"(UN-)MAKING" DATA TO "MAKE" SECURITY:

A DISCURSIVE AND VISUAL INQUIRY INTO THE PRODUCTION, CIRCULATION AND USE OF DATA ACROSS THE PAN-EUROPEAN INFORMATION INFRASTRUCTURE

Thesis submitted to the School of International Studies, University of Trento in partial fulfilment of the requirements for the degree of Doctor of Philosophy in International Studies

Submitted: 16th January 2023

Author: Vanessa Ugolini

(35th Cohort)

Supervisor: Alessandra Russo

Advisor: Georgios Glouftsios

Vanessa Ugolini

Abstract

To counter hybrid threats – for example, international terrorism, transnational organised crime and (cyber-)attacks – security and intelligence communities increasingly gather, process and exchange vast amounts of data on presumably suspect individuals. This trend has been enabled by recent developments in surveillance capacities related to Information and Communications Technologies (ICTs). As a result, cross-border data transfers have become not only an element of international trade but also an important component of law enforcement strategies. Nevertheless, the exchange of data for policing purposes is not always smooth. Rather, there are frictions that emerge therein as well as technical and legal issues relating to the combination of data from different information systems and under different formats. This study advances the concept of *data lifecycle* in relation to the practices, such as the collection, entry, processing, storing, and analysis that direct data in specific ways to create multiple "cycles" of uses. Through the analytical lens of the *lifecycle* I aim to examine specifically how data are repurposed, not only by digital technologies, but also by provisions regulating access, storage and use of information for criminal matters. The core task consists in identifying the *socio-political*, *legal* and *technical* conditions of possibility that allow for the exchange of data at the pan-European level. By bringing together multiple conceptual and methodological subfields, I shed light on the politicality of EU data infrastructures that appear physically very remote or less visible, yet in a way that people do not realise how mundane they have become. Investigating the *data lifecycle* as a network of practices generates findings that are useful for understanding how security is enacted through the collection and use of different forms of data and hence for interpreting the evolving landscape of data-driven security governance in the EU.

Keywords: Data practices, data lifecycle, data repurposing, network, security knowledge, intelligence production, infrastructure, information sharing, law enforcement, EU internal security, visual network analysis.

TABLE OF CONTENTS

List of Tables

(All the listed tables and figures have been elaborated by the Author).

List of Figures

Table of Acronyms

AFIS	Automated Fingerprint Identification System
AFSJ	Area of Freedom, Security and Justice
ANT	Actor-Network Theory
API	Advance Passenger Information
BLNI	Backup Local National Interface
CISA	Convention Implementing the Schengen Agreement
CJEU	Court of Justice of the European Union
CODIS	Combined DNA Index System
CSS	Critical Security Studies
DAPIX	Council Working Party on Information Exchange and Data Protection
DCS	Departure Control System
EC	European Commission
ECRIS	European Criminal Records Information System
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EFTA	European Free Trade Area
ENU	EUROPOL National Unit
ESS	European Standard Set
EU	European Union
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
iAPI	Interactive API system

IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICT	Information Communication Technology
II	Information Infrastructure
ISSOL	Interpol Standard Set of Loci
IR	International Relations
IT	Information Technology
JHA	Justice and Home Affairs
JSA	Joint Supervisory Authority
LEEd	Law Enforcement Education Platform
LIBE	Civil Liberties, Justice and Home Affairs
LNI	Local National Interface
MAP	Mutual Assistance Procedures
MLA	Mutual Legal Assistance
MRTD	Machine Readable Travel Document
MRV	Machine Readable Visas
MRZ	Machine Readable Zone
MS	Member State
NCP	National Contact Point
OSCE	Organization for Security and Co-operation in Europe
PIU	Passenger Information Unit
PNR	Passenger Name Record
R&R	Request and Response
SIENA	Secure Information Exchange Network Application

SIRENE	Supplementary Information Request at the National Entries
SIS	Schengen Information System
STS	Science and Technology Studies
TESTA	Trans European Services for Telematics between Administrations
TFEU	Treaty on the Functioning of the European Union
TRIP	Traveller Identification Programme
UN	United Nations
VIN	Vehicle Identification Number
VIS	Visa Information System
VIZ	Visual Inspection Zone
VNA	Visual Network Analysis
VRD	Vehicle Registration Data
WCO	World Custom Organisation

Introduction

Over the past decade, an increasingly dense landscape of data and information exchange schemes has grown out of policy initiatives in the fields of law enforcement, border security and migration management at the pan-European level. In an overview of what is called "information management" in the European Union (EU),[1] published in 2010, the European Commission identified 25 such schemes in the Area of Freedom, Security and Justice (AFSJ), most of them implemented over the past ten years, and with more being under development. What is striking about this landscape is the way in which each new initiative is framed as a necessary measure to "fill the gaps" or "connect the dots" (Kaufmann 2019; Lyon 2016) in the data that national and EU law enforcement agencies can use to prosecute individuals. Associated with other information systems, these schemes lay down the conditions for the proactive monitoring, tracking and sorting of large numbers of persons. Accordingly, having access to information with operational importance is regarded as a major asset in the hands of law enforcement authorities to effectively and efficiently counter criminal activities. Nevertheless, from the citizen's perspective, it is becoming increasingly difficult to understand what data are being collected, by whom and for what purposes.

Temporally and spatially the production of data varies, thus entailing that information infrastructures have their own history and geography. In a growing number of criminal cases, judicial authorities require the extraction of personal data that is stored across dispersed information systems, located in different countries. Data collected for a former purpose, for example, to establish the identity of travellers at borders, can contribute to build typologies of "risk" through profiling techniques, and in turn to identify different persons at different security sites. The term "control creep" refers specifically to data that are being repurposed in ways that differ from the initial intent underpinning their generation (Kitchin 2014: 13). However, individuals do not necessarily anticipate that the data they provide through administrative

[1] See "EU Information Management Instruments, Memo/10/349, Brussels, 20 July 2010. https://www.statewatch.org/media/documents/news/2010/jul/eu-com-info-systems-memo-jul-10.pdf

procedures might be made available to state authorities, and then used for intrusive processing purposes. As a result, the ability to capture and use data across borders is creating a "data citizen" whose rights and obligations do not derive exclusively from the state because of the transnational nature of the transmission of data (Gabrys 2019: 248). In terms of research, these considerations create the need for shedding light on the socio-political, legal and technical processes of data production for security purposes.

The ability to extract data and use them in the context of law enforcement fits within the move towards multi-purpose databases, which constitutes the key trend in the current EU AFSJ information landscape. The EU Commission has recently launched a series of consultations to address the technical, operational and legal challenges derived from the increased expansion of its data management architecture. Especially, in June 2016 the Commission set up a "High-level Expert Group on information systems and interoperability" (OJEU 2016d), tasked with identifying and addressing the structural shortcomings resulting from the fragmented architecture of data management for border control and security. The issues identified concern mainly the sub-optimal use of the services offered by existing EU information systems, such as the Visa Information System (VIS), the Schengen Information System (SIS I and II) and the Passenger Name Record (PNR) scheme. These systems have been designed to store large amounts of personal data for different purposes, such as for visa applications, border management and the identification of suspect individuals travelling to the EU.

Notwithstanding the centrality of the technologies that allow for the exchange of data cross-borders, the focus of this research is on the data practices that mediate the collection, transfer and use of information in the context of EU data-driven security governance. Understanding the purpose for which data are exchanged across different information systems is crucial to determine when information can be accessed by law enforcement authorities. To this regard, there is a fundamental difference between accessing data for identification purposes and for investigative purposes. In general, the former does not require prior authorisation, and thus an Information Technology (IT) system can be consulted through a single search for alphanumeric (or biometric in specific circumstances) data. Whereas the latter is subject to more stringent procedures since it requires to extract data in the search for evidence to build criminal cases. This occurs, for instance, when data are extracted for reconstructing the travel history of a known suspect. Therefore, establishing how data are "recycled" (Bellanova and Fuster 2019:

355) across different infrastructures is not less important than examining how data are rendered transportable through the deployment of security solutions.

Context and research questions

Cooperation and exchange of information in the context of criminal investigations have to some extent always taken place through informal agreements and, increasingly, on a formalised basis (e.g. through automated means). In light of the increased threat of terrorist acts and the cross-border nature of criminal activities, it became necessary for law enforcement authorities within the EU to request and obtain information from other Member States in more streamlined and effective ways. The need to improve information exchange for law enforcement purposes was first mentioned in the European Council conclusions of Tampere as early as 1999. Then, it was reiterated in the Hague Programme of November 2004 and has been remarked ever since. These discussions resulted in the call for the consolidation and standardisation of the pan-European information infrastructure through the introduction of a number of legislative instruments that now form the legal basis of information exchange. The first piece of legislation that foresees the possibility of establishing measures in relation to "the collection, storage, processing, analysis and exchange of relevant information" – regards the provisions contained in Article 87 of the Treaty on the Functioning of the European Union (TFEU):

> "The Union shall establish police cooperation involving all the Member States' competent authorities, including police, customs and other specialised law enforcement services in relation to the prevention, detection and investigation of criminal offences".
>
> (OJEU 2012: 83)

This Article provided the foundation for the introduction of a number of treaties that have significantly expanded the scope of information exchange to policy areas (e.g. law enforcement) as well as to data categories (e.g., facial images, biometrics, etc.) for policing and criminal justice purposes. Among them, the most important are the 1990 Schengen Convention (OJEU 2000a), the 1995 Convention on the Establishment of a European Police Office (EUROPOL) (OJEU 1995b), the Hague Programme (OJEU 2005a), the Prüm Decisions (OJEU 2008b and OJEU 2008c), the Swedish Initiative (OJEU 2006d) and the Lisbon Treaty (OJEU 2007c). These are the primary sources of EU law and include provisions on police co-operation and information exchange. More specifically, the Hague Programme, the Prüm Decisions and the Swedish Initiative are acts of law that legally ground information exchange

between Member States' law enforcement authorities for the purpose of detecting, preventing and investigating criminal activities.[2] This extensive toolbox resulted in the emergence of several policy initiatives for collecting, processing and sharing information in the AFSJ.

The above-mentioned legal provisions comprise two dimensions. On the one hand, they imply an extensive view of access to personal data afforded to law-enforcement authorities. This idea underpins a very wide understanding of what kind of data and information law-enforcement agencies should have access to. On the other hand, they point towards the possibility of preventive data-driven action – instead of a reactive response to a committed criminal act – in the field of criminal investigations (see Amoore 2013; Aradau and Blanke 2017a; Egbert and Leese 2020). These two dimensions emphasise how the interrelatedness between security and technology actually occurs through the everyday practices of the agents of security (both public and private actors, e.g., border authorities, police officers, software developers, legislators, etc.). Especially, three key aspects of the EU approach to security emerge from this framework. First, it is highly focused on data, especially on digital data. Second, it is increasingly cross-border and cross-sectorial. Third, it reflects a larger shift in the temporality by which crimes are sought, that is, from reaction to prevention.

The first aspect reveals that digital data constitute the major asset in the EU fight against terrorism and transnational crimes. Existing systems such as the Visa Information System (VIS), the Schengen Information System (SIS) and the Passenger Name Record (PNR) scheme along with proposals to develop new systems (and render them interoperable) are all framed in a way as to allowing public authorities to gather, store, process and exchange large amounts of personal data for a range of purposes, such as for border management, visa applications and law enforcement activities. At the same time, these initiatives reveal the second aspect of the EU approach to security, concerning the partnership with the private sector for the development of technological "solutions" to turn data into actionable resources (see Bigo and Carrera 2004; Martins and Jumbert 2020; Oliveira and Gabrielsen 2022). Based on the assumption that all data are pertinent, information is gathered "in bulk" through large-scale information systems before possessing sufficient indicia of suspicion that a criminal act has been committed. The obsession with risks, not already identified, has generated an extensive industrial and governmental drive to fill information gaps about potential criminals through the preventive

[2] Criminal investigations also include law enforcement activities aimed at the collection of admissible evidence to be used during judicial procedures.

collection of different categories of data (Amoore 2013; Aradau and Blanke 2017a; Hall 2017; Kaufmann et al. 2019; Leese 2014).

This future-oriented rationality is reflected in the third aspect of the EU security strategy which is geared towards understanding, detecting, preventing and deterring against security threats. The literature on surveillance refers to such anticipatory mode to address crime and discern suspects as "prospective surveillance" (Matzner 2016: 199). This mode is concerned with the circumspect collection of data, then stored into databases only temporarily, yet, with the prospect to cite a range of information at any time in the future (Matzner 2016). Accordingly, despite they may not reveal their utility in the present, every bit of information is stored in anticipation of their future use. The goal of predicting human behaviour through the implementation of technological solutions has detached the state's ability to chase crimes from within its physical boundaries. While it has opened up unprecedented possibilities for pre-emptive action in the digital domain (see Amoore 2013; Aradau and Blanke 2017a-b; De Goede et al. 2014; Egbert and Leese 2020). A further consequence of EU data-driven governance concerns the effects derived from the broader shifts by which crimes are sought, both in the temporality, from past to future offense, and in the rationality, from ex-post to ex-ante interventions (McCulloch and Pickering 2009).

Protecting against unpredictable threats requires to render them knowable first by relying on a plethora of algorithmic techniques, from pattern recognition to anomaly detection, used to identify suspicious streams of data (Aradau and Blanke 2017b). The high-tech nature of the instruments deployable by security agencies and law enforcement authorities has promoted an anticipatory, future-oriented approach to the prosecution of crimes (Aykut et al. 2019). In this context, information systems at large figure as performative machines that generate security-related knowledge by recording multiple behaviours and interactions and by translating both into data to be further processed (De Goede 2018). These machines are part of a broader configuration of technological devices such as automated gates, interfaces, IT networks etc., that together with security authorities form a "dense socio-technical environment" (Bellanova and Duez, 2012: 110), where both the "social" and "technical" elements co-participate in the EU policymaking process (Jeandesboz 2016). Accordingly, the EU "data-centric", "cross-border", "preventive" approach to security has instituted new logics for governing the population and in turn has foregrounded the socio-technical nature of EU security governance.

The implications of the preventive acquisition of data for the governance of future contingencies touches upon salient debates within the realm of security, with attendant ethical and normative considerations concerning the effects of cross-border data exchanges on the privacy of individuals. Especially, the rhetoric used to establish large-scale information exchange schemes purports a threat that does not seem to wither away in the short-term, but rather that permeates our lives. This view has paved the way for the profusion of a vast number of different systems designed to be "sticky" – that is, set to remain with use – in order to attain security through the mundane exchange of information between private (i.e. airline and telecommunication companies) and public bodies (i.e. national police and judicial authorities). In view of the increased expansion of the pan-European data management architecture, the core task of this research consists in addressing the technical, operational and legal issues derived from the extraction and storing of data across multiple information systems, designed for different purposes. By advancing my own interpretation of the "lifecycle of data" (Kaufmann 2020) – how data are collected, processed, exchanged, and ultimately operationalized in the law enforcement context – I aim to address the following research question:

What are the *socio-political*, *legal* and *technical* conditions of possibility that allow for the exchange of data at the pan-European level for criminal matters?

Framed as such, this question tackles the various heterogeneous elements and conditions that shape how different data sources are rendered transportable, re-combinable and actionable at the pan-European level. Personal data collected for a former purpose, for example, to establish the identity of travellers at borders, can in fact contribute to build typologies of "risk", and in turn to assess different persons at different security sites. Nevertheless, personal data are highly contextual. Data need to be fit for purpose in order to ensure that legal guarantees, such as the right to private life, are respected. Therefore, examining the ways in which data are repurposed – cross-border and cross-sector – is key to establishing what are the processes that shape the governance of security through data. I am particularly interested in understanding how different modes of "making" security are enacted through the exchange of different forms of data – or, in other words, how security governance at the EU level happens *through* the data gathered, stored and processed by multiple AFSJ information systems. Demonstrating how security is context-dependent on the data practices that mediate the exchange of information for security purposes aims at generating findings that are useful to interpret the evolving landscape of EU data-driven security governance.

This research brings together different conceptual and methodological subfields to explore the politicality of EU data infrastructures that appear physically very remote or less visible, yet in a way that people do not realise how mundane they have become. Many of these infrastructures and devices have come to form the infrastructural basis for undertaking security-related decisions concerning our mobility across borders or our categorisation into levels of "risk." By investigating the multiple ways in which specific categories of data (mandated by EU directives, regulations, etc.) become part of crime prevention strategies I aim to shed light on several sub-research questions. The first bulk regards the functioning of information exchange more broadly understood: what are the principles that drive information exchange in the AFSJ area? Are these principles reflective of a particular security logic/rationale (i.e. traceability, pre-emption)? How are these principles translated into the functional characteristics of information systems? The second bulk regards the specificities of information exchange: who are the actors that share information for criminal justice finalities? What are their tasks and powers? What type of information can they transfer? Under what conditions are national law enforcement authorities allowed to provide the authorities of other Member States with data stored in their national systems?

By addressing these questions I aim to fulfil the following set of objectives. First, I aim to build upon and further scholarly works that have emphasised the importance of data practices in the making of international security (e.g., Amoore and De Goede 2005; Amoore and Raley 2017; Bigo 2014; Scheel et al. 2019). What I call the processing, archiving, analysing, and sharing of data are essentially practices through which security comes into being. These practices matter in the context of international security because they direct the setup of information systems for data exchanges. Second, I aim to complement current research on the infrastructural politics of European integration in the AFSJ (e.g., Bellanova and De Goede 2020; Glouftsios 2021; Jeandesboz 2016), by considering how data practices in general, and information exchange for law enforcement purposes in particular, affect processes of crime and terrorism prevention (e.g., Amoore 2011; Egbert and Leese 2020; Kaufmann et al. 2019; Leese 2014). Third, by offering a visualisation of emerging networks of data practices I aim to understand how the relations between transnational security professionals and technological infrastructures support the circulation of information at the EU level. Fourth, I aim to identify the technical and legal issues resulting from the combination of data from different systems, under different formats; and especially, to address how the legal and technical configuration of EU data infrastructures impacts on individual privacy and freedoms, such as the freedom of movement and the right to

private life. On the basis of these objectives, this research aims at making several, yet interrelated contributions, of conceptual, methodological and empirical relevance.

Conceptual contribution: The "lifecycle" of data

One of the premises of this research is that the exchange of data does not occur smoothly, with data flowing from one information infrastructure to another. Data need to be rendered transportable both technically and juridically in order to be re-combinable across different datasets. The possibility of 'recycling' data derives from the technical ability to receive and handle a variety of information sources, to process them through adequate computing infrastructures, and from the expertise in the use of data analytics software to make sense of them (Bellanova and Fuster 2019: 355). These activities are highly contextual and vary from site to site. More importantly, they highlight how data stand in a mutual relationship with both the humans who design and operate information systems and the infrastructures that handle them (Kaufmann and Leese 2021). As Bellanova and Fuster (2019: 355) put it, through "processes of coming apart, breaking down and decay" the life of data is constantly reinvented. Discussions about the "liveliness" of data are not new. Many scholars (e.g., Lupton 2015 and 2016; Ruppert et al. 2013; Savage 2013) have developed new materialist approaches (Barad 2007; Mol 2008) in order to conceptualise the agency of data in the production of knowledge for a range of different purposes, not necessarily strictly related to security.

Among them, Kaufmann (2020) was ground-breaking in advancing the idea of an "analytic of the life cycle" as a reconstructive method through which to grasp the agency of data in any type of data-based environment. She borrowed this conceptual device from Van den Eynden (2014), who has first introduced the notion of "lifecycle" with the intention to inspire reflection about the making of data. However, in Van den Eynden's account, the lifecycle features as a model within the research process rather than as a method to capture the liveliness of data as such. Only later, the growing interest in theorizing the relationship between data, infrastructures and humans have led other authors, such as Roth and Luczak-Roesch (2018), to utilize the concept as means to reconstruct the life of technologies. Moving even further, Kaufmann and Leese (2021) have foregrounded the value of the "data lifecycle" as a theoretical and methodological framework that helps illustrate the active role of data – in their case crime data – across different empirical contexts (e.g. predictive policing). They draw particular attention to the circularity of the lifecycle by showing how data come into being and how in turn become productive in and through the relations with humans and digital devices.

While they offer an empirically-oriented case (i.e. predictive policing) for tying the notion of lifecycle to the liveliness and agency of data, their account brings into focus data as matters that have a generative force of their own. Yet data, indeed crime data, – instead of the "lifecycle" – lie at the core of their analysis. However, if we seek to enrich the notion both conceptually and empirically, we should shed light on the "lifecycle of data" per se, by asking: in what ways is the lifecycle of data structured? What are the forces at stake? How is security generated through it? If we limit our vision to data – how data come to life and how in turn they shape life (Kaufmann and Leese 2021) – we inherently limit the analytic potential of the notion of "lifecycle". In this vein, I find room through my research for expanding the scope of this notion by offering a detailed account of the *socio-political*, *legal* and *technical* conditions of possibility of data becoming knowledge and thus governable inputs into security processes. Rather than asking how data are rendered "lively", I move past these strands and use the lens of the lifecycle to better understand how security is both context-dependent on the information systems used to gather specific categories of data and how in turn it is generated from them.

With my research, thus, I seek to continue the discussion that Kaufmann (2020) has started by postulating the idea that digital data have a lifecycle. Yet my own elaboration of the notion allows for a two-layers analysis: on one hand, it enables to zoom-in on the specificities of the lifecycle of data in the EU AFSJ domain; on the other, it enables to zoom-out on the dynamics through which the lifecycle of data becomes ordering power in the production of security knowledge. From this perspective, the lifecycle functions as more than an analytical lens. It is both a conceptual device for theorizing the relationship between digital data, security and infrastructures, and a process which lends itself to be studied as a "network" of human and non-human practices. Applied to my research then, the data lifecycle points to the ways in which the variety of practices that "make" and "un-make" data – that is, the collection, entry, handling, processing, storing, and analysis – as well as the provisions that regulate such practices, direct data in specific ways by creating channels of information exchange.

Methodological contribution: Network visualisation

Based on the above conceptual premises, it is crucial to mark the distinct methodological contribution that I seek to make by approaching the lifecycle of data as a "network" of human and non-human practices. In their paper, Kaufmann and Leese (2021) have remarked that, when used as a reconstructive method, the lifecycle helps tracing the life of data – how they come into being and how they become "in-formation" (Ibid: 69) – and their relations with

humans and infrastructures. Yet, they do not really provide a method that assists in capturing these dynamics. If we assume that data circulate in different data-based environments and are opened to constant repurposing, we are purporting that data can take multiple trajectories by constantly being exchanged and repurposed. The question to ask then is not how the lifecycle of data can assist us in understanding the dynamics and productivities of data (Kaufmann and Leese 2021), but rather, how can the lifecycle be studied inductively? How can it be reconstructed? What method is best suited to bring data and their dynamics into focus? In terms of methodology, these questions demand to trespass the lifecycle of data as an analytical notion to focus on the many ways in which both material and normative conditions come to shape the "cycles" of uses (and re-uses) of different categories of data (e.g., biographical, dactyloscopic, biometric, travel data, etc.).

