, Vol. 39, No. 8, pp. 1201–1218.
- Busuioc, M. (2016) 'Friend or Foe? Inter-Agency Cooperation, Organizational Reputation and Turf'. *Public Administration*, Vol. 94, No. 1, pp. 40–56.

- Busuioc, M. and Groenleer, M. (2013) 'Beyond Design: The Evolution of Europol and Eurojust'. *Perspectives on European Politics and Society*, Vol. 14, No. 3, pp. 285–304.
- Carrera, S. and Hernanz, N. (2015) 'Re-framing Mobility and Identity Controls: The Next Generation of the EU Migration Management Toolkit'. *Journal of Borderlands Studies*, Vol. 30, No. 1, pp. 69–84.
- Chesbrough, H. and Spohrer, J. (2006) 'A Research Manifesto for Service Science'. *Communications of the ACM*, Vol. 49, No. 7, pp. 35–40.
- Collective, C.A.S.E. (2006) 'Critical Approaches to Security in Europe: A Networked Manifesto'. *Security Dialogue*, Vol. 37, No. 4, pp. 443–487.
- Corvellec, H. and Hultman, J. (2014) 'Managing the Politics of Value Propositions'. *Marketing Theory*, Vol. 14, No. 4, pp. 355–375.
- Davidshofer, S., Jeandesboz, J. and Ragazzi, F. (2016) 'Technology and Security Practices: Situating the Technological Imperative'. In Basaran, T., Bigo, D., Guittet, E. and Walker, R.B.J. (eds) *International Political Sociology* (London: Routledge), pp. 205–227.
- De Goede, M. (2020) 'Engagement All the Way Down'. *Critical Studies on Security*, Vol. 8, No. 2, pp. 101–115.
- Echeverri, P. and Skålen, P. (2011) 'Co-creation and Co-destruction: A Practice-Theory Based Study of Interactive Value Formation'. *Marketing Theory*, Vol. 11, No. 3, pp. 351–373.
- Egeberg, M. and Trondal, J. (2017) 'Researching European Union Agencies: What Have We Learned (and Where Do We Go From Here)?'. *Journal of Common Market Studies*, Vol. 55, No. 4, pp. 675–690.
- eu-LISA. (2014) eu-LISA Strategy 2014–2020. Available at: <https://www.eulisa.europa.eu/Publications/Corporate/EL0114595ENC.pdf> [Accessed 17th July 2022].
- eu-LISA. (2017) eu-LISA Strategy 2018–2022. Available at: <https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Strategy%202018-2022.pdf> [Accessed 17th July 2022].
- eu-LISA. (2018) eu-LISA Single Programming Document 2020–2022. Available at: <https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Single%20Programming%20Document%20%202020-2022.pdf> [Accessed 17th July 2022].
- eu-LISA. (2021) eu-LISA Strategy 2021–2027. Available at: <https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Strategy%202021-2027.pdf> [Accessed 17th July 2022].
- European Commission. (2009) Commission staff working document *accompanying document to the proposal for a regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a COUNCIL DECISION conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty IMPACT ASSESSMENT*. SEC (2009) 837.
- European Commission. (2016) *Communication From the Commission to the European Parliament and the Council. Stronger and Smarter Information Systems for Borders and Security*. COM (2016) 205 Final.
- Fjørtoft, T.N. (2022) 'More Power, More Control: The Legitimizing Role of Expertise in Frontex After the Refugee Crisis'. *Regulation & Governance*, Vol. 16, No. 2, pp. 557–571.
- Folkers, A. (2017) 'Existential Provisions: The Technopolitics of Public Infrastructure'. *Environment and Planning D: Society and Space*, Vol. 35, No. 5, pp. 855–874.
- Glouftsiou, G. (2021a) *Engineering Digitised Borders. Designing and Managing the Visa Information System*. (Singapore: Palgrave Macmillan).