This research means to contribute to such reflection by advancing a tentative methodological framework that I have modelled to the investigation of the lifecycle as a network of practices. In particular, I recurred to a methodological approach that utilizes "networks" as a tool of visualisation analysis. By "network visualisation", I refer specifically to a methodological process that – rather than identifying the structural properties of the phenomenon under observation – functions as a means of exploratory analysis. In their paper, Venturini et al. (2015) provide the basics for carrying out the visual analysis of networks and for interpreting their topological features in a two-dimensional space. This technique – known formally as visual network analysis (VNA) – has been applied extensively to explore relational datasets across the natural and social sciences (see Venturini et al. 2021). Yet given the lack of formalization and the scarcity of guidelines on how to design a network and read its visual features, it has found limited application as a practice-oriented way for studying digitally-mediated security among the methodologies developed by CSS scholars.

In general, the primary aim of VNA is to come to a visual understanding of the relational composition of a particular practice under investigation, and of the effects that such composition generates (Decuypere 2020). It is thus best suited to study the lifecycle of data as a network of practices. Applied specifically to my research, then, visual network analysis serves the purpose of exploring how the normative conditions inscribed in texts combine with material elements, such as software and electronic communication channels, to become pathways of data exchange. One of the reasons for creating a "visualisation network" is the structural opacity of information systems. Looking at their technical specifications and

functional characteristics has so far remained a challenge to most non-IT specialists. As a consequence, through VNA I seek to introduce a point of departure for furthering the study of the complex linkages between data, technology and security. A methodology of network visualisation is indeed an invitation to reflect on the formation, constitution and arrangement of different circuits of data exchanges, and, most importantly, on their unseen effects on the "life-like" trajectories of data.

Therefore, I use the notion of "network" to come to a graphical representation of the data lifecycle and the trajectories it actualizes. Far from being merely an aesthetic device, a network is a powerful conceptual tool (Venturini et al. 2015) that enables to enclose in a single "snapshot" the complex entanglements between data and the environment to which they are attuned. Through visualisation analysis, the data lifecycle thus becomes a network, though of a very particular type. The graphical representation of the lifecycle has an intrinsic hermeneutic value. It is more than the projection of a map on the screen or paper. It is a tool that can be exploited for the study of social phenomena (Venturini et al. 2015). Applied to the study of the lifecycle of data, network visualisation makes us aware of the recursive trajectories that data take by being initially produced and subsequently repurposed for policing purposes. The choice to stress the visual aspect of the data lifecycle along with its structural properties opens up a fruitful avenue of reflection that focuses on the framing of different technological systems for the exchange of data which are not the of the same nature, but yet contribute to the "making" of different modes of security.

Precisely because I use this method not to provide clear-cut answers on the constitution of the lifecycle of data, but rather to illuminate particular properties of its composition, I conceive the visual analysis of the data lifecycle as a method for exploratory analysis. Such method encourages to challenge previous knowledge about the practices under investigation and to search ground for new findings by thinking *through* the "network" – as a visual element that complements the qualitative data. By capturing its spatial representation "on paper", the lifecycle of data thus becomes part and parcel of my research. In order to reproduce it graphically, I relied on a software called "Gephi" (gephi.github.io). Gephi is a digital tool that allows to design networks on the basis of the gathered qualitative data and to visualize their spatialization in a two-dimensional space. Accordingly, the visual device produced is but a medium of visualisation (Decuypere 2020). The form it takes is dependent on both the algorithmic premises of the software that structures the resulting network and the qualitative

analysis conducted preliminary by the researcher. It is then the role of the researcher to interpret the knowledge produced and prompt insights with an analytical value.

Empirical contribution: "Securing" *through* data

By framing the data lifecycle as "network" I seek to provide an empirically-oriented way to reflect on the social, political and institutional dynamics that give rise to knowledge about security. In this way it is possible to create knowledge from the phenomena observed, rather than just replicating through writing what the object of research is. In terms of reflexive research practice this has a number of implications of empirical relevance. First, by using the lifecycle of data as focal point of analysis it is possible to explore a different facet of security and conceptualise it in terms of a mundane process for governing society *transversally*. Empirically, this approach provides a new avenue for researching security and technology that goes beyond looking at digital data as pioneering means to secure society at large, but rather accounts for the social, political and institutional dynamics that have "securitised" digital data. Second, attending to the notion of lifecycle creates a novel framework to theorise and understand the messy relationship between the object of research, the concepts engaged and the technological devices that have come to shape the representation of security in the social world. Third, visualising the lifecycle of data in the form of a network enables to unpack the broader configurations of the logics and processes through which security is operationalized.

This construction of the research space impacts on the way we come to understand and study datafication as a process, and the effects it generates on social life. Instead of focusing exclusively on information systems as security sites comprised of databases, communication channels and codes, I pay close attention to both the networks related to the gathering, processing and sharing of data, and the legal frameworks that direct these practices in specific ways. More closely, I assume that the distinct modes of ordering, organising, regulating and governing data are informed by a number of political rationalities before being translated into the technical specifications of IT systems (see also Glouftsios 2019). Simultaneously, such technical aspects matter politically since they enable a data-driven mode of governing. For instance, IT systems designed for preventive purposes mediate political decisions of exclusion by filtering out "risky" elements (e.g. individuals suspected of terrorism or organised crime) (see Aradau and Blanke 2017b; Kaufmann 2019; Lyon 2003). The effects of such filtering do not concern solely the data produced by IT systems, but also impact on the international mobility of those individuals considered "risky".

The central concern then is on investigating how the lifecycle of data is regulated at the political level and how it is arranged both technically and legally. On this basis, rather than regarding functional characteristics and normative provisions as supra-layers, I treat them as co-constitutive of the design and operation of information systems that circulate data in particular ways. In doing so, I seek to open up a new avenue for examining how data politics, data structuring and data protection are inscribed into the socio-technical arrangement of different data infrastructures and how they contribute to creating multiple cycles of uses for pre-existing data. Moving beyond the focus on the ethical and legal concerns that data practices raise in relation to individual privacy, liberty and mobility, I propose to investigate how the operationalization and legal enforcement of values, such as privacy and accountability, occur *through* data infrastructures, rather than as a result of them. Such normative reflection enables to address the complexities derived from the combination of different categories of data, from different sectors of security. Additionally, it contributes to understanding how security is forged, and how it is aligned through material and legal requirements with data practices.

The core argument that I seek to elaborate through the notion of "data lifecycle" then is that security is produced *through* data. Even more crucially, data practices give form to data and in turn shape security knowledge. This is why I suggest to focus on how the lifecycle is regulated instead of trying to use it as an analytical device to describe the agency of data across multiple data-based contexts – such as Kaufmann and Leese (2021)'s case of predictive policing. Most importantly, if we know how it is regulated, we know more about the internal arrangement of its relations: how different information systems speak to different security logics and different data categories. Accordingly, the lifecycle of data can take multiple empirical forms that vary according to the socio-political, legal and technical conditions that structure it. In turn, this entails that security is multiple and dependent on both data practices and the logics inscribed into the functional characteristics of information systems. The empirical salience of my research then is realized by applying the notion of data lifecycle to better understand how digitally-mediated security is generated *through* data and how it works through different data infrastructures, as well as to engage more closely with the empirical contexts in which data are exchanged.

Research structure

Having marked the distinct conceptual, methodological and empirical contributions, in what follows, I lay out the research structure. In Chapter 1 I align my research with the material turn

taken – in the IR research agenda in general, and critical security studies in particular – to the study of digitally-mediated security (e.g., Acuto and Curtis 2014; Bellanova and Duez 2012; Hoijtink and Leese 2019; Jeandesboz 2016; Leese 2015). I thus proceed to review the relevant literature – Science and Technology Studies (STS), critical security studies (CSS), surveillance studies, and critical data studies. Drawing on the theoretical and conceptual resources offered by these variegated disciplines I discuss how they can be used to describe the complexity and heterogeneity of the relations between humans and technologies in enacting data practices, and in turn how they can illuminate the role of data in the production of security knowledge. I then introduce the key indicators for the empirical analysis and explain how my study can contribute to reinvigorate the academic understanding of security as discipline and practice. A growing body of literature indeed explores how digital, technoscientific developments reconfigure the rationales, techniques, and practices of security. Fewer accounts examine the effects of these developments on security theory.

In Chapter 2 I present the multi-methodological approach that I have adopted in the investigation of the lifecycle of data. I draw out first the techniques of data collection and analysis, to then move on to describe what texts – as they result from the collection of written documents of different nature and origin – reveal and what they do not, how I process them and for what purposes. More closely, I emphasise how the tasks of archival research, document analysis and visual network analysis are functional to address my research objectives. Then I explain how the practices related to the gathering, storing, processing and sharing of data can be studied through the notion of the data lifecycle and how the tentative framework that I advance contributes to debates in critical security studies revolving around methods. I also clarify how studying the lifecycle in the form of a network enables to shed some light on the relations and practices of the actors involved in the exchange of multiple forms of data categories.

In Chapters 3, 4 and 5 I reconstruct the *socio-political*, *legal* and *technical* conditions of possibility for the exchange of data in the AFSJ domain by considering four case studies: the Schengen Information System (I and II), the Prüm Framework, and the API and PNR systems. Each empirical chapter consider how the discourse of security (as both knowledge and practice) operates as a process of historical formation marked by contestations and frictions over the development and extension of different AFSJ infrastructures for data exchanges. I examine in particular the dynamics that characterise the lifecycle of data behind four selected AFSJ

information infrastructures – the SIS (I and II), the Prüm framework of cross-border information exchange, API and PNR – in order to expose the power relations and stakes involved in enacting security *through* data. By considering the multiple activities of data structuring – that is, data collection, processing and analysis – I empirically reconstruct how the enactment of security is context-dependent on the data infrastructures that combine varied data categories (e.g., dactyloscopic, identity and travel data, etc.) and types of security logics.

In Chapter 6 I weave the threads of the empirical analysis by discussing how the AFSJ information infrastructures considered operate in some combination to constitute law enforcement tools for data repurposing. I draw particular emphasis on the comparative element among the four case studies in order to expose how security is multiple and dependent on both the systems, the data therein, and the actors that design and operate them. By reflecting on the different ways in which data circulate, I aim to provoke in the readers an epistemological reflection on the meaning of "making" security through technology. Some observations that I raise in this respect concern: what are the epistemological and conceptual implications for studying security when data and the digital become a central arena of security policies? Why is the "making" of security through digital technologies important to investigate as a matter of contemporary governance? How can we, as researchers, provide more fruitful ways of analysing security beyond studying the technologies that allow for its operationalisation? And again, what happens if we disentangle security discourses from the agents, instruments and devices that contribute to the production of security knowledge?

Chapter 1

The "Co-Production" of Security Knowledge

1.1. Situating digital technologies in critical security studies

Processes linked to the collection, storage, analysis and sharing of digital data for security purposes have been problematised by scholars whose research lies at the intersections of critical security studies (CSS), surveillance studies, and science and technology studies (STS) (e.g., Bellanova and De Goede 2020; Bellanova and Glouftsios 2020; Davidshofer et al. 2017; Matzner 2017). This hybrid strand of literature identifies a number of themes related to the entanglements between security and (digital) technology. In particular, critical scholars have opened up new avenues for researching the role of IT systems across different domains, such as counterterrorism and intelligence cooperation (e.g., Aradau and Blanke 2017b; Bigo 2014), as well as the management of global mobility and borders (e.g., Besters and Brom 2010; Broeders and Dijstelbloem 2016; Jeandesboz 2016; Pickering and Weber 2006). Studying distinct modes of governing (in)security through data-driven practices highlights how the security field is shaped by and shapes technological developments. We are witnessing a proliferation of tools that, we are said, help practitioners to respond more effectively and swiftly to emerging security threats. For such effective and swift responses, actionable security knowledge is regarded as essential; knowledge that is produced by heterogeneous, situated, and contingent processes in which security practitioners, digital technologies and infrastructures take part.

A growing body of literature explores how digital, technoscientific developments reconfigure the rationales, techniques, and practices of security. To this regard, Layton explains that

"science and technology have become intermixed. Modern technology involves scientists who 'do' technology and technologists who function as scientists. [...] The old view that basic sciences generate all the knowledge which technologists then apply will simply not help in understanding contemporary technology" (1977: 210; see also Douglas 2012: 14). The multiplicity of disciplines that engage the topic regard both science and technology as practices. Especially, the idea that technology allows for the production of security knowledge, and thus possesses 'agency', constitutes the common denominator among variegated theoretical and methodological approaches. Critical scholars focus on the agency of technology for the production of security knowledge (e.g., Hoijtink and Leese 2019; Lindskov and Monsees 2019), and explore in particular how such production informs the practices of a wide range of actors – such as border guards, asylum authorities, police officers, law enforcement and intelligence services (e.g., Glouftsios and Scheel 2021; Jeandesboz 2016; Kaufmann 2019; Scheel et al. 2019).

Despite the growing interest in the intersection of security practices and digital technology, there are still some under-researched aspects, concerning for example the struggle between the social use of technology and predictive analytics, the technical and legal complexities derived from the combination of data sources from different systems, or again how judicial oversight can be organized in face of dispersed data infrastructures that yet have become so crucial to policing practices. These gaps are mainly due to the heterogeneity of the literature that cuts through multiple disciplines. I suggest that an interesting aspect of the entanglement between security and technology is that they do not operate independently of each other, but rather they exist in a complex relationship to the materiality of data themselves. Accordingly, to better understand the role of data infrastructures in the production of security knowledge – and to situate my research in the relevant literature – this review chapter draws on diverse disciplinary perspectives; in particular, CSS, STS, surveillance studies and critical data studies. Each disciplinary perspective illuminates the topic by providing a varied set of analytical sensitivities – informed especially by material-semiotic/ANT approaches (Law 2008; Mol 2010) – that are useful to describe the complexity and heterogeneity of the relations between humans and technologies in enacting security. Building on these insights, each section of this chapter explains how these multiple conceptual and theoretical perspectives inform this research.

In the first section I lay out the framework for synthetizing the role of technological systems across different domains, such as counterterrorism and intelligence cooperation (e.g. Egbert

and Leese 2020; Kaufmann 2019) and the management of global mobility and borders (e.g., Broeders and Dijstelbloem 2016; Jeandesboz 2016; Pickering and Weber 2006; Oliveira and Gabrielsen 2022), among others. In particular, I conceptualise sites of production of security knowledge as 'socio-technical' environments, where human and non-human actors produce new, quasi- automated forms of social control. The conceptualisation of technology as an active participant in heterogenous and situated security processes is important because it offers a more promising perspective for assessing the wider societal and normative consequences that emerge from data-driven governance. In the second section, I mobilize these insights to unravel the formation and functioning of socio-technical assemblages that enable the collection, processing, analysis and sharing of data. Here, I also engage with literatures related to surveillance studies and anticipatory policing (e.g., Egbert and Leese 2020; Kaufmann and Leese 2021; Leese 2014; Lyon 2016) in order to trace the evolution of surveillance practices from the traditional 'panoptic' observation of the human body – for example, in the prison setting discussed by Michel Foucault (1975) – towards a 'technologized' form directed at monitoring digital footprints (e.g., Logan 2017; Lupton 2016; Murakami 2007).

In the third section, I provide a more profound engagement with the role of data in the production of actionable security knowledge. In particular, I conceptualise data as key inputs that are continuously analysed, interpreted, cleaned, categorised, curated and stored by different security actors. These processes (analysis, curation, storing, cleaning, interpretation) are mediated by different technologies – such as hard disks, processors, desktops, data analysis tools, etc. – and thus they are socially and materially constructed (see Glouftsios 2018; Hoijtink and Leese 2019; Lindskov and Monsees 2019). In the fourth section, I explore how dynamics of anticipatory expertise have become embedded in security interventions and in the governance of contested policy issues through protocols, institutional arrangements and policymaking (see Aykut 2019). More specifically, I examine how the design and implementation of digital systems bind heterogenous security actors to a complex Big Data machinery for enacting predictions. I focus in particular on the role of algorithms in data-driven analysis for the governance of security (e.g., Amoore and Raley 2017; Aradau and Blanke 2015). In the final section, I set out the basis for incorporating legal considerations in the analysis of data infrastructures, pertaining specifically to the regulation of the production of data. I suggest that academic research should attain to legal issues by providing a normative reflection on both architectural and socio-legal infrastructural constraints behind the development of data assemblages.

1.1.1. The "agency/structure" problem

Within studies where security and technology intersect, the importance accorded to technology's agency is not always uniform. The traditional conceptualization of agency within IR has prevented an analytical appreciation of technology not only in the security field, but also in international politics more in general. The main tendency in the discipline of IR is to approach agency as part of the "agent-structure problem" that ascribes the 'capacity to act' only to humans (Wendt 1987). Actor-Network Theory (AN-T) allows to overcome the structure/agency debate by introducing a thinking tool that widens the scope of agency to the synthetization of both human and non-human components (Fenwick and Edwards 2010; Latour 2005; Law 2008; Mol 2010). In particular, the notion of 'actor-networks' underpins the analytical equality between actors (agency) and networks (structure), thus it introduces a socio-technical understanding of agency (Passoth and Rowland 2010). By enabling to account for technology as an 'agent', AN-T has challenged the traditional understanding of non-human elements as passive objects, while it has paved the way for researching their role as active agents in the production of (in)security (Hoijtink and Leese 2019). In order to transcend the traditional dichotomy between subjects and objects, scholars working at the intersection of STS and critical security studies have developed a rich methodological and conceptual toolkit for studying the role of technology in a range of security settings (e.g., Bigo 2014; Decuypere 2020; Douglas 2012; Hoijtink and Leese 2019; Salter and Mutlu and Salter 2012).

In particular, STS studies provide thick narratives about the formation and maintenance of different assemblages and the work required to make them durable (Bueger and Gadinger 2018; Glouftsios 2021). These accounts merge human and non-human actors as parts of "assemblages", or "actor-networks", and pay particular attention to interactions within what they call "socio-technical" systems. The general "capacity to act" [ascribed to technology] […] "is predicated upon the ability to collect information about the world through sensors or data inputs" (Leese and Hoijtink 2019: 1). However, technologies do not act in an autonomous fashion, rather "they assist, pre-structure, point out and make suggestions" to humans (Leese and Hoijtink 2019: 2). The conceptual tool of "co-production" first advanced by Jasanoff (2004), highlights how agency is co-produced in human-material networks through previously largely unconnected set of actors (Lindskov and Monsees 2019: 24). This process constitutes

a form of "heterogenous engineering"[3] (Douglas 2012: 107; see also Law 1987) since multiple actors gather, synthetise, and negotiate upon diverse kinds of knowledges – technical, technoscientific, and legal – in the design and development of technologies (Glouftsios and Scheel 2021).

Applied to my research the tool of "co-production"[4] highlights how data infrastructures implemented in the EU AFSJ operate as socio-technical settings that expand across multiple levels – the socio-political, the material and the digital – through which security is enacted. Yet adopting an AN-T approach does not offer a consistent perspective. AN-T is a form of open repository of material-semiotic tools, sensibilities and methods of analysis that treat everything in the social and natural worlds as continuously generated effects of webs of relations within which they are embedded (Law 2008). Indeed, the art of AN-T consists in tracing out the effects and exploring the "hows", rather than haunting for causes (Mol 2010). For Mol, ANT is a "loose assemblage of related, shifting, clashing, notions, sensitivities and concerns" (2010: 281). Therefore, approaching security practices through the AN-T lenses requires conducting a situated study that explores the socio-legal, material and technical dynamics that give form to datafication processes. AN-T is in fact embedded in a tradition of empirical case studies that go into "different directions", rather than attempting to draw the findings into an overarching explanatory framework (Mol 2010: 261).

1.1.2. Data infrastructures as "socio-technical" assemblages

When it comes to analyse the formation of data infrastructures, in particular IT systems, the AN-T perspective suggests to pay equal attention to technicalities (e.g. software, hardware) and to the communities of actors using them (police officers, security agencies, etc.) (Bueger and Gadinger 2018; Hoijtink and Leese 2019). Setting up a data infrastructure indeed involves technical but also social and political considerations. In particular, diverse forms of technoscientific, security and policy concerns are translated into the design characteristics of the system through discussions, negotiations, and redrafting of various texts, and are then retranslated into technical-infrastructural specifications through feasibility studies (Glouftsios

[3] The concept of "heterogeneous engineering" was first introduced by John Law in 1987 with his book *Technology and Heterogeneous Engineering: The Case of Portuguese Expansion* (MIT Presse).
[4] The work of Jasanoff on "co-production" (2004) offers a valuable point of departure for studying the production of (in)security through technology because it does not reduce "agency" to question of whom or what possesses agency. See also, Lindskov and Monsees (2019).

2019). The functional requirements inscribed in an information system further detail the exact procedures that should be followed by its end-users. This nexus of recursive design practices produce a real material impact on the technical-infrastructural features of the systems and on their functionalities. As a result, they provide a practical-oriented way for examining the process of becoming of heterogenous set of concerns into a socio-technical assemblage (see Acuto and Curtis 2014; Glouftsios 2019). These considerations have informed the choice to consider EU AFSJ information systems as "assemblages" of different data practices that create network(s) of data exchanges.

More closely, the notion of "assemblage" (Contini 2009; Velicogna 2014) refers to a system characterized by distributed human/non-human agency that emerges from a loose set of associations and interactions among its operating parts (Lindskov and Monsees 2019). CSS scholars Abrahamsen and Williams define "security assemblages" as "transnational structures and networks in which a range of different actors and 'normativities' interact, cooperate, and compete to produce new institutions, practices and forms of deterritorialized security governance" (2010: 90). In general, they are characterized by a contingent and volatile nature since the relations among human and material actors require constant "enactment" (Hoijtink and Leese 2019). Their capacity to interconnect spaces, end-users, and technologies enables data to 'travel across spatial and temporal registers' and be deployed at different security sites (Bellanova and Glouftsios 2020: 9). Through the process of 'unmooring', data can thus be de-contextualised and in turn can act as transferable forms of knowledge (Kitchin 2014: 22). There are several studies that approach data infrastructures as socio-technical assemblages whose design, development, and maintenance depend upon bundles of contingent and relational practices (e.g., Bellanova and Duez 2012; Bellanova and De Goede 2020; Glouftsios 2021).

In my research I develop this view of technological development as 'co-constituted' by human and non-human interventions in relation to the setup of AFSJ information systems, by drawing attention to data practices that bring together populations of security practitioners and technological devices such as databases. Analysing data practices as an 'assemblage' requires to carefully unpack and deconstruct their contingent, relational, and contextual nature. In line with the AN-T perspective, I conceive agency as 'multiple, variegated, and context dependent', that is, as a force that humans and non-humans exert in their associations and interactions (Leese and Hoijtink 2019: 11). In particular, I highlight how technologies are co-produced through protocols, regulations, and legislative and non-legislative practices that together

inform and shape the requirements and functionalities of different information systems in the AFSJ area. Accordingly, it is only by situating information technologies within their political, legal, and organizational contexts that it is possible to appreciate the formation of socio-technical systems presented as security "solutions" (see Bigo and Carrera 2004; Martins and Jumbert 2020; Oliveira and Gabrielsen 2022).