- Glouftsiou, G. (2021b) 'Governing Border Security Infrastructures: Maintaining Large-Scale Information Systems'. *Security Dialogue*, Vol. 52, No. 5, pp. 452–470.
- Glouftsiou, G. and Scheel, S. (2021) 'An Inquiry Into the Digitisation of Border and Migration Management: Performativity, Contestation and Heterogeneous Engineering'. *Third World Quarterly*, Vol. 42, No. 1, pp. 123–140.

- Guittet, E. and Jeandesboz, J. (2010) 'Security Technologies'. In Burgess, P. (ed.) *The Routledge Handbook of New Security Studies*. (London and New York: Routledge), pp. 229–239.
- Hagmann, J., Hegemann, H. and Neal, A. (2018) 'The Politicisation of Security'. *European Review of International Studies*, Vol. 5, No. 3, pp. 3–29.
- Hietanen, J., Andéhn, M. and Bradshaw, A. (2018) 'Against the Implicit Politics of Service-Dominant Logic'. *Marketing Theory*, Vol. 18, No. 1, pp. 101–119.
- Hudson, J. (2006) 'Institutional Trust and Subjective Well-Being Across the EU'. *Kyklos*, Vol. 59, No. 1, pp. 43–62.
- Jeandesboz, J. (2016) 'Smartening Border Security in the European Union: An Associational Inquiry'. *Security Dialogue*, Vol. 47, No. 4, pp. 292–309.
- Jeandesboz, J. (2017) 'European Border Policing: EUROSUR, Knowledge, Calculation'. *Global Crime*, Vol. 18, No. 3, pp. 256–285.
- Laamanen, M. and Skålén, P. (2015) 'Collective-Conflictual Value Co-creation: A Strategic Action Field Approach'. *Marketing Theory*, Vol. 15, No. 3, pp. 381–400.
- Leander, A. (2013) 'Technological Agency in the Co-constitution of Legal Expertise and the US Drone Program'. *Leiden Journal of International Law*, Vol. 26, No. 4, pp. 811–831.
- Leese, M. (2016) 'Exploring the Security/Facilitation Nexus: Foucault as the 'Smart' Border'. *Global Society*, Vol. 30, No. 3, pp. 412–429.
- Leese, M., Noori, S. and Scheel, S. (2022) 'Data Matters: The Politics and Practices of Digital Border and Migration Management'. *Geopolitics*, Vol. 27, No. 1, pp. 5–25.
- Lord, C. (2011) 'The European Parliament and the Legitimation of Agencification'. *Journal of European Public Policy*, Vol. 18, No. 6, pp. 909–925.
- Maglio, P.P. and Spohrer, J. (2008) 'Fundamentals of Service Science'. *Journal of the Academy of Marketing Science*, Vol. 36, No. 1, pp. 18–20.
- Mikecz, R. (2012) 'Interviewing Elites: Addressing Methodological Issues'. *Qualitative Inquiry*, Vol. 18, No. 6, pp. 482–493.
- Moloney, N. (2016) 'International Financial Governance, the EU, and Brexit: The 'Agencification' of EU Financial Governance and the Implications'. *European Business Organization Law Review*, Vol. 17, No. 4, pp. 451–480.
- Montesinos Coleman, L. and Rosenow, D. (2016) 'Security (Studies) and the Limits of Critique: Why We Should Think Through Struggle'. *Critical Studies on Security*, Vol. 4, No. 2, pp. 202–220.
- Moynihan, D. (2006) 'Ambiguity in Policy Lessons: The Agencification Process'. *Public Administration*, Vol. 84, No. 4, pp. 1029–1050.
- Murphy, E. and Maguire, M. (2015) 'Speed, Time and Security Anthropological Perspectives in Automated Border Control'. *Ethnofoor Anthropological Journal*, Vol. 27, No. 2, pp. 157–178.
- Parkin, J. (2012) *EU Home Affairs Agencies and the Construction of EU Internal Security (CEPS Paper in Liberty and Security in Europe)*. Available at: <https://www.ceps.eu/ceps-publications/eu-home-affairs-agencies-and-construction-eu-internal-security/> [Accessed 25th October 2022].
- Perkowski, N. (2019) "'There Are Voices in Every Direction': Organizational Decoupling in Frontex'. *Journal of Common Market Studies*, Vol. 57, No. 5, pp. 1182–1199.
- Plé, L. and Chumpitaz Cáceres, R. (2010) 'Not Always Co-creation: Introducing Interactional Co-destruction of Value in Service-Dominant Logic'. *Journal of Services Marketing*, Vol. 24, No. 6, pp. 430–437.
- Radaelli, C. (1999) 'The Public Policy of the European Union: Whither Politics of Expertise?' *Journal of European Public Policy*, Vol. 6, No. 5, pp. 757–774.

- Salter, M.B. (2004) 'Passports, Mobility and Security: How Smart Can the Border Be?' *International Studies Perspective*, Vol. 5, No. 1, pp. 71–91.
- Salter, M.B. and Mutlu, C.E. (2013) *Research Methods in Critical Security Studies: An Introduction* (Abingdon: Routledge).
- Sampson, S.E. (2010) 'The Unified Theory of Service. A Paradigm for Service Science'. In Maglio, P.P., Kieliszewski, C.A. and Spohrer, J.C. (eds) *Handbook of Service Science* (New York: Springer), pp. 107–131.
- Scheel, S., Ruppert, E. and Ustek-Spilda, F. (2019) 'Enacting Migration Through Data Practices'. *Environment and Planning D: Society & Space*, Vol. 37, No. 4, pp. 579–588.
- Schneider, S. and Nieswandt, C. (2018) 'EASSO – Support Office or Asylum Authority? Boundary Disputes in the European Field of Asylum Administration'. *Österreichische Zeitschrift für Soziologie*, Vol. 43, No. Supplement 1, pp. 13–35.
- Scipioni, M. (2018) 'De Novo Bodies and EU Integration: What Is the Story Behind EU Agencies' Expansion?' *Journal of Common Market Studies*, Vol. 56, No. 4, pp. 768–784.
- Trauttmansdorff, P. (2022) 'The Fabrication of a Necessary Policy Fiction: The Interoperability 'Solution' for Biometric Borders'. *Critical Policy Studies*, online first, pp. 1–19. <https://doi.org/10.1080/19460171.2022.2147851>
- Trondal, J. (2010) *An Emergent European Executive Order* (Oxford: Oxford University Press).
- Tsianos, V.S. and Kuster, B. (2016) 'Eurodac in Times of Bigness: The Power of Big Data Within the Emerging European IT Agency'. *Journal of Borderlands Studies*, Vol. 31, No. 2, pp. 235–249.
- Vargo, S.L. and Lusch, R.F. (2004) 'Evolving to a New Dominant Logic for Marketing'. *Journal of Marketing*, Vol. 68, No. 1, pp. 1–17.
- Vargo, S.L. and Lusch, R.F. (2008) 'Service-Dominant Logic: Continuing the Evolution'. *Journal of the Academy of Marketing Science*, Vol. 36, No. 1, pp. 1–10.
- Walters, W. (2017) 'Live Governance, Borders, and the Time-Space of the Situation: EUROSUR and the Genealogy of Bordering in Europe'. *Comparative European Politics*, Vol. 15, No. 5, pp. 794–781.
- Weingart, P. (1999) 'Scientific Expertise and Political Accountability: Paradoxes of Science in Politics'. *Science and Public Policy*, Vol. 26, No. 3, pp. 151–161.
- Winzen, T. (2011) 'Technical or Political? An Exploration of the Work of Officials in the Committees of the European Parliament'. *The Journal of Legislative Studies*, Vol. 17, No. 1, pp. 27–44.