Practice-oriented approaches within STS provide a conceptual toolkit useful to understand how the enrolment of a technology lock-ins certain practices. In the attempt to redress the interrelatedness between security and technology, Lindskov and Monsees (2019) have advanced a three-steps model that is well-suited to explain how the socio-material composition of different information infrastructures is the result of a collaborative effort between human and non-human agents. According to them, security technologies emerge as a result of three processes: problematization, translation and stabilization. The first step refers to the ways in which a particular technology is problematized in order to make its use desirable and legitimate in response to a security issue. The creation of a problematization then initiates the translation process. This second step consists in translating security concerns into concrete technological requirements and specifications, that is into the design characteristics and technological configurations of information systems. The result of this process is the formation of an assemblage that synthetize heterogenous considerations and knowledges. Finally, the end point concerns the stabilization process that eventually creates durable and stable security assemblages in which the net of socio-material relations has been locked-in, thus making it entirely opaque.

To sidestep such structural opacity I propose to look beyond the inner workings of information systems by studying how their technical specifications and functional characteristics are embedded into protocols, organisational procedures as well as other socio-legal sources that regulate their design. Nevertheless, far from being linear and smooth, each of the three steps is subject to negotiation, controversy, and organisational and infrastructural requirements (Cavelty and Leese 2018). Accordingly, the formation and functioning of security assemblages ought to be studied in a situated manner. I have applied Lindskov and Monsees' model to my research in order to foreground the socio-material character of the production of security *through* data. I will look specifically at two levels of production. The first regards what Lindskov and Monsees (2019: 27) term the "social production *of* technology", that is, the social processes through which an information infrastructure, respectively, gets constituted and in

turn generates effects on the given order of things. This first stage highlights the developmental process through which political categories and security logics become embedded in data infrastructures.

Especially, it is a process that involves multiple human and non-human elements – for instance, EU bureaucrats, security experts, servers, network cables, interfaces, and algorithms – that are being tied together in the constitution of a security system. While the second – that is, the "social production *by* technology" (Lindskov and Monsees 2019: 29) illuminates the agentic capacity of information systems, that is their ability to be productive and generate the desired effects behind their implementation. Consequently, in order to offer a socio-material reading of the life of information infrastructures in the EU AFSJ I provide a thick description of the technical, social, and political conditions and rationales involved in the design and implementation of different AFSJ information systems. By treating technology as an active participant and not simply as a passive and inanimate tool at the disposal of human users, this STS-inspired approach offers a promising perspective for examining heterogeneous, situated, and contingent security processes, such as data practices. Indeed, the three-steps model, borrowed from Lindskov and Monsees, functions as an analytical devices useful to make sense of the rationales and practices behind the development, adoption, operation, and stabilization of different information infrastructures in the AFSJ domain.

1.2. The social and material construction of digital data

I suggest that studying the life of technologies – how they are developed, assembled, and ultimately used for a specific security purpose – requires a broader view than the sole observance of the object. According to CSS scholars, context matters for the ways in which socio-technical systems are produced. Therefore, an empirical engagement with sites of practices requires to situate technology in their political, social, and institutional dimensions. This research builds upon this view by developing a genealogical account of data production that traces the complex web of relations and stakes involved in the constitution of information infrastructures of data exchanges for law enforcement purposes. Understanding the production of security knowledge in terms of a process demands so-called "data infrastructure literacy" (Gray et al. 2018: 1). The growing development of digital data infrastructures raises questions about the nature of data, how they are being produced, organized, analysed, and employed.

Especially, there is a pressing need to better understand how various forms of digital data become embedded and set to work within different security sites (e.g., border control agencies, law enforcement bodies, etc.).

To clarify these aspects, my research uses data practices as the focal point – 'object' – of analysis in order to deconstruct how data are entered, selected into a particular form, related to each other and how they become information and ultimately knowledge. To reflect this processual character of knowledge formation, I combine genealogical research with visual network analysis (VNA), that allows for a traceable mapping of data practices. In general, the adoption of a genealogical method enables to trace out the contingent formation and unfolding of multiple, complex, and contradictory iterations of an assemblage (Kitchin 2014). To grasp the agency of technology in a transversal way, I re-elaborate the concept of "data lifecycle" (Kaufmann 2019; Kaufmann and Leese 2021) and use it as a heuristic device through which to unfold the web of relations in which data exchanges are embedded. Tracing the inherent workings of an object involves a "mapping exercise" that documents its life as well as its historical development (Leese and Hoijtink 2019: 144). This is why, I suggest, a genealogical approach to the study of the data lifecycle is best suited to deconstruct the complex web of discourses and practices that are central to the normative and organisational structures surrounding information exchange.

Research and notions from diverse disciplinary perspectives, such as CSS, STS, critical data studies, and computing already invite to consider data as socially and materially constructed artefacts and as generative of new forms of power relations at different interconnected security sites (e.g., Bellanova and Fuster 2019; Bigo et al. 2019; Kaufmann et al. 2019; Kitchin 2014). The focus of these inquiries concerns in particular how data are generated, analysed, and leveraged into insights and value. For example, Kitchin (2014) conceives data as the base of the knowledge pyramid: data precede information, which precedes knowledge, which precedes wisdom. Accordingly, they are raw elements that can be abstracted from phenomena, then measured and recorded. Furthermore, they are meaningful, "pre-analytical" and "pre-factual" since they exist prior to argument (Kitchin 2014: 3). More broadly, data are considered as the building blocks from which information and knowledge are created. To this regard, there are relatively numerous accounts that consider data as key inputs into information systems that paradoxically are implemented to make societies more secure, efficient, transparent, and

accountable by means of monitoring, discipline, and control (e.g., Lupton 2015, 2016; Matzner 2016; Scheel et al. 2019).

The tendency to present data in immaterial terms as an instrumental entity is thus giving way to an emerging literature among critical data studies that foregrounds the value of digital data *before* it is translated into actionable knowledge through computing practices (e.g., Bellanova and Fuster 2019; Kaufmann 2020; Kaufmann and Leese 2021; Lupton 2015 and 2016). This view opens up a new research space that shifts the focus from the end-product (e.g., data derivatives, patterns, mosaic) to the raw material with which different digital security compositions are assembled. For instance, Bellanova and Fuster describe digital data as "debris" that make up different governing rationales (2019: 364). Their work invites to explore the diverse ways in which data are "recycled" and "composted" to form different security compositions (Ibid: 355). In line with this scholarship, I regard data as the object of inquiry and, even more crucially, as lively elements of knowledge production that do not just exist and produce effects in and of themselves. Rather, they have to be generated and computed in order to produce the desirable output (e.g. identify "risky" patterns of behaviour, or stop suspicious individuals at borders).

1.2.1. "Making" and "un-making" data

Along this line, this research seeks to broaden the CSS and critical data studies scholarship by offering a contribution that accommodates the study of security practices as matters of data compositions. In order to account for the diverse ways in which data become part of an information system, I draw attention to the distinct processes of data structuring, curation, and integration. More specifically, two tropes – "composting" and "computing" – proposed by Bellanova and Fuster (2019: 347), permit thinking of data in their process of becoming. Both tropes assume that the materiality, meaning and productivity of data should be investigated in a situated manner. The theoretical trope of "compost" – from "componere", that is, "put together" – invites to think of digital data as lively elements that are composable into a "mosaic". The notion of "mosaic" is understood as the outcome of the process of "piecing together" different entities (Amoore 2013: 84; see also Dijstelbloem et al. 2017). Specifically, the operation of "composting" refers to the transformation of data into storable and actionable elements through computing techniques (Bellanova and Fuster 2019: 347). This operation lays down the material conditions that enable security compositions to come into being.

The theoretical trope of "computing" – from "com" and "putare", that is, "bringing together" – concerns the connections between compost, compositions, computers, and data. Specifically, through the process of "computing", digital data are 'enriched with further meta-data, stored away and then mobilised in support of an investigation' (Bellanova and Fuster 2019: 354). As digital data are "brought together" to form a security composition, their ontology is constantly modified in the encounter. Specifically, digital data act as "compost" when extracted from larger datasets for speculative security action. They are then reinvented, re-assembled and ultimately computed to form the material basis of digital security compositions. Taken together these two tropes (composting and computing) enable to better apprehend the role that digital data come to play in the fabric of security knowledge. Informed by these considerations, this research aims to elucidate how different categories of data sources are recycled across EU AFSJ information systems to inform law enforcement practices. Data are thus rendered re-composable across different sites of "anticipatory governance" (see Amoore and De Goede 2005; Aradau and Blanke 2017a and 2017b; Aykut et al. 2019; De Goede 2012; Egbert and Leese 2020; Leese 2014).

To this regard, Kitchin (2014) further distinguishes between information and knowledge. The former is the accumulation of associated data that is transformed into knowledge through processing, management, and usage. He explains that information is structured data that has gained currency as a commodity. Whereas knowledge is actionable information, that is the 'know-how' used to formulate policy actions. Consequently, in my elaboration of the "lifecycle of data", data figure as basic inputs into processes such as categorising, matching, profiling, and sorting that in turn create knowledge *from* the data, to inform different security practices. In line with Foucault's (1981) then, data constitute a form of 'power/knowledge'. Although their value is realised only when information is extracted, they constitute "key ingredients" for constructing political agendas and legitimising evidence-informed narratives and counter-discourses (Kitchin 2014: 12). For instance, data are collected, processed, and analysed with the aim of creating lists of threats and especially for identifying suspects. Nevertheless, they are never entirely raw since their production is underpinned by systems of thought, forms of knowledge, governmentalities, and legalities. The transformation of data into politically-relevant information is performed through the analytical practices of security professionals that involve the collection of information and the performance of algorithmic calculations. Therefore, data practices are not carried out independently of the ideas, instruments, practices, contexts, and knowledges used to generate, process, and analyse data (Scheel et al. 2019).

These theoretical insights have several implications for researching the genesis, constitution, functioning and sustenance of information exchange in the EU AFSJ. First, understanding data as unstable elements of security compositions implies that data are in a constant process of "becoming something" (Bellanova and Fuster 2019: 347). Recycling information enables to form the material basis of different digital security compositions that ought to be studied in a situated manner. The engagement between STS and critical security studies offer empirically rich examples of such critical attentiveness to situated security practices (e.g., e.g., Acuto and Curtis 2014; Bellanova and Duez 2012; Davidshofer et al. 2017; Hoijtink and Leese 2019; Jeandesboz 2016; Leese 2015). The central theme in this literature is that digital technology allows for the production of security knowledge, and thus informs the practices of a wide range of actors, such as border management, asylum authorities, police officers, law enforcement and intelligence services. This view implies that attention should be paid to security actors' organisational efforts underpinning the employment of data for different purposes. Along this line, this research questions how data come to be part of security systems through different practices of abstracting, processing, and recycling data into different entities depending on the purpose of use.

Both the notions of 'performativity' and 'enactment' highlight the socio-material character of knowledge production. Inspired by the works of Annamarie Mol (2002) and Karen Barad (2007), Glouftsios and Scheel (2021) explains how the performative effects of information systems derive from the possibility to produce and re-produce the ontologies of both objects and subjects through knowledge practices. In particular, the notion of 'performativity' highlights how their ontology is not fixed, or pre-given, but rather, it is the result of reiterative processes of interactions between human actors and technological systems (Glouftsios and Scheel 2021). Similarly, the conceptual tool of 'enactment' assumes that the ontology of subjects and objects making up transnational circulations of data 'constantly mutates and multiplies in practice' (Mol 2002: 32; see also Glouftsios 2018: 187). As data infrastructures create a 'visible fabric for data exchange', they provide state authorities with a new form of 'digital' power that enables them to attune their decisions to the body of knowledge generated by information systems (Bellanova and Glouftsios 2020: 4). Therefore, data infrastructures are not neutral since they materially, legally, and politically support specific ways of enacting security.

Second, incorporating the material dimension in the analysis of knowledge production highlights the processual character of its formation, that, in the security realm, is 'creative and constructive', rather than 'routine and habitual' (De Goede 2018: 38). Taken as a starting point, this reasoning opens up a new avenue for theorising and researching the role of data practices in the constitution of security interventions. Conceptually, it enables to move the understanding of security knowledge beyond the notion of the routine, to focus on the sequenced mode by which security knowledge is generated and unsettled in practice. To this regard, De Goede has introduced the concept of 'security chain' to suggest that: "security knowledge is often not settled, in the background, routine, and unspoken" [..]. "It is formed in a situated and subjective manner, across public and private spheres" (2018: 38). Understood as a reiterative process of translations and deliberations, the locus of security judgements is therefore dispersed, as it depends upon the agency of both technical infrastructures (e.g. computer networks, communication channels, and software applications) and human actors (e.g. data scientists, software developers and end-users).

1.3. How digital data come to matter

Based on these analytical insights that favour portraying data as a "lively objects" (see Lupton 2015 and 2016; Kaufmann 2020), several governmentality-inspired studies have explored how the collection and processing of data are mediated by technologies of control (e.g., Bellanova and Duez 2012; Douglas 2012; Glouftsios and Leese 2023; Oliveira and Gabrielsen 2022; Pickering and Weber 2006). In these accounts, digital data are regarded as translations of behaviours into information that in turn create the conditions of possibility to govern people and things. This line of scholarship has particularly focused on issues concerning surveillance, privacy, and anonymity along with other ethical and legal issues that the generation and use of data engender. CSS researchers were among the first to study how data-driven systems reshape the governance of the international through the deployment of biometric control and the multiplication of databases (e.g., Bellanova and Duez 2012; Bellanova and Glouftsios 2020; Dijstelbloem and Broeders 2015; Jeandesboz 2016). Their work generally develop situated analyses of digitised control apparatuses and of the subjects that they target. For instance, Scheel et al. (2019) describe how data practices are mobilized to produce knowledge on migration in support to the biopolitical control of populations crossing the EU borders. Other critical accounts further explore the establishment of the Schengen area as a "controlled space"

of transnational circulations built upon ICT infrastructures that allow national authorities to share information on suspect mobilities (Bellanova and Glouftsios 2020: 4).

Among these critical accounts attention is paid to 'both the will to *govern through data* and the will to *govern data*' (Bellanova 2017: 333). The main contribution of these studies consists into offering an approach that broadens the study of security to the accommodation of different forms of knowledge production. Through this research then, I seek to enter in conversation with these common threads about infrastructural politics, across STS, critical security studies and political geography, that increasingly question EU data infrastructures and their deployment. Central to such an inquiry is the ongoing "datafication" of society through processes of translation of the "offline" world into "virtual" data (e.g., Broeders and Dijstelbloem 2016; Scheel et al. 2019; Van Dijck 2014). In this regard, scholars from critical security and surveillance studies have noticed how policy problems are more technologically mediated and "datafied" along lines that favour governing through a "statistically constructed future" (Broeders and Dijstelbloem 2016: 14). Similarly, critical data studies scholars have drawn attention to the processes by which digital data come to matter through its deployments, uptakes, and production (see Lupton 2015; Kaufmann 2020; Kaufman and Leese 2021). For example, Ruppert and Scheel (2019) take on an historical and sociological approach in the analysis of datafication processes by focusing on the social dynamics that give meaning to data practices. In these accounts, digital technologies figure as performative machines that record multiple behaviours and interactions (both online and offline), and translate these into data to be further processed (Logan 2017).

More recently, this strand of literature has started to develop critical interrogations of how the use of algorithms affect the modes and targets of regulation in problematic ways (e.g., Amoore and Raley 2017; Aradau and Blanke 2017b; Bellanova 2017; Bellanova and De Goede 2020; Leese 2014; Yeung 2018). The notion of 'algorithmic governmentality' refers specifically to 'the governance steered by learning machines and intelligent computing systems able to automatically capture and process data from multiple sources' (Bellanova 2017: 330). Accordingly, peering into data practices requires to consider techniques of data mining and predictive analytics – borrowed from computer science and then remediated to the security field (see Amoore and Raley 2017; Aradau and Blanke 2017b; Lyon 2016; Van Dijck 2014) – in order to understand how data inform different modes of "making" security. This is particularly crucial since modern methods for collecting, processing, managing and analysing

large quantities of data are not confined merely to the IT domain, rather, they have become central practices of governance (Ruppert and Scheel 2019). By problematizing EU data infrastructures and their deployment then, it is possible to derive how crimes, hotspots, and offender groups are prioritized through data, and especially, digital data (Kaufmann et al. 2019). To this regard, Amoore and Raley note that 'human and algorithmic systems have co-evolved in complex processes of techno-genesis that have transformed security practices by instituting new logics for governing populations' (2017: 7).

However, thinking in "IT terms" is necessarily complicated by the ambiguity of digital innovations: what is known, negotiated, and targeted as a security issue is mediated by a plethora of techniques – from pattern recognition to anomaly detection – mobilized to produce knowledge for purposes of its management (Aradau and Blanke 2017b; see also Matzner 2016). Accordingly, algorithms have become active contributors to the production of security knowledge (Kaufmann 2019). By providing ways of visualizing, calculating, and knowing about future events security they carry the promise of creating "meaningful information for targeted security decisions" (Bellanova and Fuster 2019: 346). They are in fact framed as matters of technocratic expertise that enable to enumerate, classify, quantify, and visualize knowable categories of people and interesting relations among datasets (Matzner 2016). CSS scholars that have produced empirical accounts on the politics of design and implementation of algorithmic systems have attempted to resist the idea of conceiving them as "black boxes" whose production is entirely opaque (Leese 2014; Matzner 2017). Bellanova and Fuster (2019: 364), for instance, suggest to focus on the subject of security compositions, that is, digital data and to view them as "ecosystems" of embodied and embodying elements that can be abstracted, recycled, and ultimately used for different purposes. Another promising way of inducing visibility to the inherent opaque workings of information systems, I suggest, is by unearthing the political categories embedded in protocols, regulations and policy documents, in order to reveal how they have influenced the setup and implementation of AFSJ information exchange schemes and how security is forged through them.

1.3.1. Risk, algorithms and anticipatory knowledge

The growing body of research that is concerned with the increased datafication of society also demonstrates how data practices are linked to the rise of pre-emptive security logics that call for the pro-active addressing of risks (see Amoore 2014; Amoore and Raley 2017; Aradau and Blanke 2017a-b; De Goede et al. 2014; Egbert and Leese 2020; Kaufmann et al. 2019; Leese

2014). According to Rose (2001: 7) risk can be understood as a "family of ways of thinking and acting, involving calculations about probable futures in the present followed by interventions into the present in order to control that potential future". The possibility to perform calculations reveals the emergence of a "digitally enhanced" logic of control that derives from the ability of information systems to store, analyse, and process immense volumes of data at any point of their lifecycle (Glouftsios and Scheel 2021: 8). The high-tech nature of the instruments deployable by security authorities has indeed promoted a shift, first from reaction to prevention, and then, from prevention to pre-emption and calculation (see Amoore 2014; Amoore and Raley 2017; De Goede et al. 2014). This research takes account of such anticipatory logics by questioning how they have informed the setup of AFSJ information infrastructures and in turn how they have become so entrenched in the cybernetic-like loop of data extraction, knowledge generation and security regulation.

As a result, it is crucial to consider how the reliance on different technological infrastructures enables to undertake security-related decisions and in turn informs different modes of "making" security – increasingly "data-driven". Enacting predictions through calculability indeed offers new ways of rationalizing human behaviour. In the case of data-driven systems, many bits of data are extracted, compared, and processed to create novel distinctions, deviant groups and to build the basis for taking action in the present (Matzner 2017). The performance of calculations on digital data is then used to rationalize decisions about whom to act upon, resulting in new forms of subjectivation. While the power to subjectivise is based on the collection of data "in bulk", the ultimate use of such data enables to produce 'unique verdicts rather than generalizing judgements' (Matzner 2017: 38). This in turn has led to the emergence of individualized approaches to predictive policing, security checks at borders and other security interventions. For instance, in the case of border checks at the airport, even a single data-based judgement at the border can exert subjectivising power by allowing, restricting, or denying entrance to an individual. As Rouvroy puts it: "Algorithmic governmentality […] attunes the actions to be taken in the physical environment to the predictions contained in the informational body" (2013: 157).

This new form of subjectivising power reveals an augmentation in the surveillant capacities of security agencies and accentuates the extent of the reliance on information infrastructures for security governance (see Bunyan 2010; Haggerty and Ericson 2000; Lyon 2003, 2014). Cukier has coined the term "dataveillance" in reference to the replication of every aspect of sociality

into quantifiable data for purposes of anticipatory analysis (Cukier and Mayer-Schonberger 2013; see also Amoore and De Goede 2005; Van Dijck 2014). As Lyon suggests, this mode of surveillance is complemented by the implementation of a complex big data architecture that comprises software, codes and algorithms harnessed to the production of data subjects (Lyon 2016; see also Janssen and Kuk 2016). The performance of such technologized form of observation has implications for how we come to study data and their circulation across different information infrastructures. Especially, anticipatory expertise spans a variety of different scales of governance and policy domains at the local, national, and transnational level. Many issues of crime control have become particularly central to the transnational level, calling for its incorporation in the analysis of anticipatory security governance (see Aradau and Blanke 2015; Aradau and Blanke 2017a; Aykut et al. 2019; Leese 2014). In terms of research, then, it is crucial to focus on competing dynamics of knowledge production in order to understand how security interventions are shaped by the central features of policymaking in a given domain.

Also crucially important is to examine how, through software harnessed to the collection of data "in bulk", data are turned into resources that can be mined, enriched, and repurposed in the creation of multiple cycles of uses (Van Dijck 2014). This perspective incentivises the adoption of the analytical lens of the "lifecycle of data" (Kaufmann 2019) to study the "making" of security through data practices. The "data lifecycle" is particularly concerned with the circumspect collection of data, then stored into databases only temporarily, yet, with the prospect to cite a range of information in different sites of authority, at any time in the future (Matzner 2016). McCulloch and Pickering have conceptualised this shift towards anticipatory modes of governing in the form of an 'antithesis of the temporally linear criminal justice process' (2009: 632). Instead of commencing from the presumption of innocence and then progressing through discrete stages: 'investigations, evidence collection, charge, trial and ultimate punishment', preventative interventions prescribe to act in the present in order to tame the possibility that a criminal act materializes in the future (2009: 638). By prioritizing the detection of patterns, the criminal act itself loses its salience as the instant that defines criminality (Matzner 2017). The criminal, as it is traditionally understood, is now the product of the collection of data footprints in a form that renders them comparable to detect delinquent individuals before they commit a crime. These insights open up new avenues for research around the extent to which the governance of subjects and populations depends on the monitoring, control, adaptation, and repurposing of data contained across different information infrastructures.

Conclusion

This review had the objective to engage the multiple sub-fields that span critical security studies (CSS), science and technology studies (STS), surveillance studies and governmentality studies in order to set the stage for the conceptual and theoretical contribution of this research. The growing trend in academia to peer into datafication technologies has indeed paved the way to hybrid approaches within security studies that sought to redress the interrelatedness between security and technology (e.g. Bueger and Gadinger 2018; Douglas 2012; Hoijtink and Leese 2019). Central to such transdisciplinary accounts is an engagement with data practices associated with information systems and mechanisms for the exchange of information. What I call the entry, processing, archiving, analysing, and sharing of data are essentially operations through which security comes into being. These practices matter in the context of international security since they reveal how the "making" of security is dependent on the "(un-)making" of different data categories. Accordingly, it was crucial to review the literature that has emphasised the importance of data practices for the constitution of the international (e.g., Acuto and Curtis 2014; Bellanova and Duez 2012; Bigo 2014; Davidshofer et al. 2017; Hansen 2006; Scheel et al. 2019). These disciplinary fields, in particular CSS and STS, have developed a conceptual toolbox useful not only for researching technology in IR, but more broadly, for addressing how high-tech information infrastructures have come to shape and make up our world by reconfiguring security governance at large.

Most of the insights offered by STS foregrounds the sociotechnical nature of security practices, from border and migration management (e.g., Côté-Boucher 2020; Dijstelbloem and Broeders 2015; Glouftsios and Scheel 2021; Leese and Wittendorp 2017; Pickering and Weber 2006) to predictive policing (e.g., Egbert and Leese 2020; Leese 2014; Kaufmann 2019; Kaufmann et al. 2019), and attend to the more or less visible aspects of the interaction between human actors and technologies. STS-informed approaches are mobilized throughout this research to study the socio-technical nature of the "co-production" of security knowledge (Jasanoff 2004). Within this strand of conceptual resources, I rely especially on Actor-Network Theory (ANT), since it enables to overcome the 'agency/structure' binary in the study of data practices by considering agency as 'co-constituted' by the interactions between humans and technologies. In particular, by ascribing agency also to 'non-humans' – such as objects, material structures, and technologies – ANT favours thinking of the "lifecycle of data" as a web of relations where both humans and technologies assume an active role (Amoore and Raley 2017). Along this

line, I consider the development and functioning of data infrastructures as inherently 'socio-technical' since they result from the associations and interactions between security actors and technological artefacts that together form "practice-networks" (e.g., Latour 2005; Law 1992; Mol 2010).

Accordingly, a practice-oriented approach applied to the study of digitally-mediated security suggests to look at the contingent relations between heterogenous human and non-human elements – such as software developers, end users, and technical devices – that together take part in the lifecycle of data. Such an approach highlights also the processual character of knowledge production, that, rather than being linear and smooth, it is subject to political controversies and normative frictions (see Côté-Boucher 2020 and De Goede 2018). I drew particular attention to the notion of 'enactment' that is descriptive of the constituent and generative moments through which realities – in my case information infrastructures – are brought to life (Barad 2007; Mol 2002). Informed by these theoretical strands, I conceptualised sites of production of security knowledge as 'socio-technical' environments, where human and non-human actors produce new, quasi- automated forms of social control. Equally, I aimed to provide a more profound engagement with the role of data in the constitution of data infrastructures: in line with new materialist approaches, I conceptualised data as 'lively' inputs that are continuously analysed, interpreted, categorised, and curated by different security actors (Lupton 2015 and 2016; Bellanova and Fuster 2019; Kaufmann and Leese 2021). These processes are mediated by different technologies – such as hard disks, processors, desktops, data analysis tools, etc. – and thus they are socially and materially constructed (Glouftsios 2018; Hoijtink and Leese 2019; Lindskov and Monsees 2019).

The conceptualisation of technology as an active participant in heterogenous and situated security processes offers a promising perspective for assessing the wider societal and normative consequences that emerge from data-driven governance. Even more crucially, it favours studying the lifecycle of data in a situated manner, by considering the institutional, normative and organisational contexts behind the development and implementation of information infrastructures. On the basis of the theoretical and conceptual insights offered by STS and CSS, it is possible to synthetize the role of technological systems across different domains, such as counterterrorism and police cooperation and the management of global mobility and borders, among others. To shed light on the logics that drive the setup and functioning of different infrastructures for the collection, processing, analysis and sharing of data, I also engaged the

literature related to surveillance studies and anticipatory policing (e.g., Amoore and De Goede 2005; Aradau and Blanke 2015; Aradau and Blanke 2017a; Aykut et al. 2019; Leese 2014; Van Dijck 2014). This strand of scholarship is concerned with illustrating the evolution of surveillance practices from the traditional panoptic observation of the human body – for example, in the prison setting discussed by Michel Foucault (1975) – towards a 'technologized' form directed at monitoring digital footprints (e.g. Murakami 2007). It is therefore equally important both theoretically and conceptually since this literature engages crucial debates that regard how dynamics of anticipatory expertise have become embedded in security interventions and in the governance of contested policy issues.

The concepts discussed in this review are constantly mobilized throughout the empirical analysis in order to illuminate various aspects related to the mediation of both digital technologies (technicalities) and legislative and non-legislative provisions (socio-political and legal considerations) in the "making" of security through the "un-making" of data. Thus framed, this research makes three distinct yet interrelated contributions to the literature engaged. First, within the currents of STS and CSS, I seek to contribute to data infrastructure literacy, by carrying out a practice-driven analysis of the lifecycle of data, honing, in particular, on the normative and technical processes that data undergo in order to be "recycled" for different uses. Second, in terms methodological approaches developed within these two strands, I provide a practice-oriented approach by recurring to visual network analysis (see Chapter 2 on methods) in order to study visually the lifecycle of data as a network of practices. Third, in the context of EU studies, I complement current research on the infrastructural politics of European integration in the EU AFSJ (e.g., Glouftsios 2021; Bellanova and De Goede 2020; Jeandesboz 2016) by providing an empirically-oriented analysis of four case studies in order to demonstrate that security governance at the EU level does not only involve policy-making and legislation-drafting, but also the development, deployment and use of infrastructures that interconnect Europe. Empirically, I attend to the EU instruments that, to date, have been introduced in the AFSJ domain in order to step up information exchange and cooperation among law enforcement authorities.

Chapter 2

Investigating the "Lifecycle of Data"

Introduction

One of the core arguments that I want to elaborate through this research is that cross-border data exchanges are directed in particular ways, not only by digital technologies, but also by provisions regulating access, storage and use of information for security-related purposes. There are several reasons for conducting an empirical inquiry into the production of data for law enforcement finalities. First, this conceptualisation has an important implication for how we come to understand and study the making of international security. Lately critical scholars have devoted much attention to discussing information systems, databases, and related security practices (e.g., Aradau and Blanke 2017b; Bellanova and Duez 2012; Bellanova and Glouftsios 2020; Dijstelbloem and Broeders 2015; Glouftsios and Scheel 2021). Some of the preoccupations of existing debates concern the importance of data for the setup and maintenance of the EU information infrastructure as well as for policy-making in the EU Area of Freedom, Security and Justice (AFSJ). The collection, processing, analysis, and sharing of data are essentially practices through which security comes into being. These practices matter politically because they produce knowledge that forms the base upon which "suspicious" criminal activities are sought to be detected and prevented (see Aradau and Blanke 2017b; Davidshofer 2017; Kaufmann et al. 2019; Lyon 2016). They matter also socially because of the impact that they have on the life chances of data subjects (see Bigo et al. 2019; Gabrys 2019).

Second, rather than focusing exclusively on information systems as security sites, I suggest to pay close attention to both the practices related to the gathering, processing and sharing of data

and the legal frameworks that regulate such practices. I investigate both data practices and legal provisions by attending to the concept of "data lifecycle" (Kaufmann 2020; Kaufmann and Leese 2021): how certain data categories (e.g., identity, reservation data, biometrics, etc.) are initially produced and how they are subsequently repurposed for policing purposes. In my own elaboration of the notion (see below), the lifecycle provides an analytical angle that avoids overly emphasising the role of technology in the "making" of security. Third, among academic literature that explores the nexus between security and technology (e.g., Acuto and Curtis, 2014; Amoore and Raley 2017; Jeandesboz, 2016; Leese, 2015; Oliveira and Gabrielsen 2022), the proposed research design enables to proceed bottom-up, from empirical observation to theory building, with the scope to understand how the extraction and use of data for law enforcement purposes are regulated through normative and technical arrangements behind data infrastructures. In terms of methodology, this design provides an incentive for adopting a liminal approach between the different methodologies developed within critical security studies, STS, and socio-legal studies.

Rather than constituting a limitation, such liminality created the conditions for meddling through the interstitial spaces of these disciplines and thus for accommodating a critical inquiry into the relation between normative and technological power in matters of knowledge production for security governance. To carry out the empirical analysis, I elaborated a multi-methodological approach to the constitution of the lifecycle of data as the object of research, that relied on extensive archival research and document analysis, as well as visual network analysis (VNA). The way in which these methods were combined enabled to constitute the lifecycle of data as a network of practices rather than purely as a linear chain of data exchanges (De Goede 2018). The aspects considered in this respect concern mainly the legal dimension, the communications channels and the technical instruments implemented to streamline and support information exchange in the EU AFSJ. Such methodological stance leaves space for investigating the multiple ways in which specific categories of data (e.g. identity and travel data) become part of crime prevention strategies and demonstrate that their lifecycle is influenced not only by digital technologies, but also by provisions regulating access, storage and use of information for security-related purposes. Accordingly, from the circumspect collection and processing of data to their use in a criminal investigation, multiple actors, institutional arrangements and legal frameworks are involved.

This chapter is dedicated to illustrating how I investigated the lifecycle of data methodologically and is largely divided in three parts. In the first part I start with a concise overview of the main features of this concept and I explain why I have decided to frame it as the object of research. In particular, I illuminate the meaningfulness of the words "life" and "cycle" in relation to the functioning of data exchange schemes and the performance of data practices. These practices are essentially multiple activities that "make" and "un-make" data, which include the entry, processing, analysis and sharing of data for policing purposes (Bellanova and Fuster 2019; see also Scheel et al. 2019). After that, I unpack the multi-methodological approach that I have developed for analysing the making and un-making of data through data infrastructures in a relational manner. The adopted approach relies specifically on two analytical pillars: a genealogical analysis and a visual analysis of networks of practices. In relation to these pillars, I identify three aspects, that is the *socio-political*, *legal* and *technical* conditions of possibility for the collection, processing and exchange of data at the level of EU AFSJ information systems.

Having outlined the methodological stance, in the second part of the chapter I provide a brief recount of how I gathered relevant qualitative material. Then, I define the main blocs of the empirical analysis and the criteria for the selection of the case studies. Following a discussion of the primary and secondary sources, I proceed with elucidating how I have used disparate forms of texts inductively in order to reconstruct the lifecycle of data for each of the four EU AFSJ information schemes considered. Moving on to the third part, I explain how I have elaborated the empirical material in consideration of the research tools selected, that is document analysis and visual network analysis. In particular, I address the specificities of each analytical approach in relation to the study of the complex linkages between data, technology and security. Finally, I move forward to presenting how I have composed and visualised the network of data practices out of the qualitative data gathered. I then conclude with some reflections on the value of practice-driven approaches for analysing and interpreting networks visually.

2.1. The "lifecycle" as analytical lens

Talking about "life" assumes that there is a temporality, a period between the birth and death of a living thing. While I do not contend the conceptualisation of data as a living object (see

Lupton 2015 and 2016; Kaufmann 2020; Kaufmann and Leese 2021), I question the use of the term "life" when referring to the multiple data practices that place AFSJ information schemes such as the SIS, Prüm, API and PNR in an environment of constant scrutiny. Verifying an identity requires the confirmation that the person you claim to be is actually who you are. Accordingly, crossing a border, booking a flight, being issued with a passport etc., are all instances that require you to claim your identity by releasing your personal data. The provision of personal data is not a one-time act but occurs reiteratively by directing data subjects to an assessment of their "risk" level. Data are in this sense never verified, but rather, they are ascertained once and then stored away in order to feed threat analysis and/or risk assessment. These considerations led me to subscribe to the idea of a circular trajectory in the life of data (Kaufmann and Leese 2021). A cycle is a series of events that are constantly repeated. However, in the case of data practices this repetition does not necessarily occur in an ordered fashion.

By acting on data, multiple activities – that include, the collection, storing, processing, and analysis – inherently intervene on the "life" chances of data, thus transforming their ontology. Through these practices data are constantly reassembled, recombined and repurposed across different security infrastructures (Bellanova and Fuster 2019). Repurposing means that the data gathered and stored away are first extracted, either in toto or only partially, and are then transferred for another end (see Bellanova and De Goede 2020; Hartong and Förschler 2019; Van Dijck 2014). Data are in fact captured and stored within different databases, at different moments and across different spaces. Intuitively, the trajectories of data exchanges are multiple, never linear and potentially limitless since data travel back and forth from one system to another. These considerations suggest that data are "unsettled" because their life never repeat itself in the same order, or by following the same trajectory. Accordingly, I have adopted the term "lifecycle" (see Kaufmann 2020; Kaufmann and Leese 2021) in order to better capture conceptually the multiple acts of power in the making and un-making of data.

Innes (2001) has coined the term "control creep" in reference to the repurposing of data in ways that differ from the initial intent underpinning their generation. This is generally achieved through technological solutions that render data transportable and thus "re-usable" entries across different domains. By attending to the analytic notion of "lifecycle", I seek not only to emphasise the technical dimension of data repurposing, but also, and more importantly, to shed light on the institutional and normative aspects of data production and transfer for policing

purposes. The distinct modes of ordering, organising, regulating and governing data are informed by a number of political rationalities before being translated into the technical specifications of IT systems (Glouftsios 2019). Simultaneously, such technical aspects matter politically since they enable a data-driven mode of governing (Leese 2014). For instance, IT systems designed for preventive purposes mediate security interventions by filtering out "risky" elements (e.g. individuals suspected of terrorism or organised crime) (Amoore 2008; Amoore and De Goede 2005; Lyon 2014). The effects of such filtering do not concern solely the data produced by IT systems, but impact also on the international mobility of those individuals considered "risky" (see Broeders and Dijstelbloem 2016; Glouftsios 2018).

There are several reasons for focusing on the lifecycle of data in order to understand how the collection of information is set to work for the investigation, prosecution and prevention of terrorism and other serious crimes in the EU AFSJ. First, such analytical attentiveness to data infrastructures as units of analysis enables to carry out a situated empirical study and to contribute to the literature on "data infrastructure literacy" (Gray et al. 2018; see also Glouftsios 2021; Hartong and Förschler 2019; Ruppert et al. 2013; Scheel et al. 2019). Especially, proceeding inductively allows to trace out the material and cognitive inner workings at play in the formation of their sociotechnical arrangements. Second, by focusing on data as the foundational element of different infrastructures, this research contributes to the nascent CSS scholarship (e.g., Bellanova and De Goede 2020; Dijstelbloem and Broeders 2015; Jeandesboz 2016; Kaufmann and Leese 2021) that analyses how security interventions are enabled through the exchange of data between different categories of end-users (e.g.. police, border guards, judicial authorities, etc.) involved in the management of security. Third, attending to the notion of "data lifecycle" enables to address both the technical and juridical complexities behind processes that render data transportable, re-combinable and actionable at the pan-European level.

Informed by these conceptual considerations, I have framed the lifecycle of data, and hence the data practices by which it is constituted, as the object of study. Central to such multi-layered analysis is an engagement with the multiple knowledges and technologies that have come to be associated with the exchange of information. The choice to represent data practices as "objects" is in line with the material turn taken in the IR research agenda in general, and critical security studies in particular. Object-oriented analysis, as a research method, allows for a traceable mapping that combines genealogical research with practice-driven approaches

(Mutlu and Salter 2012). In order to investigate the lifecycle of data in relation to the setup and operation of AFSJ information systems I propose a multi-methodological framework that relies on the tools of deconstruction analysis and visual network analysis (VNA). This combination represents a point of departure through which furthering the study of the complex linkages between data, technology and security. Below, I address the specificities of the first component of the methodology adopted, that is the genealogical approach.

2.1.1. Genealogical approach

The notion of "genealogy" refers to the type of analysis that I have conducted in the reconstruction of the lifecycle of data. Instead of reproducing an historical account of the emergence of the phenomenon observed (i.e. data practices), I conceive "genealogy" as a method through which to unearth the conditions of possibility for data exchanges in the EU AFSJ area. On genealogy, Bonditti et al. (2014: 163) stated that "genealogy should not be the writing of histories [...] but rather a critical intervention that unsettles such histories." Along this line, rather than aspiring to create a chronology of events, I aim at tracing the constitution of data practices, by drawing attention to the multiple dynamics that led to their gradual emergence. Three aspects co-constitute the genealogical analysis of the data lifecycle: the *socio-political*, *legal* and *technical* conditions of possibility that allow for the collection, processing and exchange of data at the level of EU AFSJ information systems. Therefore, the central concern remains the data lifecycle, honing on the variegated ways in which different categories of data give form to knowledge about terrorism and other forms of serious crimes and are then operationalised in the context of policing.

The adoption of a genealogical approach is regarded as central in order to reveal the contingency of ideas, practices and values behind the setup of AFSJ information systems. The exposure of the power relations and stakes involved in the constitution of data infrastructures and policy-making in the AFSJ domain turns much needed attention towards the often taken-for-granted discourses of security (as knowledge, discipline, and practice). In order to zoom out on the process of historical formation marked by continuities and discontinuities over the production and extension of different infrastructures, I sought to identify in each case study the *socio-political*, *legal* and *technical* conditions of possibility for the exchange of data at the level of AFSJ information systems. These conditions are highly interrelated. The technological solutions are in fact first envisaged at the political level, and then embedded into a series of legal requirements through regulations and directives which inform their technical features.

The material that inform the analysis of the *socio-political* and *legal* aspects (i.e. legislative proposals, feasibility and impact studies, directives, etc.) constitutes a valid source for examining also how security rationales and policy concerns are translated into the *technical* characteristics of IT system through discussions, negotiations, and redrafting of various texts (Jeandesboz 2016; Glouftsios and Scheel 2021).

The identification of the *socio-political* conditions has the objective of analysing the establishment of EU AFSJ information infrastructures in relation to the historical and policy processes that have shaped their function and scope. The focus of this part is very much dedicated to unearthing the EU logic in the set-up of different configurations of systems for data exchanges (e.g., centralised and decentralised databases, etc.). In particular, I examine first how central EU agencies organise the exchange of data at the pan-European level; second, how data eventually become operational at the level of national police authorities. In terms of empirical analysis, this procedure consisted in untangling how the obligations contained in the relevant EU directives (i.e. regulations and decisions on the establishment and functioning of information systems) entail inputs and actions by the side of public and private actors which then translate into the desired outputs for law enforcement authorities.

Broadly, the identification of the *legal* conditions concerns the progress that has been made since the beginning of the 1990s in improving cooperation between law enforcement authorities by streamlining the sharing of information. By looking at both legislative and non-legislative proposals, such as working papers, I reconstruct the legal basis that allows for the collection, processing and exchange of data at the pan-European level. In particular, I consider a number of treaties through which the EU sought to expand information exchange for the purpose of criminal investigations. Among these the most important are the 1990 Schengen Convention (OJEU 2000a); the 1995 Convention on the Establishment of a European Police Office (EUROPOL) (OJEU 1995b); the Hague Programme (OJEU 2005a); the Prüm Decisions (OJEU 2008b-c); the Swedish Initiative (OJEU 2006d); and the Lisbon Treaty (OJEU 2007c). These acts are the primary sources of EU law and include provisions that legally ground information exchange between Member States' law enforcement authorities with the objective to detect, prevent and investigate criminal activities.[5]

[5] Criminal investigation also includes law enforcement activities aimed at the collection of admissible evidence to be used during judicial procedures.

Lastly, the identification of the *technical* conditions has the objective of addressing how the production of data for security purposes is enabled by technical solutions that render data transferable and meaningful in different security contexts across national, organizational, and legal boundaries (Bellanova and De Goede 2020). In the analysis of the technical arrangement of AFSJ information systems, I considered, for instance, the data elements collected, the choice of software, the communication network for transmitting the data, and again, the analytic techniques used for processing them. These technical specifications along with the functional characteristics and scope of information systems, such as the possibility to enter and search for certain alerts, result from the rules laid down in EU regulations and decisions. This kind of documents reflect the security vision as it has been defined at the political level. Accordingly, by placing AFSJ information infrastructures in their respective institutional, normative and organisational contexts, I sought to scrutinize how different logics for enacting security (i.e. pre-emption, traceability, etc.) were first translated into material requirements through legislative acts and then into functional characteristics.

The possibility to act politically, materially, and computationally as granted to a multiplicity of agents, "makes" and "(un-)makes" the data, and hence constitutes the so-called "data lifecycle". Two considerations can be drawn in this respect. First, the definition of the purposes for which data are generated imply a political and normative process, along with a technical one. Protocols, organisational procedures, categories of data and data standards are first designed, negotiated, and debated at the political level before being implemented by data scientists in the design of information systems. Second, access to information has to be timely and accurate. It is necessary for law enforcement authorities to request and obtain information related to criminal activities from other Member States expeditiously, and for as long as it is necessary for the fulfilment of their tasks. The transfer may occur at different investigative stages – from the gathering (preventive stage) to the analysis of data for a criminal investigation (operational stage). As a result, transferring data for policing purposes, that is repurposing it, follows different arrangements and directions. These considerations shaped the criteria for the choice of the case studies among EU AFSJ information systems, and in turn influenced the choice of the elements to focus on.

In particular, the analysis of each scheme revolves around the identification of three core aspects: that is, the authorities involved in the different phases of the lifecycle of data, including the design of information infrastructures, their development and implementation, and finally

their use; the existing legal arrangements, as well as their loopholes, related to the transfer of information for security purposes; and lastly, the modalities of the transfer, concerning for example, direct requests for information, the spontaneous exchange of information, or again the electronic transfer of data through databases. These elements compose the main pillars of the empirical analysis. The multiple arrangements between them lead to assume that the obligations contained in EU directives and regulations direct the transfer of data in multiple ways. Between the initial site (i.e. database) where data are collected for a specific purpose, for instance, to establish the identity of travellers at borders, and the site where data are processed (e.g. in the context of on-going criminal investigations), multiple (human and non-human) interventions "act on" the lifecycle and in turn impact on its constitution and arrangement. This understanding further advances the conceptualisation of the lifecycle of data as a process informed by different logics, which in turn produce a network of distinct components of a normative, technological and organisational nature. Below I further dig into the notion of "network" and explain how it has informed the choice of a practice-driven approach to reproduce visually the lifecycle of data.

2.1.2. Data practices as "networks"

The notion of "network"[6] has been adopted within a variety of currents, such as STS, A-NT and technology studies as a means to trace the complex entanglements that constitute specific practices (see Attride-Stirling 2001; Knox et al., 2006). In line with this approach, I have applied the notion of network to the study of EU AFSJ information systems in order to represent the relational disposition of the actors (human and non-human) that participate in the lifecycle of data. This approach favours thinking of the relations among actors as they are established through the everyday exchange of data. It is important to remark that the multiple data practices, such as the entry, processing and analysis of data, are inherently socio-technical (Scheel et al. 2019) because they are performed by human subjects and non-human components.[7] For example, entering an alert via a police information system requires not only technical instruments (e.g., computer terminals, interfaces, internet connections, cables, etc.) but also the manpower of the officer in order to function properly and perform the tasks for

[6] The contributions of Law 1992; Law 2008; Latour 2005; Mol 2010 and Passoth and Rowland 2010 are particularly noteworthy for the development and advancement of the study of "networks".
[7] This understanding of data practices as activities has been elaborated in various concepts developed in critical studies and in the broader social studies literature. In Chapter 1, I briefly identified those concepts (e.g., the notion of "performativity" and "enactment", see Mol 2002, Barad 2007 and Law 2008) and entered in conversation with them, in relation to the constitution and formation of different "assemblages".

which they have been developed. These elements are all different technical and organisational units that create a bundle of contingent practices.

The personnel that works with these systems and that directly or indirectly participates to the lifecycle of data is highly heterogenous. These are mainly central European agencies, such as Europol, that gather and process data in the broader context of European security; and criminal investigators and judicial authorities that request such data to prosecute individuals. Within this network of actors, Europol functions as the central information hub through its instrument – Europol's Secure Information Exchange Network Application (SIENA). SIENA allows European competent authorities to exchange information in a swift, secure, and user-friendly way, with each other, Europol, and a number of third parties. Its databases facilitate cooperation by allowing EU countries to identify common investigations and providing the basis for strategic and thematic analysis. As a rule, information and intelligence are mainly exchanged via national central authorities or national contact points (INTERPOL National Units, EUROPOL National Units (ENUs), SIRENE Bureaux). Yet, a criminal investigation can involve parallel or sequential use of more than one communication channel which can be further combined with additional instruments.

Judiciary and law enforcement authorities generally rely on two main investigative tools to obtain direct access to data for criminal investigations – production and requests orders (European Commission 2018). These straightforward requests are not necessarily dependant on information systems as channels through which data are exchanged. The network of data practices is indeed far more intricate. In particular, the channels for information exchange depend on an intricate network of actors that comprise both human and non-human agents. These are mainly "material" actors in the form of regulations and directives; "humans" such as software developers, engineers, legislators and security authorities; and "technical" actors such as databases, cables etc. Their agency is conceived to be interdependent due to the relations in which they are embedded. Crucially, each of them have the power to re-compose the data in order to form the fabric of actionable security knowledge (Bellanova and Fuster 2019). They participate in fact to the multiple activities (e.g., entry, storage and processing) that intervene on the data in the creation of multiple cycles of uses.

Along this line, I conceive the lifecycle of data as a network of practices constituted by – and at the same time, resulting from – a multiplicity of actors and structures. This net is formed by situated human interventions and technical activities related to entering, updating and

consulting data through information systems. By travelling from one information system to another, it is the data that inevitably interrelate them and produce a network of contingent practices. Yet analysing the form of a network only makes sense if one considers both the visual characteristics (topological dimensions) of the network and the contextual information gathered through qualitative analysis (Decuypere 2020). The quality, accuracy and completeness of the empirical material are therefore of central importance. As Decuypere suggests, 'networks should be considered as being thick descriptions themselves' (2020: 84) and thus, once reproduced, they provide a visual basis useful to describe the relational composition of the practice under investigation. Accordingly, the narrative function of networks (Offenhuber 2010; Segel and Heer 2010) is particularly suited to reconstruct the lifecycle of data by examining the socio-political, legal and technical conditions behind the setup of AFSJ information systems.

In the resulting distribution of actors – that is, the network – humans and non-humans are placed in the same flat, relational field (Payne 2017). As Crossley posits, 'individuals are shaped by, and become social actors within, interaction' (2015: 66). The actors that participate in the lifecycle of data interact not only through the exchange of data, but also under multiple circumstances concerning for instance the institutional arrangement of both the normative and technical dimensions of information infrastructures. The design and development of an infrastructure are indeed subject to the mediation of different governance organizations in order to reach a technical, functional and institutional compatibility. These interventions are local, fragmented and confronted by unexpected frictions and deviations from the defined development path (Contini 2009; Velicogna 2014). These observations affirm the value of a visual method of analysis to chart the phenomena under investigation and to give insights into what matters most in the network of practices. Visual network analysis (VNA) is best suited to this objective. It is often described as an analytical technique that allows to exploratively visualise how practices are constant effects of relations, without having to invoke holistic or individualistic explanations (Packer 2018).

I further expand on the application of VNA to the study of the lifecycle of data in the last section of this chapter, in consideration of the methods deployed to reproduce the network of data practices. The question of "who" is involved in the lifecycle of data brings to the logical question of the "what and why" – which kind of data are stored in these databases and why? How is the collection, storage and processing of data related to borders and crime linked? Under

what conditions can information collected for a defined initial purpose, be used for others as well? What are the data protection and privacy implications of data repurposing? Addressing these questions constitutes one of the core tasks that I seek to attend by reconstructing the socio-political, legal and technical conditions of possibility for the exchange of data through AFSJ information systems. The results of the empirical analysis are then used on one hand, to differentiate between the characteristics, structure and composition of the data requested for policing purposes; and on the other, to identify how the enactment of security is context-dependent on the data infrastructures that combine varied data categories (e.g., dactyloscopic, identity and travel data, etc.) and types of security logics.

2.2. Gathering empirical material

To know which debates and documents are important for the collection of qualitative data, I began with an understanding of the AFSJ institutional context. Uncovering this practically, the first step consisted in retrieving publicly available information from the EU Commission portal (EUR-lex)[8] about the relevant acts (e.g., Hague Programme, Treaty of Prüm and Swedish Initiative etc.) and policy documents (e.g., directives, regulations etc.) that regulate information exchange in the AFSJ. The EUR-Lex portal holds a repository of current as well as historical (i.e. rejected or amended) documents, records and other sources relating to the activities and initiatives of the EU Commission and the Council and it can thus be conceived as an archive, although not in the strict, historical sense. Conducting archival research on this virtual repository involved specific analytical tasks that parsed out political categories, technical arrangements, institutional frameworks, and regulatory practices to understand how data exchanges have become operative as a political infrastructure for enacting security practices. Conducting archival research was key also to determine the extent to which the functional characteristics of information systems are reflective of the legal obligations, principles and values inscribed in EU Treaties. In particular, by considering the principle of availability Commission of the European Communities (2005) and of mutual recognition OJEU (2006d) I reconstruct the evolution of information exchange – its expansion to policy areas (e.g. law enforcement) as well as to data categories (e.g., dactyloscopic data, facial images, etc.).

[8] EUR-Lex grants access to a number of policy initiatives and related legislation, such as treaties, legal acts, case law, agreements, law-making procedures, among others.

The second step in the collection of the empirical material consisted in familiarizing myself with the language of the regulations and directives that have created the legal basis, either for strengthening information exchange and law enforcement cooperation among EU Member States or, for introducing new IT infrastructures. Policymaking in the EU AFSJ has indeed paved the way for the profusion of a vast number of different systems designed to ensure timely access to a wide range of data categories and to facilitate their transfer for the purpose of conducting criminal investigations and criminal intelligence operations across the EU. Hence, the EUR-lex archive functioned as a site of interrogation, rather than as mere depository of knowledge, through which I derived some of the elements that helped me to unpack the focal point of my research – that is, the lifecycle of data. About this conception, Lobo-Guerrero writes: "if archives are depositories of how things have been thought of and dealt with in a past, it means that they are spaces from which to interrogate those imaginaries" (2012: 121). Indeed archival research has been an aide to thinking and a source of material on the basis of which I defined the main pillars of the empirical analysis and the criteria for the choice of the case studies.

Central to the third stage then was gathering empirical material that could provide insights into the work processes – dealing with the collection, storage and exchange of data for law enforcement purposes – in order to discern the normative and organisational patterns behind the setup of data infrastructures. The EU Commission regularly produces review reports with the scope to assess the status of the functioning of information systems in relation to the objectives of their implementation. Yet, this third stage was hampered by the fact that most sources only shared insights into the legislative framework that regulates AFSJ schemes. Whereas information about their functioning was lacking due to the secrecy that generally surrounds the technical specificities of information systems. Therefore, one of the reasons for focusing on policy initiatives and to examine their legislative arrangement through regulations and feasibility studies is the structural opacity of information systems. Looking at their technical specifications and functional characteristics has thus far remained a challenge to most non-IT specialists. As a consequence, among academic researchers that study the nexus between security and technology, I had to come up with ad hoc research tactics to pierce through them.

In terms of methodology, I proceeded on the basis of a research design that encompasses the methods and tools of document analysis (Shah 2012; see also Hansen 2006), complemented by

visual network analysis. As a result, texts in general, and words in particular – derived, not only from written documents, but also from power point presentation and official speeches – constituted the primary sources from which I have drawn most insights about the aims and rationales underlying data practices and through which I have illuminated the political rationalities embedded in data infrastructures. In order to do so, I relied on several spread out sources of different nature. These were mainly legislations, impact assessments, feasibility studies, but also policy papers and reports issued by relevant agencies, like eu-LISA. Furthermore, I gathered and analysed documents published by the European Council and reports assessing the implementation of legislation, which are often published by the Commission. This liminality between empirical sources, rather than constituting an obstacle, provided the rationale for adopting a multi-methodological approach to the elaboration of the case studies and to the analysis of the material gathered.

2.2.1. Case studies selection

Before selecting the case studies, I reflected on which elements that characterise an information infrastructure – i.e. centralised or decentralised database, the type of data collected, and the purpose of implementation – are meaningful when reconstructing the socio-political, legal and technical conditions of possibility for the exchange of information at the AFSJ level. Accordingly, rather than starting from a working definition of what constitutes a "AFSJ infrastructure", I considered those parameters as a practical way for categorising AFSJ instruments and for comparing how different categories of data are collected, processed and analysed in the creation of a network of data practices. This choice partly derives from the fact that the AFSJ landscape is made up of distributed schemes and instruments, pointing to the fragmented nature of information management in the AFSJ area. These schemes comprise a variety of set-ups with different scopes, technical architectures, rules of access and data protection provisions. In the selection of the case studies I considered in particular the following aspects: the context and purpose of implementation; the legal and policy frameworks; the functionalities and scope of the systems; and the information exchange instruments, that is the channels used for sharing information.

Among this (non-comprehensive) list of elements for the selection of the case studies, the most critical factor was the purpose of implementation. I restricted the circle to those schemes that have been implemented in the AFSJ with the aim to preventing and combatting terrorism and other forms of serious transnational crimes. The scope of these initiatives is generally very

broad as it covers a wide range of criminal activities, and thus a variegated set of data sources, according to which individuals are targeted. The diversity of data subjects and of law enforcement actors having access to those data, create a blurring of boundaries between different categories, such as between security and migration, suspects and criminals, legitimate or illegitimate travellers; and in turn result in the wide variation between the scope of implementation of AFSJ schemes. On the basis of these criteria, I selected four cases: the "Schengen Information System" (SIS I, now SIS II) (Chapter 3); the "Prüm framework of cross-border information exchange" (Chapter 4); the "Advanced Passenger Information" (API) and the "Passengers Name Records" (PNR) systems (Chapter 5). All the technical instances related to the possible consultations and uses of the SIS II, Prüm, API and PNR take place in activities related to border checks, and the investigation and prosecution of terrorism and serious crimes.

Since one of the trends in the current AFSJ landscape is the move towards multi-purpose measures, distinguishing between systems that have been attributed a main or preferential purpose (i.e. border checks or law enforcement), and systems that generally are multi-purpose, and thus serve more than one policy area, is not effective. What is crucially important for the empirical analysis is not this distinction, rather, it is the comparative element between the four cases in terms of the data categories that are exchanged through these infrastructures, and the practices that allow for the variety of data sources to be re-composed and re-purposed in order to inform different policing practices. It is precisely this wide variation that endorses the idea of studying technology in a situated manner in order to reveal how security is context-dependent on different system configurations, and, even more crucially, on the (un-)making of different categories of data. Accordingly, the aim is to reconstruct the data generation process behind the implementation of the four infrastructures selected, honing on the variegated ways in which different categories of data give form to knowledge about crimes and are operationalised in the conduct of law enforcement investigations. Therefore, the central concern is to unearth the individual security logics that have guided their setup and that in turn enable a data-driven mode of security governance.

The first case study is the Schengen Information System (SIS I, now SIS II) (Chapter 3). This instrument has been operational since 1995, and it was later integrated into the EU framework by the Treaty of Amsterdam in 1999. The SIS is the mother of all existing and future pan–European IT systems which support transnational information exchange between law

enforcement authorities. It operates in two areas of competence: external border controls and police and judicial cooperation. This dual purpose has been institutionalized in the SIS II legal base through two legal instruments: Regulation (EC) No 1987/2006 (OJEU 2006c) and Council Decision 2007/533/JHA (OJEU 2007b) (hereinafter jointly referred to as the "SIS legal instruments"). Technically, the SIS has been configured as a centralised architecture, thus allowing direct access to the competent authorities for the purpose of identifying or locating wanted persons and stolen objects on the basis of the so-called 'alert data'. The data entered concern specifically information necessary for identifying the person or object that is the subject of the alert and clear instructions on what to do when the person or object has been found.

The second case study is the Prüm framework of cross-border information exchange (Chapter 4). The Prüm framework is an information exchange tool used for the search and automated comparison of DNA profiles, dactyloscopic (i.e. fingerprint) data and vehicle registration data. This scheme has fostered technical and scientific standardisation in the transnational exchange of genetic information and is thus regarded as key for detecting crimes (terrorism and other forms of serious organized crime) and for building the basis of criminal cases. Its architecture has been conceived in the form of a sub-set of national databases arranged on a decentralised basis. Therefore, in the absence of a centralised database that would grant "access" to the national authorities in each Member State, the Prüm is bound together by the information that travels through its network, and especially by its legal framework, rather than by any technical component. The normative "skeleton" of the Prüm is formed by the so-called "Prüm Decisions" (OJEU 2008b-c), which include obligations to establish databases (at the national level), as well as procedures and modalities for Member States' access to each other's databases in the context of cross-border law enforcement operations.

The third case study analyses jointly Advance Passenger Information (API) systems and Passenger Name Record (PNR) systems, thus forming one empirical chapter (Chapter 5). These systems collect passengers-related information and reservation data in support to travellers identification and risk assessment programmes. The collection of API and PNR data is regulated by two EU Directives: Directive 2004/82/EC ("API Directive") (OJEU 2004) and Directive 2016/681 ("PNR Directive") (OJEU 2016c). These provisions regulate the collection, processing, and use of identity and travel data from air passengers in the context of border checks and for the investigation, detection and prevention of terrorism and other forms of

serious crimes. The presence of the comparative element between API and PNR constitutes an added-value for analysing how commercial datasets created by airlines are turned into sources of security knowledge and are then mobilised for a wide range of different law enforcement purposes. Given the peculiar context in which passenger data are generated, that is, the commercial (airline) sector, the analysis of API and PNR contributes to understand how the private and public sectors are enmeshed in the implementation, functioning and use of security infrastructures.

2.3. Elaboration of the empirical material

2.3.1. Document analysis

To explore how security rationales are embedded in data practices, I have widely relied on texts as they result from written documents of different nature and origin. The primary sources used were mainly legal papers in the form of EU directives and regulations; EU reports on the functioning of information systems (e.g., impact assessments and feasibility studies produced regularly by EU bodies such as eu-LISA); and lastly, technical documents produced by commercial actors involved in the exchange of data for security purposes (e.g. airline industry, etc.). This material forms the backbone of the infrastructures developed in the EU AFSJ domain and thus constitutes the main bloc of the empirical analysis. Since they are matter of public record, I did not encounter any difficulties in retrieving these sources online, either through EUR-lex or from related websites that publish material about the works and activities of the EU Commission, eu-LISA, Europol, and other EU official bodies. As discursive artefacts, these texts are indicators of how security is understood and how that understanding has changed over time and is reflected in policy initiatives. Gaining access to them was therefore fundamental to attend to the main task of my research, that is determining how security is produced *through* the implementation of multiple infrastructures for the exchange of data.

Rather than reducing the content of these texts to categories and then code for patterns or emerging themes, I proceeded through a research design based on "deconstruction" (Derrida and Caputo 1997) as a tool for qualitative analysis. Deconstructing these sources served the purpose of exploring how the normative conditions inscribed in texts combine with material

elements such as information systems and communication channels, to become pathways of data exchange. On "deconstruction" as a method of analysis Derrida and Caputo write:

> "The very notion of unpacking something would imply enclosing, encapsulating, sheltering, and protecting, while everything in deconstruction is turned toward opening, exposure, expansion, and complexification". According to them, the very meaning and mission of deconstruction is "to show that things-texts, institutions, traditions, societies, beliefs, and practices of whatever size and sort – do not have definable meanings and determinable missions…".
>
> (Derrida and Caputo 1997: 31-32)

Inspired by this view, I conceived deconstruction as a form of textual criticism through which to unpack ideas and logics that at first appeared disjointed and disparate across the EU policy and legal documents gathered. Assuming that texts do not have a fixed meaning allowed me to intervene on the qualitative material in three ways. First, to identify hidden political categories and to reveal their implicit meaning. Second, to derive observations and break them down into component parts. Third, to expose the binary oppositions that underpin the EU ways of thinking about security and technology.

Peering into the technical aspect of data practices was empirically more challenging. The methodological and theoretical approaches favoured in critical security studies have often proved insufficient to the study of the technicalities of IT systems, which are more or less obscure. The technical aspects generally concern how information systems are designed, developed and produced and according to which standards. Yet access to technical documents is generally surrounded by a veil of secrecy in order to ensure that external developers do not reproduce the technological solutions of the private IT companies commissioned; or again, that the software implemented are not vulnerable to cyber-attacks. Additionally, investigating technical solutions requires specialized knowledge of the IT domain, and hence to be familiar with software, codes, algorithms and other technical components. To deal with this lack of transparency compared to other EU policy areas, I relied on secondary sources in the form of commercial reports (e.g. industry roundtables etc.), training manuals (e.g. CEPOL training courses[9]) and technical and administrative studies conducted on behalf of EU bodies. Although

[9] CEPOL is an agency of the European Union dedicated to developing, implementing and coordinating the training for law enforcement officials through a network of training institutes in EU Member States. CEPOL

only complementary, these sources proved to be a valid point of departure for studying the "making" of security through AFSJ instruments: how information systems are configured and re-configured through the exchange of information; and how they are put to uses other than those for which they have been designed.

Similarly to documents, power point presentations illuminated important aspects of the actors involved in the lifecycle of data. Especially, they revealed how infrastructures are assembled, implemented and used in certain standardized ways by commercial actors. For example, several power point presentations on PNR and API data were produced in the context of seminars on aviation security, or again, during technical workshops and symposiums[10] involving chief officials and coordinators of the API and PNR programmes within ICAO and IATA. These visual artifacts proved equally useful in revealing how data are gathered, processed and shared according to a particular security logic. This logic is that of the actors – generally private companies, such as the airline industry – that conduct impact assessment studies on behalf of the EU Commission. The EU is bounded by law to regularly produce reports on the status of implementation of information systems. Accordingly, by scraping the surfaces of some of these technical and administrative reviews, I have come across the names of the industries that participated into industry roundtables as well as parliamentary discussions in order to provide their own stake on the functioning of existing systems. These artefacts mixed visual and textual content that I have analysed qualitatively through the tool of deconstruction analysis.

2.3.2. Visual Network Analysis

The method that I have applied to the constitution of the lifecycle of data as a network of practices is a qualitative elaboration of visual network analysis (e.g., Latour et al. 2012; Venturini et al., 2015). I have come across this method by reviewing the literature on relationism within the currents of STS and ANT (e.g., Crosley 2015; Decuypere and Simons 2016; Knox et al. 2006). Since this approach has been applied only recently to the study of

provides frontline training on security priorities, law enforcement cooperation and information exchange through a dedicated online education platform - "LEEd" - open only to members of the law enforcement community. Source: https://www.cepol.europa.eu/about/the-agency

[10] See, for example, ICAO (2017b) Annex 9 to the Convention on International Civil Aviation, Facilitation, Fifteenth Edition, Montreal, October 2017; United Nations Office on Drugs and Crime (UNODC) (2018) Airport Communication Project (AIRCOP) Real Time Operational Communication Between International Airports to Fight Transnational Organized Crime, Including Drug Trafficking, and Terrorism, Egypt, November 2018; ICAO (2013a) Proposal for an ICAO Traveller Identification Programme (ICAO TRIP) Strategy, Working Paper, A38-WP/11, Assembly – 38th session, 17 May 2013.

networks, and thus, it allowed me to "think outside the box" about how to reproduce the lifecycle of data as a network. The notion of network is largely conceived within VNA as a method that allows to trace the complex entanglements that constitute specific practices in a qualitative manner (Attride-Stirling 2001; Knox et al. 2006). It is therefore well-suited to the reconstruction of the data lifecycle. Applied to my research, VNA served the purpose of creating and visualising the networks that bind together EU central agencies and national enforcement officials to the information infrastructures that they use for exchanging different categories of data (i.e. SIS II, Prüm and API and PNR). In particular, VNA allowed me to come to an integrated understanding of the relational composition of the data practices under investigation and to discern with greater depth the emergent interactions between various actors. In this vein, Decuypere (2020: 74) affirmed that: 'VNA is concerned with the visual rather than the structural (social) properties of networks and offers a conceptual toolkit to analyse and interpret these visual properties'.

The process of data collection is central to VNA since the resulting visualisations are contingent upon the quality, systematicity and comprehensiveness of the empirical material gathered (Decuypere 2020). Accordingly, document analysis was key to investigating first, who the actors involved in the lifecycle of data are; second, how these actors gather, process and share data. This closeness to the practice level reminisces ethnographic approaches that equally emphasise the importance to study everyday actions and activities of both human and non-human actors (Fenwick and Edwards 2010). In Chapter 1, I explained extensively the necessity to take into account human beings and objects in order to fully apprehend the relational composition of networks. Transforming interactions between dispersed practice-networks into visual representations served the objective of understanding how security practices acquire meaning in their relationality with data practices and vice versa (Glouftsios 2018). As Latour posits, a network is "a concept, not a thing out there" (2005: 131). VNA is indeed exclusively concerned with describing the visual properties of networks, rather than attempting to provide contextualizing and/or explanatory factors for their emergence.

There is a growing number of specialized software that has been designed to support the creation of network-like visualizations. Among them, I employed an open source platform called Gephi.[11] By offering an accessible interface, Gephi allows to create and visualise networks in the form of maps or graphs. As Decuypere explains (2020: 81), 'Gephi spatializes

[11] Gephi (gephi.github.io)

practice based on a continuous interplay between forces of attraction and repulsion, where the importance of relations between actors prevails above the assumed relevance of these actors themselves'. Crucially, the network visualizations required a careful reflection on design choices. Before spatializing the inputted data as a set of dots and lines, I have created tables (for each scheme considered) – either in Excel or directly in Gephi – detailing the actors involved in the exchange of data, the type of relations between them, the databases used, and other contextual information. The crucial operations in this design phase concerned finding a suitable label for each node, as well as deciding which colours to use, which style, and which rules to follow to compose the network. I have done so by considering the individual elements that make up the SIS II, Prüm, API and PNR networks on the basis of the qualitative inquiry.

To obtain an interpretable visualization of the topology of each network, Gephi offered multiple algorithms. What was interesting is that different algorithms shaped the resulting networks differently and therefore highlighted distinct features. Specifically, I relied on three algorithms.[12] The first one is called "ForceAtlas2", and its core feature is to shape networks on the basis of the relations between indexed nodes (Jacomy et al. 2014). The second is "Fruchterman Reingold", a force-directed algorithm that models the graph drawing problem by a system of springs between neighbouring vertices (Fruchterman and Reingold 1991). The third one is "Yifan Hu", a multilevel algorithm that reduces network complexity (Hu 2005). At the basic level, these algorithms function by giving a repulsive force to nodes that are different from one another, which drives them apart. Nodes are normally bridged through edges that act as springs (i.e. connections). Once an algorithm is launched the disposition of nodes changes until it reaches the equilibrium between the forces of repulsion and attraction (Venturini et al. 2015). Such spatialization technique gives sense to the disposition of nodes by maximizing the legibility of the graph.

Having described the importance of design choices to network spatializations, the other crucial operation involved making sense of the resulting map. Since visual network analysis lacks the conceptual tools and the vocabulary to interpret the projection of networks (Venturini et al. 2021), the only way of proceeding consisted in observing the consistency between the insights that can be drawn from the visual properties of the spatialized network and the previous knowledge of the phenomenon it reproduces. The researcher is thus constantly engaged in this

[12] Note that I have not necessarily used all three algorithms to create the visualisations of each network. Depending on the structure of the scheme, I have used one or more algorithms to emphasise a specific visual feature of the resulting network.

"continuous iteration between observation data and interpretation of findings. […] Visual analysis is indeed meant to confront the enquirer to their data, to explore their networks, to question their ideas" (Venturini et al. 2015: 19). Yet, this does not entail that the visual investigation of networks cannot offer any surprises. One of the central features that generally emerge from the reading process are regions with a higher density of nodes – also called "clusters". According to the size and density of a cluster, it is possible to draw a number of conclusions on the nodes it contains vis-à-vis the other nodes which appear far removed from the central one or are located at its periphery. This stage offers the opportunity to identify which nodes are central to the network and thus to prompt insights into both its typology and topology.

Precisely because visual analysis displays the interconnections between human and non-human actors, it is best suited to reproduce the lifecycle of data as a network of practices. Therefore, by applying this technique to the study of the data lifecycle I not only aim to smooth out the complexities of the SIS II, Prüm, as well as API and PNR networks of data exchanges, but also to extend the marketplace of network analysis to the study of digitally-mediated security. In each empirical chapter I provide specific guidelines to explain how I have produced through Gephi the network visualisations for each case study. The guidelines include for example, the data entered, the steps taken to create Excel tables, the labels chosen for each indexed node, and the edges drawn – that is, the type of connections between nodes. The resulting spatializations consist of a combination of actors, implying that each network necessitates both nodes (i.e. actors) and edges (i.e. relations between various types of actors) in order to be operable. No one network is able to operate by means of human, material or digital actors alone. Therefore, each visualisation possesses an explorative function that allows to scrutinize the object under investigation and construct a particular interpretation out of the formed network (Offenhuber 2010; Segel and Heer 2010).

Conclusion

In this chapter I sought to explain how I investigated the object of research, that is, the lifecycle of data. My methodological choices were partly driven by new understandings of how "securing" takes place through the implementation of data infrastructures. I began to reflect on the "making" of security through infrastructures for the exchange of data after careful consideration of the means available for gathering the empirical material and of the activities

of data elaboration conducted. These two tasks contributed to inform the choice of the case studies, to develop the skeleton of the qualitative analysis, to outline the basis for conducting document analysis and to elaborate the visual reproduction of networks. The liminality of my research stems from the need to investigate *transversally* data practices, technologies and legal frameworks that form the backbone of data exchanges in the AFSJ. Thus, the resources used cut through multiple fields, such as critical security studies, STS, socio-legal studies and IT studies. These resources provided the rationale for adopting a multi-methodological approach through which to trace the constitution of security across institutional boundaries (e.g. Bonelli and Ragazzi 2014). Doing so required a pragmatic and practice-oriented perspective, which "involve[d] focusing on how security works in practice and what it 'does' in different empirical contexts…" (Nyman 2016: 132).

Accordingly, in order to reinvigorate the attention to security as a mundane, dispersed practice, I have developed a research design and methodological framework that sit at the intersection between different fields of study. In this vein, I structured the empirical analysis on the basis of two analytical methods: a genealogical approach and a visual analysis of networks. In relation to the first pillar, I clarified my personal interpretation of the notion of genealogy and showed how I applied it to this research. The notion of genealogy refers in particular to the approach that I have adopted in the reconstruction of the socio-political, legal and technical conditions of possibility for the exchange of data. Rather than providing a mere historical account, through a genealogical reading of data production I aim to account for the discontinuities, contestations and frictions over the production and use of data in the context of EU AFSJ information systems. Whereas the second methodological pillar, that is visual network analysis, highlights the importance of relationism to the investigation of the lifecycle of data. This notion is related to the practices, and in particular to the entry, processing, analysing and sharing, that "act on" the data in the creation of multiple cycles of uses. The necessity for relational thinking, and thus for thinking in terms of a "network", enables to account for the relations among the actors and technological objects involved in the lifecycle of data.

This complimentary approach ensures a stronger analytical accuracy in the study of the selected schemes. At the same time it provides a comprehensive picture of the actors and practices involved in the exchange of data. Especially, through this multi-methodological approach I trace the relations between, for example, the airline industry (in particular personnel from

ICAO, IATA, etc.), EU Commission officials, personnel from other EU agencies (i.e. Europol, Eurojust, CEPOL) and national police officers. The interplay between texts and the visual then is of central importance to illuminate the work processes of the lifecycle of data. Such work processes emerge only after considering the links among texts, such as between legislations and the reports published by the Commission, the Council, eu-LISA and Europol. If texts provide thick descriptions, the visual investigation of networks serves the purpose of mapping the links between concepts. Therefore, this dual approach is essential to reconstructing the socio-political, legal and technical conditions of possibility for the exchange of information in the EU AFSJ area, and in turn to examine broader processes of data-driven security governance by attending specifically to the ways in which different systems are assembled, implemented and used.

The choice to adopt this dual approach to the analysis of the empirical material serves two main purposes. First, to unearth the institutional and legal arrangements and the functional requirements that structure EU AFSJ information systems. Second, to represent these normative and organisational arrangements visually. Conducting document analysis of proposals, regulations, feasibility studies as well as of secondary sources, such as power point presentations, results from the need to set out the context in which EU instruments have been developed. While VNA offers a visual device useful to interpret such qualitative material empirically. On this basis, a genealogical approach to the constitution of the lifecycle of data complemented with a visual analysis of the network of data practices contributes to the methodologies developed by CSS scholars by providing a practice-oriented way to study digitally-mediated security in the EU AFSJ (Mutlu 2012; see also Austin 2019). Equipping this research with the means and resources necessary to deconstruct the complex web of rationalities, practices and technical elements that surround the production of data for policing purposes is indeed one of the central stages of this research. Accordingly, both the concepts introduced in Chapter 1, such as “assemblage”, “composting” and “computing” data, “actor/networks” etc., and the methodological choices outlined in this chapter, shape the analysis of the selected AFSJ information schemes (Chapters 3, 4 and 5).

Chapter 3

Towards EU Multi-Purpose Information Systems:

The Schengen Information System (I and II)

Introduction

The concept of "assemblage" (Lanzara 2009) – discussed in Chapter 1 – allows to evoke an imaginary of EU AFSJ information systems as a set of highly heterogeneous and loosely integrated elements. These systems are characterised by the presence of distinct components that have been designed and developed across different institutional, normative, and organisational contexts by a multiplicity of actors and structures (Velicogna 2014). None of them exercises full control over the development and implementation of a system. Rather, their activities form a network of situated interventions whose fragmented nature either halt the presumed linear path of the system's development or result in unexpected frictions and deviations (Contini 2009; Velicogna 2014). Hanseth and Lyytinen define information infrastructures (IIs) as a "shared, open (and unbounded), heterogeneous and evolving socio-technical system of Information Technology (IT) capabilities" (2010: 4). The components and functionalities of these infrastructures are constantly mediated and negotiated by different governance organizations in order to reach a technical, functional and institutional compatibility. In this sense, "'IIs' [information infrastructures]… evolutionary dynamics are nonlinear, path-dependent and influenced by network effects and unbounded user and designer learning" (Hanseth and Lyytinen 2010: 1). In this chapter, I resort to this definition in relation to the set-up and functioning of the Schengen Information System (SIS), by tracing its evolution from the introduction of the first-generation Schengen Information System (SIS I)

through to the implementation of the second-generation Schengen Information System (SIS II).

The aim is to attend to the core task of this research, that is to identify the *socio-political*, *legal* and *technical* conditions that allow for the data collected and stored in the SIS to become "re-usable" entries in policing activities. To illuminate each condition, I have organised this chapter in three parts. Part I evaluates the socio-political aspect in consideration of the historical and policy processes that have shaped the function and scope of the SIS. The focus of this part is very much dedicated to unearthing the EU's logic in the set-up of a hi-tech information infrastructure for security purposes. If Part I reconstructs the socio-political history of its evolution, Part II focuses on the legislative backbone of the SIS. In particular, it considers the most prominent regulations and decisions through which the EU Commission and the Council sought to expand the legal basis of the system. Part II is directed specifically at reconnecting the different moments of the system's expansion in regulation of its architecture, the type of alerts that can be inserted, the authorities that have access to the system and the related use-cases. After this initial presentation, Part II builds on the specificities of SIS II in terms of added functionalities and users. Especially, I consider the provisions that are laid down in legislative packages in relation to the concept of 'latent development', which refers to the potential to enrich technological systems with additional functionalities as soon as this becomes 'technically feasible' (Council of the European Union 2003; see also Besters and Brom 2010: 463). Part III is inherently more technical since it is dedicated to unravelling the different stages in the lifecycle of SIS data – from the decision to register an alert, through to when data are ready for search – and to showing how these technicalities matter politically.

I consider in particular three distinct stages – that is, data entry, search and processing – in order to understand how the production and circulation of data through the SIS architecture intervene in security processes and practices across the EU. The aim is to explain the functioning of SIS II by examining the technical and organisational relationship between the central database (C-SIS), the national systems (N-NIS) and the SIRENE[13]. I then present the network visualisations that I have created on the basis of the actors involved, the type of relation between them and other contextual information. The interpretation of the findings from the

[13] SIRENE stands for 'supplementary information request at the national entries.' Each country that uses SIS has set up a national SIRENE Bureau, operational 24 hours a day, 7 days a week, and responsible for exchanging information and coordinating activities connected to SIS alerts. Source: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/sirene-cooperation_en.

visual network analysis is premised by a brief discussion on the procedure that I followed to elaborate the qualitative data visually as well as on the reasons for creating a visual device in consideration of the object of this chapter – that is, the lifecycle of SIS data. Finally, I summarise the findings by considering the multiple activities of data structuring – that is, data collection, processing and analysis – through which SIS data are rendered transferable and meaningful across different security infrastructures. I then conclude this first empirical chapter by drawing the preliminary observations from the qualitative analysis and the network visualisations of SIS II.

3.1. Socio-political setup

With the introduction of the first generation Schengen Information System (SIS I), the EU Commission paved the way for developing the infrastructural basis of the EU Area of Freedom, Security and Justice (AFSJ). The establishment of SIS I and its subsequent evolution revealed that political ends were becoming increasingly dependent on technological means (Guild et al. 2009). From the outset, it appeared clear that the EU Commission conceived Information Technology (IT) and related information systems as a sheer technological concept to accomplish pre-defined political goals. In particular, SIS I was envisaged as a solution to the gradual abolition of border controls as established by the so-called "Schengen Accord". The Agreement was signed on 14 June 1985, originally by only five participating countries: the Federal Republic of Germany, France, Belgium, Luxembourg and the Netherlands. An updated version, known as the Schengen Convention (CISA) (OJEU 2000a), was signed on 19 June 1990. However, it was not until 26 March 1995 that the provisions included therein entered into force.[14] The Schengen acquis[15] was later incorporated into the EU legal framework with the Treaty of Amsterdam on 1 May 1999. Once inside the EU's legal order and institutional arrangements, SIS I shaped the infrastructural basis of the EU AFSJ.

[14] The Convention Implementing the Schengen Agreement (CISA) was signed on 19 June 1990, and it entered into force on 1 September 1993, with practical effect starting from 26 March 1995.

[15] The Schengen Agreement (CISA) and most of the rules adopted by the Schengen Executive Committee were defined as the "Schengen acquis" by OJEU (1999) Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis.

Nevertheless, at its inception, the establishment of the Schengen area was hardly concerning aspects of police and security cooperation. Largely driven by economic pressures, the initiative served the objective of promoting the free circulation of goods (Parkin 2011). As the focus of the Schengen system narrowed, from the free movement of goods to the free movement of people, its scope began to expand. The rationale underpinning Schengen cooperation is epitomised by the (in)security rhetoric according to which the lifting up of borders would constitute a security deficit (Bigo 1996). As a result, the assumption that the uncontrolled circulation of persons would produce an inevitable increase in crime began to gain traction (Faure-Atger 2008; Jeandesboz 2010; Parkin 2011). This assumption became the dominant narrative that justified the construction of a highly politicized information infrastructure at the EU level. Accordingly, the introduction of compensatory security measures – from the set-up of information systems and the digitalization of external border controls – now 'Smart Borders' (European Council 2011) – to the strengthening of police cooperation etc. – underpins this logic of (in)security (Bigo 2014).

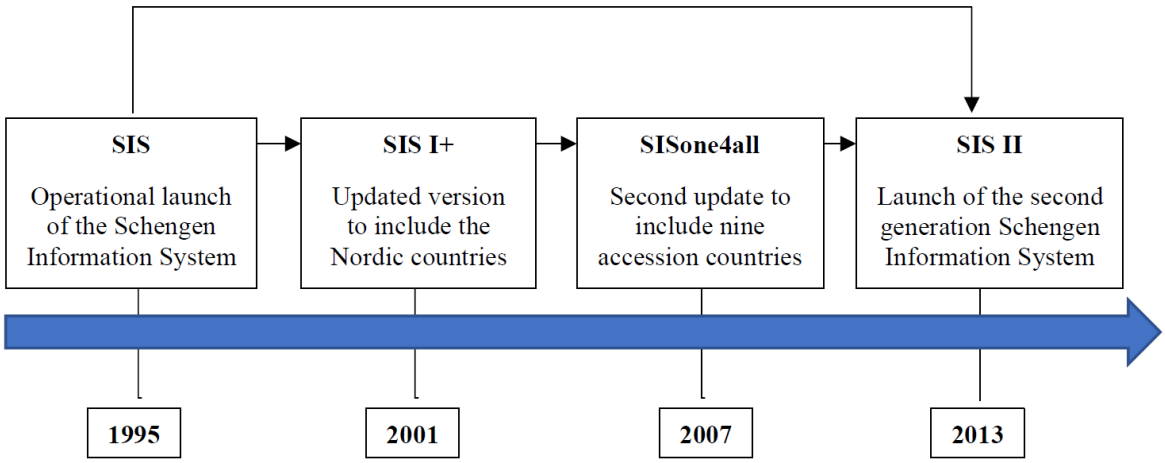

Figure 1. Chronology of the evolution of the Schengen Information System (Author's elaboration).

The first generation Schengen Information System (SIS I) is the earliest information infrastructure that has been conceived out of this rationale. How SIS I gained legitimacy is much related to the shared belief in the Schengen structures as instruments to advance the Europeanisation of internal security and law enforcement (Parkin 2011). Since it became operational in 1995, SIS I has undergone successive updates in order to accommodate the increasing use by newly acceding Member States (see Figure 1). Initially, the system was used

only by seven countries (Belgium, France, Germany, Luxembourg, Netherlands, Portugal and Spain), five of which initiated the Schengen negotiations. The first expansion into "SIS I+" occurred in 2001, in response to the inclusion of the Nordic countries (Denmark, Sweden, Finland, Norway and Iceland). In 2007 it was further expanded into "SISone4all" to manage the enlargement of the Schengen area to nine countries (Czech republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia) that acceded to the EU in 2004. The current version – known as "SIS II" – replaced SIS I with the set-up of a technically more advanced system. The second generation Schengen Information System (SIS II) became fully operational on 9 April 2013 (European Commission 2013). As we will observe later, the new architecture has been conceived not only to cope with the increase in access points and users, but also to offer additional functionalities and extended data categories.

The SIS operates in three areas of competence. First, in the area of border and migration management, it enables border guards and migration authorities to enter and consult alerts on third-country nationals for the purpose of verifying their right to enter or stay in the Schengen Area. Second, in the area of vehicle registration, it enables vehicle registration services to access alerts on stolen vehicles, number plates and vehicle registration documents, in order to check their legal status. Third, in the area of security cooperation, it supports police and judicial cooperation between Member States' authorities, by allowing them to create and consult alerts on missing persons, and on persons or objects related to criminal offences. Discussions to develop the new system (SIS II) had been underway since 2006, after the accession to the EU of nine new enlargement countries. This enlargement was seen as an opportunity to enhance the system by adding a series of up to date technical features and functionalities (Council of the European Union 2004). Compared to SIS I, SIS II provides for widened access by public authorities (e.g., Europol, Eurojust, national prosecutors, vehicle licensing authorities), the interlinking of alerts (such as an alert on a person and a vehicle), and the storage of new categories of data, including biometric data (fingerprints and photographs).

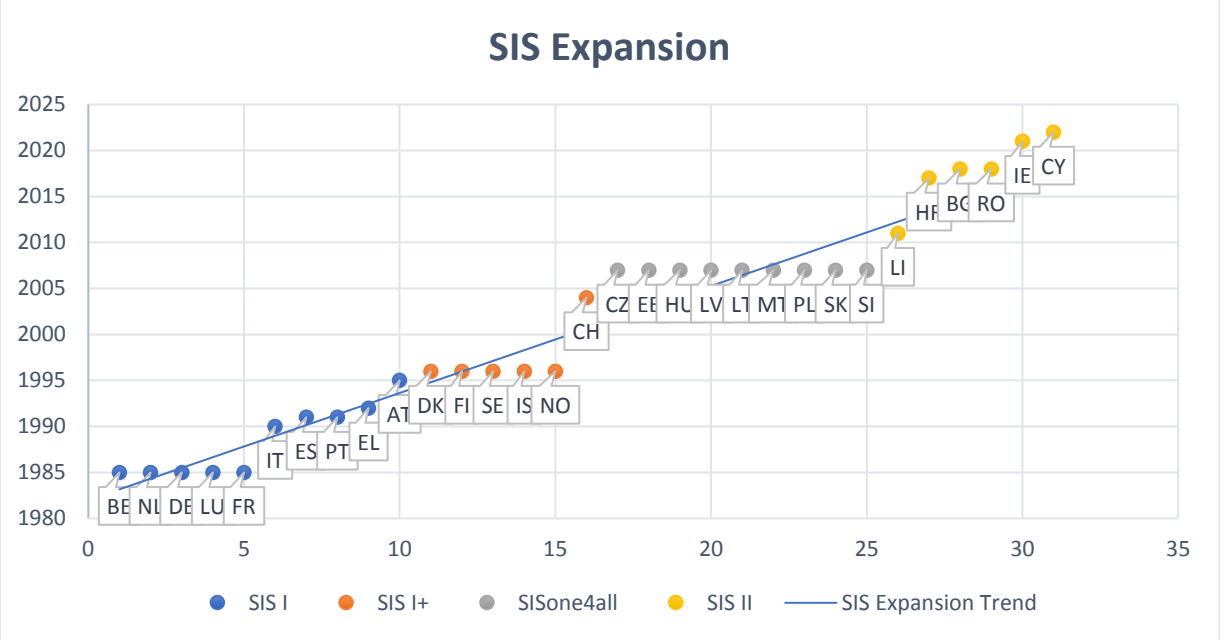

Table 1. Roadmap of SIS expansion (by country accession) (Author's elaboration).

Currently, the SIS II communication infrastructure covers 31 European countries*[16], including 26 EU Member States[17] (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus*[18], Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom*); four Schengen Associated Countries, that is European Free Trade Area (EFTA) countries (Iceland, Norway, Switzerland and Liechtenstein); and Ireland[19] (updated). For ease of reference, I have produced a roadmap that outlines the evolution of the SIS, from SIS I to SIS II (including the intermediate versions, SIS I+ and SISone4all) in relation to the different years by which new Member States joined the system (see Table 1). Its geographical coverage makes the SIS II the most widely used and largest EU large-scale IT system for security and border management in Europe. From the outset, the idea of the

[16] The microstates Monaco, San Marino and the Vatican City are de facto part of the Schengen Area, since their borders are within the Schengen States of France and Italy, and no border controls are in place.
[17] The latest addition is Cyprus. (At the moment of writing it was not yet connected to SIS II). I revised its position with the approval by the EU Parliament to grant it full access on 3 May 2022. Whereas the United Kingdom was disconnected from SIS II on 1 January 2021 and its data was consequently deleted from the central system.
[18] Source: Hazou, E. (2022) 'Cyprus Approved Access to Schengen Information on People Entering the Country', May 3, 2022 (online source). https://cyprus-mail.com/2022/05/03/cyprus-approved-access-to-schengen-information-on-people-entering-the-country/
[19] On 1 January 2021, Ireland joined the law enforcement aspect, with full access to SIS for law enforcement purposes from 15 March 2021. Source: Schengen Visa News (2021) Ireland Officially Joins the Schengen Information System – SIS II, March 16, 2021 (online source). https://www.schengenvisainfo.com/news/ireland-officially-joins-the-schengen-information-system-sis-ii/

establishment of a joint security database concerned the mere technological possibility to exchange data in a more streamlined manner. In particular, the SIS allows competent authorities in each Member State to share information on persons and objects through its communication channels. Hence, it has become an important tool in day-to-day police work and in border control procedures.

3.1.1. Deconstructing the SIS chronology

The story of the SIS is not only the story of the historical developments that have gradually led to its evolution, from SIS I to SIS II. The decisions to expand its scope were shaped by processes imbued with highly political considerations. Accordingly, instead of simply retracing the chronology of the events, in what follows, I deconstruct it briefly in order to expose the hidden assumptions and internal contradictions that have marked the origins of the system and its subsequent development into SIS II. I consider in particular the individual moments of expansion and reconnect them to specific policy processes. Negotiations on the creation of an updated version of SIS had been underway since 1996, and they continued to intensify in the following years, especially in view of the 2004 EU enlargement. While SIS I+ and SISone4all constituted only an extension of the earlier version (SIS I) to new users[20], SIS II was conceived as a brand-new system. As acknowledged in the Decision of the Executive Committee, "only SIS II will be able to meet a certain number of essential operational demands" (OJEU 2000b: 442). From the formal decision to commence development of the new system in 2001 to the adoption of the legal basis in 2006, politics and technology were going hand-in-hand in the implementation of SIS II, with little space left for democratic accountability and oversight.

In June 2002, the integration of new functional requirements, such as the addition of new categories of data and the possibility of interlinking alerts were agreed by the Ecofin Council (2002, Ibid) "with a view to ensuring greater effectiveness in combating terrorism." Nevertheless, the on-going negotiations as well as the slow technical process that characterised the development of SIS II were in sharp dissonance with the need "to act quickly" in face of contemporary threats. The temporal contrast between the two momentum – political event and implemented measure – reveals that the interest to develop a flexible EU information infrastructure, had already been in the pipeline (Bigo and Carrera 2004; Mitsilegas 2007). The politics of emergency heralded by contemporary events was primarily exploited to set up highly

[20] The original version of the SIS (SIS I) allowed for the participation of no more than 18 countries.

contested technical security measures, in first place SIS II, along with successive projects, in particular the Prüm Framework and the PNR (Parkin 2011). Thus, the question is not why political elites have expanded their powers in response to high-impact security events. But rather, how and why these features remained. Examining the introduction of datafication technologies like the SIS partly answers this question, since it exposes how the logic of emergency is now firmly embedded in administrative processes for security management that require the transfer of data to forecast and anticipate the "unknowns" (see Aradau and Blanke 2015; Aykut et al. 2019; Kaufmann et al. 2019; Lyon 2016).

3.1.2. From SIS I to SIS II

The discussions on the establishment of a brand new system gradually intensified following the acts of political violence in New York in 2001 and Madrid in 2004 (see Bigo and Carrera 2004). The politics that drove forward and shaped the implementation of SIS II was thus emergency-driven. It resulted from the necessity to build a flexible infrastructure that could respond swiftly to newly emerging transnational threats to the EU. The avenues that initially generated reciprocal opportunities for societies, such as increased interconnections through flows of finance and goods, became the ones that allowed crime to evolve into new forms and to reach cross-border. Thus, from the outset, the SIS II was designed with the built-in potential to be expanded both functionally and technically in order to benefit from the latest IT developments and to pre-empt the need for future renegotiations (Parkin 2011). The notion of an 'extendable technical infrastructure' (Commission of the European Communities 2001: 11) is nevertheless very problematic from the perspective of the transparency of the decision-making process and of democratic accountability. In the Commission of the European Communities (2003)'s view, a flexible technological architecture would enable the incorporation of new functions which, 'in the light of events such as those of 11 September, would not require too long implementation time frames in the future' (Ibid). What is technological feasible thus appeared as what is politically needed to offset security deficit in the long-run. Yet the danger is that as soon as a new functionality is added, politics is ready to accommodate it without prior discussion or supervision.

Another factor that characterised the policy process that shaped the SIS II was the presence of a multiplicity of diverse actors. These actors participated in an array of working parties since the early negotiation stages, and were responsible for the implementation of the system. Especially, a central role in the decision-making process was accorded to expert knowledge.

Expert groups emerged within the governance framework of the SIS in the form of committees, boards and task forces. They comprised technical experts, software developers, security bodies and members of the police forces, among others. Bigo refers to these transnational networks of police and security professionals as "clubs policiers" (1996: 117). Central decision-making actors, such as the European Parliament and the EDPS[21], were excluded from participating in these groups; and they were only informed of the issues concerning the advancement of the SIS II project on an informal, ad hoc basis (Parkin 2011). Therefore, knowledge and expertise "from below" were feeding into the decision-making procedures of the institutional actors (Parkin 2011: 18). This heterogenous network of expertise was "acting within highly in-transparent working structures", thus reducing sharply the possibility for democratic accountability and oversight (Parkin 2011: 2).

On the basis of this recount of the various moments that have marked the evolution of the Schengen Information System – from SIS I to SIS II – it is possible to make some preliminary observations. The first observation regards the path that was followed in the development of the SIS II architecture. This path was neither smooth, nor linear since multiple frictions emerged during the decision-making procedure. These frictions were the result of the divergent visions and the multiple interests of the actors that developed the SIS technology. The design of SIS II in particular was subject to multiple political, technical and legal re-arrangements that necessarily created delays in the system's development. The second observation concerns the consequences derived from the institutionalisation of a "flexible" infrastructure. This configuration of the SIS II is linked to the notion of "latent development" that I further elaborate in this chapter by considering the legislative base and the technical functioning of the system. In general, a system is latent when it contains the technical pre-conditions for the incorporation of new functions from the start; however these functions are not activated until the political and legal arrangements are in place (see Besters and Brom 2010: 463).

This possibility yields the potential to re-arrange the system and redefine its purpose in response to technical and political considerations with little, if none, oversight. In the case of the SIS, all the different moments of expansion that I have outlined occurred in the aftermath of external critical events. Yet, the re-arrangements of the system did not follow directly from these events, but rather they were the result of hegemonic threat-defined strategies. Accordingly, the transformation of fear into an instrument of governance allowed for the

[21] European Data Protection Supervisor.

implementation of a highly politicized infrastructure for security management. This leads to the third and final observation. The EU political decision-making on the establishment of the SIS displayed an instrumental account of technology. The purpose of the system was imbued with political considerations, while simultaneously it was advanced on the basis of the possibilities offered by information technologies. However, technologies do not come without built-in complexities. Accordingly, as political goals become increasingly dependent on technological implementation, the inherent risk is to shield their legitimacy behind a technical infrastructure like the SIS that codifies the intrinsic legal and political arrangements.

3.2. Legal setup

In the previous section I reconstructed the story of the evolution of the SIS, from SIS I to SIS II, by analysing the *politics* that drove forward its development. I did so by reconnecting the chronology of the SIS to the processes that have marked its expansion in terms of number of countries that adhered to the Schengen system of rules and procedures. Mainly informed by political considerations, these processes resulted in the establishment of a brand-new system, the so-called SIS II. This reconstruction exposed the EU Commission's 'untested belief' in security technologies as the ultimate solution for any security threat that the EU might face (Guild et al. 2009: 3; see also Besters and Brom 2010: 456). However, the roadmap of the SIS evolution by country provides only one side of the picture. The other side concerns the internal expansion of the system through legislation. The political rationale associated with emergency thinking and (in)security involved contestation, controversies, disagreements and frictions (see Côté-Boucher 2020) that led to the re-drafting of the legislation that governed the SIS. Since its operational launch in 1995, the system has indeed experienced multiple revisions in terms of scope and functionalities. In this section I retrace them by considering the legislative integrations and amendments (i.e. regulations, Council decisions, and proposals) through which the EU Commission sought to expand the purpose of the first and, subsequently, the second generation system.

3.2.1. SIS I at its infancy

Although information technology was still at its infancy in 1987, SIS I was already conceived with the purpose of registering persons and goods to be arrested and refused entry to the Schengen area (Commission of the European Communities 2001). The dynamic unleashed

suggests that information systems already held the promise of absolute control on external borders (Bigo et al. 2009). However, rather than being developed through one overarching legal document, the SIS has been developed through numerous ad-hoc amendments to the original provisions contained in the 1990 Schengen Convention. The CISA detailed the rules and procedures to be adopted by the Schengen states in order to compensate for the removal of internal border controls and to guarantee the functioning of the Schengen area (OJEU 2000a). Since its inception, the system was established as an intergovernmental initiative against the background of the CISA provisions in two areas of competence: police and judicial cooperation and external border controls. This dual purpose has later been institutionalized in the SIS II legal base through two legal instruments[22]: Regulation (EC) No 1987/2006 (OJEU 2006c) and Council Decision 2007/533/JHA (OJEU 2007b). The Regulation covers the processing of alerts on third-country nationals for the purpose of refusing their entry into or stay in the Schengen area. Whereas the Decision covers alerts on missing persons and on persons or objects related to criminal offences for the purposes of police and judicial cooperation.

Due to its dual function – as a tool for both law enforcement and immigration control – the institutional arrangements for SIS I (and later for SIS II) resulted from a fragmented approach to policy formation (Parkin 2011). In theory, a boundary between these two purposes should be maintained in order to ensure adequate legal protections with regard to data processing. In practice, this boundary has only been exercised "on paper" by obliging each Member State to declare which of its authorities has access to which set of SIS data. Despite its dual legal basis, the SIS operates as a single information system allowing the competent authorities in participating Member States to cooperate by exchanging information. It thus constitutes the essential tool for the application of the provisions of the Schengen acquis, later integrated into the framework of the European Union. As laid down in Article 1 of the SIS legal instruments, the purpose of the SIS is '(…) to ensure a high level of security within an area of freedom, security and justice of the European Union including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the (EC) Treaty (hereinafter referred to as EC Treaty) relating to the movement of persons in their territories, using information communicated via this system' (OJEU 2006c; 2007b, Ibid, Art 1).

[22] Hereinafter jointly referred to as the "SIS legal instruments".

Most of the original Schengen provisions have been replaced or built upon by EU legislation. The legal framework of the second-generation Schengen Information System constitutes one such example of body of laws that replaced the provisions of CISA Title IV, originally adopted in 2006. SIS II is governed by three legal instruments: Regulation (EC) No 1986/2006; Regulation (EC) 1987/2006; and Council Decision 2007/533/JHA (2006b; 2006c; 2007b). Together, these three Acts form the SIS II legal basis, which has undergone successive updates and integrations in order to accommodate the addition of the latest functionalities. I retrace the expansion of the SIS II legal base by considering the legislative proposals through which the EU Commission and the Council sought to implement new technical requirements in the architecture of the system. The legislative packages[23] clarify procedures, create new alert categories, extend the scope of searches of SIS data, and enlarge user access to the system. The necessity for these major updates was justified by the EU Commission and the Council by appealing to the rhetoric of "security concerns" that resulted in the first expansion of the SIS, from SIS I to SIS II.

This logic of (in)security is clearly stated in the European Council conclusions of 15 October 2015, that called for devising 'technical solutions to reinforce the control of the EU's external borders to meet both migration and security objectives, without hampering the fluidity of movement' (European Council 2015). The conclusions were in line with the strategic guidelines for Justice and Home Affairs of June 2014 that identified the need to intensify operational cooperation among Member States and to reinforce the EU's internal and external policies (European Parliamentary Research Service 2018). The proposed solutions concerned 'systematic and coordinated checks against the relevant databases based on risk assessment' […], 'while using the potential of information and communication technologies' innovations' (European Council 2015, Ibid). These declarations exemplify a 'tech-solutionist' logic (see Bigo and Carrera 2004; Martins and Jumbert 2020; Oliveira and Gabrielsen 2022; Singler 2021) according to which security is about managing the circulation, rather than blocking (irregular) flows. Many scholars working at the intersection of security and mobility (see Dijstelbloem et al. 2017; Glouftsios 2018; Scheel et al. 2019) have explored how the management of the Schengen area generated a push for the production of knowledge that

[23] Each proposal has been implemented at different stages, with a requirement for the work to be completed in 2022.

justified the extension of the collection of information to a growing number of areas of everyday life (Davidshofer et al. 2017).

3.2.2. System expansion

The first legislative package that significantly expanded the scope of SIS II both in terms of size of the database and users has been advanced by the Commission on 21 December 2016 in the form of three proposals: Proposal for a Regulation for the return of illegally staying third-country nationals; Proposal for a Regulation in the field of border checks; Proposal for a Regulation in the field of police and judicial cooperation in criminal matters (European Commission 2016b-c-d). These documents were later enforced against the background of identified gaps in the functioning of the system. Especially, an increasing number of terrorist-related cases in the EU raised concerns about the shortcomings of SIS II. Following the terrorist attacks in Paris, the Council stressed the importance of the systematic consultation of SIS II when conducting security checks on third-country nationals entering illegally the Schengen area, and when performing border checks on EU nationals (European Council 2015). The Council's response was thus once again straightforward: to every security crises, there is a technological solution (see Martins and Jumbert 2020; Oliveira and Gabrielsen 2022; Singler 2021). This view eventually resulted on 19 November 2018 in the adoption of the new set of regulations that sought to render the system more resilient in face of the identified security gaps. These rules gradually replaced the original ones established with the original package of legal instruments (OJEU 2006b; 2006c; 2007b).

The first Regulation (EU) 2018/1860 is directed at strengthening the enforcement of the EU's return policy by reducing the incentives for illegal immigration (OJEU 2018c). In particular, competent authorities are required to enter alerts in the SIS as soon as a return decision is taken in order to ensure that there is no delay between the departure of a non-EU national and the activation of an entry ban. The second Regulation (EU) 2018/1861 establishes harmonised procedures for the entry and processing of alerts on non-EU nationals that have been refused entry into or the right to stay on the territory of the Member States (OJEU 2018d). In particular, it obliges Member States to enter alerts in the SIS as regards entry bans for third-country nationals. The prime reason for refusal is because a third-country national poses a threat to the EU or is subject to a restrictive order. The third Regulation (EU) 2018/1862 provides for the extended use of SIS II by establishing the conditions and procedures for the entry and processing of alerts on persons and objects and for the exchange of supplementary information

and additional data for the purpose of police and judicial cooperation in criminal matters (OJEU 2018e). The implementation of these new regulations was set to be put into effect gradually until December 2021.

Another legislative package and, perhaps, the most prominent expansion, and the clearest manifestation of the concept of latent development, concerns the introduction of a biometric matching capability as mandated by the entry into operation of the new SIS legal basis (also referred to as "SIS recast"[24]). This new requirement enforces on all Member States an obligation to implement the Automated Fingerprint Identification System (AFIS) that permits the identification of persons on the basis of fingerprint data and facial images (OJEU 2016e). The AFIS functionality was already "latent" in the legal framework of the first generation Schengen system. According to Article 22(c), it was foreseen that SIS II may also be used to identify a person on the basis of his/her fingerprints "as soon as this becomes technically possible" (OJEU 2007b: 73). This statement clearly embodies the rationale behind the concept of latent technology: whenever the introduction of a new function was agreed on and the legal framework was arranged accordingly, the function could be updated immediately (see Besters and Brom 2010). The condition for a biometric search to become "technically possible" and thus be activated, concerns the presentation of a report (drafted by eu-LISA) on the availability and readiness of the required technology (AFIS), on which the European Parliament shall then be consulted (Beslay and Galbally Herrero 2015).

In the original version of the SIS, the storage of fingerprints and facial images of persons was allowed, however, these could not be used to search the database in order to identify a person. Only alphanumeric data were used to perform searches. In case of a positive "hit", fingerprints and facial images could then be used to verify the identity of the person (one-to-one search) who had initially been identified on the basis of alphanumeric data (e.g. name and date of birth). With the introduction of the AFIS functionality in March 2018, this situation has changed. The new regulation allows for the identification of persons also on the basis of his/her biometric identifiers (one-to-many search). These concern for example, facial images, fingerprints, palm prints, and DNA profiles. The use of DNA profiles is allowed specifically for the purpose of searching for missing persons who need to be placed under protection, and in cases where fingerprint data, photographs or facial images are not available or not suitable for identification

[24] I employ the term "SIS recast" in reference to the three Regulations mentioned above: Regulation (EU) 2018/1860; Regulation (EU) 2018/1861; Regulation (EU) 2018/1862.

(OJEU 2016e). Beyond the implementation of new functionalities, the "SIS recast" prescribes, inter alia, new categories of data, and extended access to new users such as Frontex and access for Europol and Eurojust to all categories of data in the system.

Hence, the new legislative package has provided for a number of integrations that resulted in the expansion of SIS II both in terms of size of the database and users. In terms of size, they have enriched the data it contained by introducing new alert categories, such as: alerts issued for the purpose of 'inquiry checks' that allow law enforcement authorities to question a person in order to obtain more detailed information; alerts on 'unknown suspects or wanted persons' connected to a serious crime or terrorism (e.g., persons whose fingerprints are found on a weapon used in a crime); new alerts for the purpose of return, to help enforce decisions by a member state on returning an illegally-staying non-EU national to his/her country of origin (OJEU 2008d). In addition, they have extended the scope of the existing alert category of 'missing persons' to 'vulnerable persons who need to be prevented from travelling' (e.g., children at high risk of parental abduction, children at risk of becoming victims of trafficking in human beings, and children at risk of being recruited as foreign terrorist fighters) (Council of the European Union 2018a); and finally, the list of 'objects of high value' for which alerts can be issued (e.g., false documents and high-value identifiable objects, as well as IT equipment), which can be identified and searched with a unique identification number.

In terms of users, they have enlarged the legal base to include the possibility for Europol to issue alerts in the system. This has been done by proposing a further amendment to Regulation (EU) 2018/1862. The amendment was intended to enable Europol to issue 'information alerts' on suspects and criminals, in order to provide information directly and in real-time to front-line officers (European Commission 2020g). Under the previous Regulation (EU) 2018/1862, Europol had a "read-only" access to the alert categories in SIS II. But as set out in the explanatory memorandum to the new proposal, for the EU Commission this constituted a "security gap" to be addressed through the establishment of a new alert category specifically for Europol. SIS recast has also widened access to law enforcement authorities, by granting the possibility to immigration authorities to consult the SIS in relation to irregular migrants who were not checked at a regular border control (European Commission 2020g). It has also granted full access rights to boat and aircraft registration authorities; to services responsible for registering firearms in order to allow them to verify whether the firearm is being sought for seizure in Member States or whether there is an alert on the person requesting the registration;

and finally, to the European Borders and Coast Guard Agency when conducting operations in support of Member States (OJEU 2016f).

The major consequence of these technical and operational adjustments is that more and more data are being sought after and exchanged through the SIS information infrastructure. Nevertheless, the implementation of the new functionalities and requirements is not as straightforward as it appears. In general, EU regulations set deadlines that all Member States must be able to meet in order to operate the system on the basis of the newly added functions. For example, with regard to the introduction of the AFIS functionality, Member States have been required to carry out searches by using fingerprints since 28 December 2020. But before being able to do so, they had to roll out the fingerprint search functionality to their national police officers and border guards. This transition not only requires human and technical capital, but also the time to instruct and train them to operate with the new functionalities in the SIS II. Accordingly, although the concept of latent technology is suggestive of an immediate change, the foreseen integrations are subject to the development of the required technology, which is generally slow, since it depends upon the budgetary resources of each Member State, as well as the availability of workforce (i.e. software developers and IT engineers) and of the technical equipment.

3.3. Technical setup

Personal data travel through the SIS network on the basis of technical and organisational arrangements. The SIS legal instruments not only establish rules and procedures to be followed when operating the system, but they also set out its architecture and regulate its functioning. These decisions are laid down in the SIS legal basis, and concern who can access the system; for which purposes; what type of alerts can be entered; and what type of data can be consulted. Access to the system may occur for consultation purposes only, to perform a search, to verify an identity, or to enter alerts. However, the main purpose for consulting SIS is to detecting wanted persons and stolen objects in order to allow competent security authorities to take the necessary measures. In relation to this purpose, the SIS databases (central and national) contain the so-called ‘alert data,’ that is, information that is indispensable for the identification of a person or an object as well as the necessary action to be taken. Therefore, the communication infrastructure of the SIS has been set up to enable the sharing of information about persons and

objects among competent authorities (i.e. national border control and customs and police authorities responsible for checks at the external Schengen border as well as within the Schengen Area) (OJEU 2010a).

3.3.1. System components

In order to avoid that criminals escape through the gaps of the existing law enforcement arrangements, it was clear that traditional bilateral agreements and mutual legal assistance requests could no longer support information sharing. As a result, the SIS has been implemented with the purpose of simplifying the exchange of information among Member States, and it has paved the way for the development of an EU information infrastructure highly reliant on technology. The SIS II physical architecture consist of three main components: a central system (Central SIS II) which in turn is composed of a technical support function ('CS-SIS') containing the central database (the 'SIS II database'); a uniform national interface ('NI-SIS') in each Member State, used to directly enter, update, delete and search SIS data by members; and finally, a communication infrastructure between CS-SIS and NI-SIS (the so-called 'Communication Infrastructure') that provides an encrypted virtual network[25] dedicated to SIS II data and the exchange of data between SIRENE Bureaux (Council of the European Union 2001; OJEU 2007a). The C-SIS, NI-SIS and SIRENE are all different technical and organisational units. The personnel that work with these systems are located in different buildings across national territories.

The CS-SIS is located in Strasbourg (France) where administration functions and technical supervision are performed; whereas a backup of CS-SIS is located in Salzburg (Austria) and ensures all the functionalities of the principal CS-SIS in the event of failure of the system. The NI-SIS is located within the territories of each of the Schengen Contracting Parties and it communicates directly with the C-SIS. The main function of the C-SIS is to guarantee the integrity of the data and to ensure that all the national copies in the NI-SIS are kept identical and synchronised at all times with the data file stored centrally. In particular, the NI-SIS consists of a Local National Interface (LNI) in each Member State, which physically connects the Member State to the secure communication network and contain the encryption devices dedicated to SIS II and SIRENE traffic. The NI-SIS also contains an optional Backup Local

[25] The network for Secure Trans-European Services for Telematics between Administrations (referred to as 's-TESTA') provides an encrypted, virtual, private network dedicated to SIS II data and SIRENE traffic. Pursuant to Article 4(1)(c) of the SIS II legal instruments.

National Interface (BLNI) which has the exact same content and function of the LNI. To ensure secure access to the CS-SIS, each Member State has a Central National Interface (CNI) that functions as a separate access point enabling designated national authorities to conduct searches in the system. The unique channel for the exchange of police data between participating countries is the SIRENE (OJEU 2008a). The Communication Infrastructure between the CS-SIS and the NI-SIS is part of a broader framework of police information exchange and therefore it must be able to be extended to any other country or entity acceding to C-SIS (e.g., Europol, Eurojust).

Operationally, the SIRENE forms an integral part of SIS II and it is present in every Schengen country in the form of a permanent office, the so-called "SIRENE Bureau". The SIRENE Bureau work in accordance with the provisions contained in the SIRENE Manual (OJEU 2008a and 2013)[26]. Their task consists in managing all background information on a SIS II alert which is indispensable for the officers on the ground to confirm hits and carry out the required action. In accordance with Article 7(2) of the SIS II legal instruments, each Member State is responsible for designating the authority which hosts the SIRENE single point of contact in their country. The establishment of the SIRENE Bureau was thus intended to give SIS a human interface. The SIRENE usually comes into the picture when supplementary information regarding a positive "hit" in SIS is required. The exchange of supplementary information is the principal means of ensuring that 'hits' become successful outcomes, resulting, for example, in the extradition of a wanted person or the correct seizure of stolen property. In such circumstances, the request is sent directly to the SIRENE office and not to a particular person. The contact with the SIRENE Bureaux takes place principally via a dedicated, structured hit-reporting form that contains electronic files on all relevant case information, including fingerprints and photographs if needed for identification purposes.

Although it functions as a separate communication network, the operation of SIS II is inseparable from the SIRENE Bureau, as they are at the very heart of SIS II information exchange. Both the C-SIS II and the SIRENE communication infrastructure are managed by the EU agency eu-LISA (OJEU 2011). According to Regulation (EU) 2018/1726 the Agency is responsible for the development and operational management of all large-scale IT systems in the EU AFSJ (OJEU 2018a). At the development level, eu-LISA is mandated by the

[26] The SIRENE Manual is a set of instructions, which describes in detail the rules and procedures governing the bilateral or multilateral exchange of supplementary information.

Commission for the design and implementation of new functionalities. In this regard, following the Communication from the European Commission (2016a), the Agency launched phase 1 of the AFIS project in June 2016 that consisted in developing and equipping SIS II with biometric matching capabilities. At the operational level, the tasks of the SIRENE consist of conducting quality checks on the data stored centrally and ensuring that the central system functions 24/7 every day of the year. Additionally, it is responsible for the supervision and security of the SIRENE communication infrastructure as well as for the coordination between member countries and providers, and budgetary and contractual issues. Whereas the setting up, operation and maintenance of the NI-SIS are left to individual Member States.

The full list of alert categories is articulated in the form of binding Articles which detail the subject of the alert (i.e. person or object) and the purpose for which it can be issued. With regard to alerts on persons, Council Decision 2007/533/JHA foresees four categories of individuals as object of an alert in SIS II: persons subject to arrest for surrender or extradition purposes (Article 26); missing persons (adults and minors who have disappeared or who need to be placed in a place of safety for a time) (Article 32); persons sought to assist with a judicial procedure (e.g., witnesses) (Article 34); and persons for discreet (i.e. covert surveillance) or specific checks (Article 36). Directive (EU) 2016/681 has expanded this list to include a fifth category, namely, third-country nationals to be refused entry into or stay within the Schengen Area (Article 24) (OJEU 2016c). A report relating to a person may contain no more than 10 different data items (not all of them may be necessary or available).[27] With regard to alerts on objects, Article 38 covers the following categories: issued identity papers such as passports, identity cards, etc., which have been lost, misappropriated or invalidated; vehicles such as boats, aircrafts, caravans etc.; vehicle number plates, banknotes, securities and means of payment, weapons, outboard engines, industrial equipment, containers etc. (OJEU 2007b). These objects can be entered into SIS II as they are sought for the purposes of seizure or use as evidence in criminal proceedings.

3.3.2. Performing a "search" in SIS II

With the introduction of "SIS recast" the list of persons and objects has been expanded to include alerts on non-EU nationals subject to a return decision; unknown wanted persons to identify suspects of serious crimes and terrorism; preventive alerts on children and vulnerable

[27] See OJEU (2016c) Directive (EU) 2016/681, Article 94(3) for the full list of data items admitted.

adults at risk of abduction; and people and objects for inquiry checks. The data entered into the system concern information necessary for identifying the person or object that is the subject of the alert and clear instructions on what to do when the person or object has been found. Therefore an alert in SIS II always consists of three parts: (1) a set of data for identifying the person or object in the alert; (2) a statement declaring why the person or object is sought; (3) an instruction on the action to be taken when the person or object has been found. For the operational success of SIS, the data elements enabling identification must be accurate, complete and of high quality. For alerts on persons the minimum data set is name, year of birth, a reference to the decision giving rise to the alert and the action to be taken. With the integration of the AFIS functionality, photographs and fingerprints must be added in order to facilitate identification and to avoid misidentification.

The right to search data is reserved exclusively to the competent authorities as defined in Section 4.1 of the SIS II legal instruments. These include law enforcement authorities, national border control authorities, customs authorities, judicial authorities, visa and immigration authorities, vehicle, boat and aircraft registration authorities. With the introduction of Regulation (EU) 2018/1862, also Europol and Eurojust have obtained full access to the system and are now able to issue alerts (related to their mandate) (OJEU 2018e). The updated legislative framework has granted access also to the teams involved in return-related tasks and migration management support with the European Border and Coast Guard (OJEU 2016f). Pursuant to Article 31(8) and 46(8) of the SIS legal instruments[28], each Member State is required to indicate the list of authorities in their territory that are authorised to search directly the data contained in SIS II. This list[29] is published annually in the Official Journal of the European Union and specify the legal status of each authority; which data it has access to; and for what purposes. Initially, consultation of the SIS II database was carried out by using only alphanumeric data. However, this situation has changed with the implementation of the Automatic Fingerprint Identification System (AFIS) functionality.

Today consultations are carried out by using either alphanumeric or biometric data (e.g., fingerprints, palm prints and facial images) in the verification of a person's identity. All the

[28] Article 31(8) of Regulation (EC) No 1987/2006 and Article 46(8) of Council Decision 2007/533/JHA.
[29] To consult the updated list, see: OJEU (2021) List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31(8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System, 16 July 2021, C 287, pp. 1-181.

technical cases related to its possible consultations take place in activities such as investigation and prosecution, border checks and asylum processing operations. It is the responsibility of the reporting country to determine whether the case is adequate, relevant and important enough to be entered in SIS II. However, as noted in the report by the Joint Supervisory Authority (JSA), countries have produced different interpretations of what constitutes a risk to security and public policy (Statewatch 2007). Similar discrepancies were found regarding alerts entered for persons targeted for 'discreet surveillance' (Monroy 2018). These differences result from the lack of a uniform definition in the SIS II legal basis of what constitutes a "serious crime". In general, the prerequisite for using an Article 36 alert is the "prosecution of criminal offences and the prevention of threats to public security" (Ibid). However, the lack of indications on how this prerequisite is applied in practice has led states to select arbitrarily the criminal offences leading to Article 36 (Monroy 2018).

The danger is that the wide variation in practices between national authorities may lead to many cases of inaccurate, unlawful data entered when reporting individuals in the system. This lack of harmonisation is due to a series of loopholes in the legislation. Below I expose those gaps in relation to matter of privacy and data protection. One loophole concerns the data that can be entered under Article 36 on "discreet checks". This Article permits investigations on the grounds that an "overall evaluation of the person concerned" would suggest that serious criminal offences could be committed. Under such definition, the person concerned is neither arrested nor searched, but is subject to surveillance measures. In this case there are no real indications or concrete evidence of an actual threat that would justify the entry of an alert into SIS II. What constitutes a "serious crime" is based on the assessment of a *potential* intention to commit a crime. The JSA suggests that the broad scope for entering alerts on 'discreet checks' may have contributed to past discrepancies in the use of Article 36 (Hayes 2008). In 2012, France, Italy and Spain were responsible for the vast majority of entries; while other states, such as Greece and Ireland, entered very few alerts, or none (Statewatch 2012). According to the latest statistics published annually by eu-LISA, these figures remained very similar throughout the years (eu-LISA 2019; 2020; 2022a).

The persistence of these discrepancies created another loophole, concerning specifically access rights. In general, the guiding principle should be "necessity", that is, who access the data in the system must have a legitimate reason. In general, the performance of a "search" is the most usual form of access given that the objective of SIS is to offer online searchable facilities for

both criminal and immigration authorities. Competent authorities may also enter the system for updating, correcting or deleting the reported data. These rules on access (i.e. list of authorities, purpose limitation etc.) are laid down by the SIS legal instruments, yet they do not set limits to the number of persons with access authorization. Instead the regulation of this aspect is left to the national laws of Member States. Consequently, there are considerable differences in the list of authorized persons among the participating countries. As highlighted in the latest Technical Report (eu-LISA 2022b) and in the annual Statistics (eu-LISA 2019; 2020; 2022a), this has resulted in great variance in the number of reports entered. For example, in 2021 there were around 7 billion accesses in total to SIS II by Member States. This represented an increase of 88% compared to 2020 (highly impacted by the Covid-19 restrictions, especially on border crossings). At the end of December 2021, there were 89.99 million alerts stored in SIS II. The majority of alerts, and thus of entries, came from Italy (with over 24% of the total), followed by France (19%), Germany (13%) and Spain (9%) (see eu-LISA 2022a).

These huge differences indicate that SIS II is used differently by the national authorities in each participating country. Some states may be issuing alerts on persons who are merely suspected of association with criminals, thus increasing exponentially the possibility to detect innocent people. Other states may have a narrower understanding of what constitutes a "serious criminal offence" and thus may enter alerts only under stricter circumstances. The lack of clear guidelines on how to evaluate a "serious offence" has inevitably created ambiguity, that can be promptly exploited by security agencies in order to advance intrusive practices. Another major loophole concerns the lack of clarification on the meaning of "deletion" of an alert. In principle, alerts on people and objects should be kept only for the time required to achieve the purpose for which they were entered, after which they should be deleted. For alerts on people the retention period is limited to one year, in the case of discreet or specific checks; and to three years in all other cases (Article 44) (OJEU 2007b). Whereas for alerts on objects the retention period is limited to five years, in the case of discreet or specific checks; and ten years for objects entered for seizure or evidence in criminal proceedings (Article 45) (OJEU 2007b). After these deadlines, the need for retention must be reviewed by the issuing country, and unless prolonged, the alert should be automatically deleted from the C-SIS.[30] Different interpretations for when the purpose of an alert is fulfilled may yet cause disagreement on the retention period

[30] The deletion occurs regardless of whether the purpose of the report in SIS has been fulfilled or not.

between the issuing and the receiving country; in turn, if agreement is not reached, the alert is not deleted, with clear impact on the rights of individuals.

As a result of the ambiguity and the loopholes in the legislation, the scope of SIS II could potentially be expanded to include any other type of offence or activity deemed suspicious. The alert categories would in turn be extended as well as the retention period and the purpose for sharing information with the aim of preventing "serious threats" to the EU. Consequently, there is an emerging picture across the EU that any type of offence could be among the next to be targeted to enforce internal and external security. This in turn may result in increased breaches of the rights of individuals since data protection authorities will not be able to conduct any "ex ante" checks on specific records entered at the national level. The danger is that these potential expansions along with the possibility to review the need for retaining alerts pave the way to indiscriminate data processing practices, as they open up more and more data for re-use. This prospect is promoted also by the possibility of interlinking alerts (e.g., between an alert on a person and a vehicle) (Article 52) (OJEU 2007b). Introducing linkages may be a logical tool since SIS II offers the possibility to store data on both persons and objects. However, it poses serious questions regarding the impact on individuals, especially in terms of data protection. By allowing associations to be made between individuals and/or objects stored for different purposes, such as between criminals or immigrants and children at risk of abduction, this function increases the risk of violation of the principle of 'purpose limitation' (European Commission 2010).

According to Directive (EU) 2016/680, data may be processed for a purpose other than that for which it was entered only in three cases: the prevention of a serious and imminent threat to public order and safety; serious reasons of national security; and the prevention of a serious criminal offence (OJEU 2016b). Nevertheless, the dual function of the SIS inherently contravenes this principle, as the SIS database provides for the storage of both law enforcement information (e.g., persons wanted for arrest) and border control and immigration information (e.g., banned third-country nationals). The fluidity added by the possibility of interlinking alerts means that individuals registered for immigration reasons are at greater risk of becoming targets of criminal law enforcement measures or secret surveillance. Interlinking is thus a clear manifestation of the "function creep" (see Besters and Brom 2010) built in the use of the system, whereby information that has been collected for one limited purpose, is gradually used for other purposes. This function creep further deepens associations between crime and

migration and in turn increases the chances of negatively impacting on innocent persons. The possibility to incur in a function creep in the SIS database are higher, given that it is used for both immigration and criminal law purposes. While the system is unique, it has to deal with the reality of these two contexts that yet present different challenges and constraints.

3.4. Visualising the SIS II network

The above analysis has sought to unravel the *socio-political*, *legal* and *technical* conditions that allow for the sharing of information through the SIS II. In this section, I present the results derived from the visual elaboration of these three aspects, on the basis of visual network analysis. Methodologically, the integration of this approach to the study of SIS II has been essential to come to a deeper understanding of the interconnections that make up the SIS II infrastructure. In particular, by reproducing visually the technical and organisational aspects of the system, I have been able to observe the way in which its constituent parts are interrelated and arranged. Before turning to the results, I briefly recall the method that I have used to create the data visualisations, that is, visual network analysis (VNA). In Chapter 2, I presented VNA as a qualitative approach to the study of "networks". The notion of "networks" has been adopted within a variety of currents, such as STS, A-NT and assemblage studies as a means to trace the complex entanglements that constitute specific practices (see Attride-Stirling 2001; Knox et al. 2006). In line with this approach, I have applied the notion of "network" to reproduce visually the lifecycle of the SIS II.

Below I provide additional guidelines regarding the design choices that I have made, especially in relation to the software used, the data entered and the steps taken. In terms of software, I relied on Gephi (see Chapter 2). Yet rather than inserting the data directly into the software, I created tables in Excel, detailing the actors involved, the name of databases used, the type of relations between them, and other contextual information. The software allowed me to extract the data from the tables and then spatialize them in the form of the resulting network. In order to visualise the network topology, Gephi offers multiple algorithms. The visualisations reported below spatialize the SIS II network in the form of a force-directed layout. To create the first visualisation (Figure 2) I used an algorithm called "ForceAtlas2", whose core feature is to shape networks on the basis of the relations between indexed nodes (Jacomy et al. 2014). For the second (Figure 3) I ran "Fruchterman Reingold" (Fruchterman and Reingold 1991) that models the graph drawing problem by a system of springs between neighbouring vertices.

Finally, for the third (Figure 4) I relied on "Yifan Hu" (Hu 2005), a multilevel algorithm that reduces network complexity.

Before running the algorithms in Gephi, I proceeded to label each node in the Excel tables. Rather than making a deliberate choice, I used the terms reported in the legislative and technical documents detailing the functioning of the system. In particular, I labelled the central system as 'C-SIS,' the national data systems as 'N-SIS' (i.e. National Schengen database), the SIRENE Bureau, simply as 'SIRENE and the terminals used to enter a report as 'Police Station.' The labels of the N-SIS, SIRENE and Police Stations are followed by the ISO country code to which they belong (e.g., NI-SIS CH – for Switzerland; SIRENE NO – for Norway etc.). When conducting VNA, there were 30 Member States enjoying full access rights to SIS II. The situation has changed following the disconnection of the United Kingdom on 1 January 2021 and the later addition of Cyprus and Ireland in 2021, which gained full access. To account for these changes, I updated the visualisations in a second time. The ones presented below index 31 European countries that (as of 2022) have full access to SIS II. After labelling them, I assigned a colour to each node (arbitrarily) in order to distinguish between the different parts that participate in the exchange of data: red for the C-SIS, blue for N-SISs, orange for the SIRENE and green for national police stations. The size of each node is determined by the number of connections that cross it. The more the connections, the bigger the node. For example, in the case of C-SIS, the node is bigger since it is crossed multiple times, by data incoming from the information systems to which it is connected.

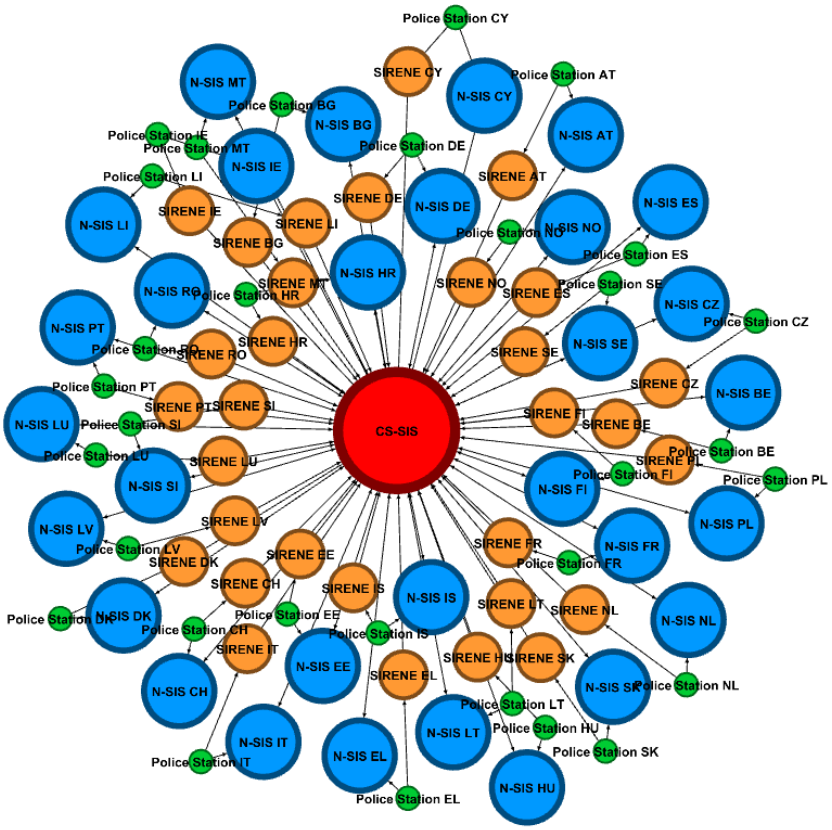

Figure 2. Force-directed layout of the SIS II network (ForceAtlas2).

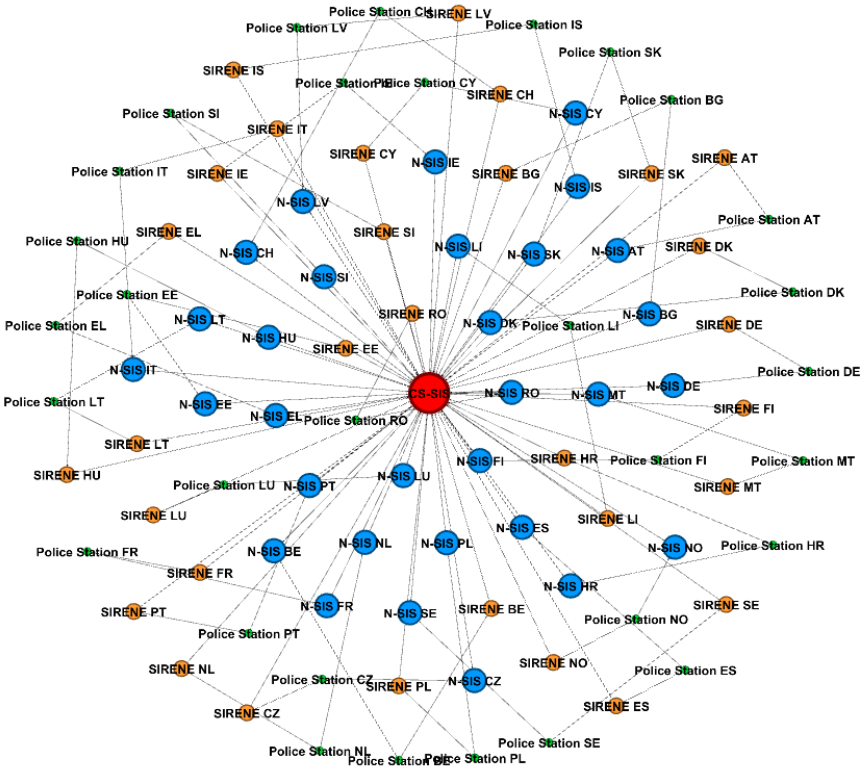

Figure 3. Force-directed layout of the SIS II network (Fruchterman Reingold).

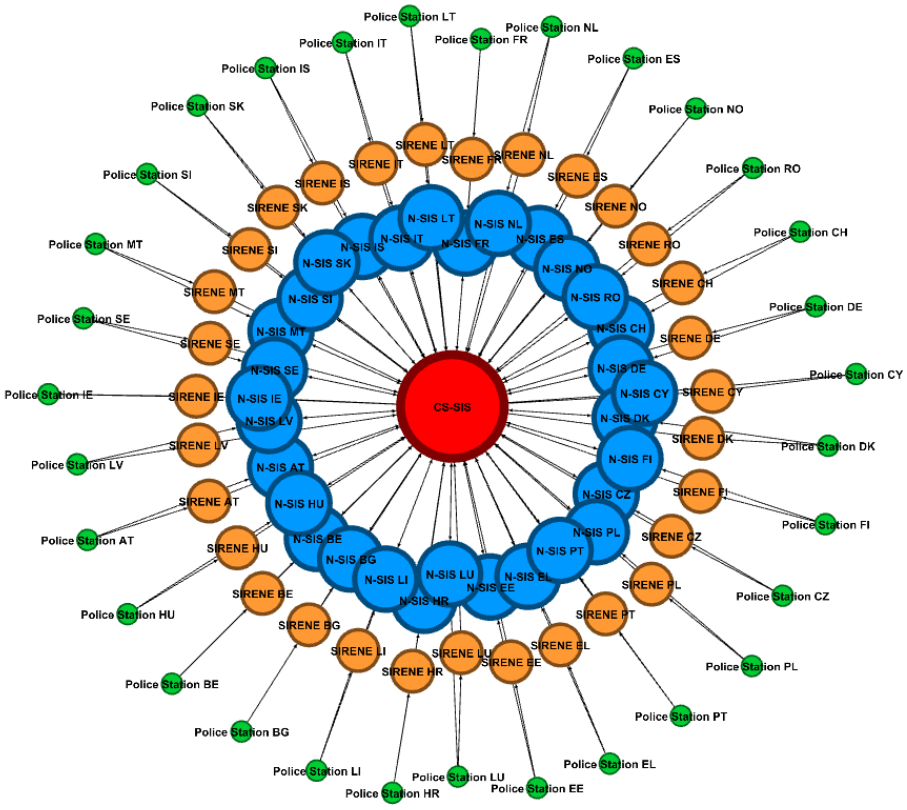

Figure 4. Force-directed layout of the SIS II network (Yifan Hu).

In order to generate the above graphs, I started tracing the flow of SIS II data from the moment when a report about a sought-after person or object is made by a Member State. "Following the data" on the basis of the legislation was essential to determine which actors (i.e. databases and authorities) are "crossed" by SIS II data exchanges. The process of entering data into SIS starts at police stations.[31] Here the competent national authorities that are allowed to enter data in SIS II, such as police officers, immigration authorities, customs services etc., create a report in the system via their terminal (step 1). The report is then transferred in real time to the central system (C-SIS) (step 2) that, after indexing the data, directs them to all the other national systems (step 3) to ensure that they are synchronised and up to date at all times. This procedure enables the competent authorities in each Schengen country to know the situation that the reporting State is facing (e.g., the sought after person is dangerous or a missing person has been located) and the action to be taken (e.g., arrest, protect or apply specific checks on the person). Visually, I reproduced these steps by adding an "edge", that is a connection, between the related parts. The first edge connects the 'Police Station' of each MS to the corresponding 'N-SIS'

[31] Obviously there are multiple terminals in each Member State, however, for ease of reference, I grouped them all together under the label 'Police Station', followed by the country code.

(step 1); the second edge connects the 'N-SISs' to the 'C-SIS'; the third edge connects the 'C-SIS' to the 'N-SIS' (step 3).[32]

Once distributed to all the N-SIS[33], the data are "searchable." By performing a "search," the examining officer can query the database to check whether it contains an alert in relation to the person or object sought. If the system produces a positive 'hit' (i.e. a positive response to the query indicating that an alert matches the details entered), the alert will automatically indicate to the officer the action to undertake in relation to the purpose of the alert (e.g., arrest or extradition). As a consequence, there is a strong link between a "search," a "match," and "action" on the ground. SIS II is in fact 100% operational since it does not only provide for the performance of a "search", but it also directs action on the ground. This procedure plugs into the picture another actor: the SIRENE. The SIRENE comes in when supplementary information regarding a positive "hit" is required. In such circumstances, a request for information by the examining officer is made to the corresponding SIRENE Bureau. The transfer of data between the national police stations and SIRENE is represented visually through another edge. Additionally, the SIRENE is responsible for checking all new reports of the national police authorities and transfer them to the C-SIS. This establishes a further edge, between the SIRENE and the C-SIS.

The central system only has a copy of the Schengen data. Hence, each national examining officer, for instance at the airport, directs the consultation to his own national N-SIS. If the data reported requires a modification, the updating of data passes through the central system. However only the owner of the information, that is, the authority who has entered the report in the system, is able to change these data. This is the so-called "ownership principle"[34] of the Schengen Information System. A modification is entered into the N-SIS through one of the terminal of the national police information system and it is then passed on to the national SIRENE that, after checking that the report is relevant to SIS II, transfer them to the C-SIS. Visually, this creates an edge between the national 'Police Station' and the corresponding 'N-SIS' as well as between the 'N-SIS' and the national 'SIRENE'. One peculiarity of SIS II is that it operates on the principle that the national systems cannot exchange computerised data

[32] Note that some edges overlap with each other, for example between the C-SIS and the N-SISs and the N-SISs and the C-SIS. Accordingly, although they represent two different moments by which data are exchanged, they are visualised as one.
[33] Including the N-SIS in the reporting country.
[34] Each State remains the owner of its own data within the SIS. Any variation is only possible with the prior consent of the reporting State.

directly between themselves, but instead only via the central system (CS-SIS). This condition substantially simplify the relations between the constituent parts of the SIS II network, as further substantiated by the more or less proportional number of nodes and edges in the graphs (91 inputted nodes, 150 edges).[35]

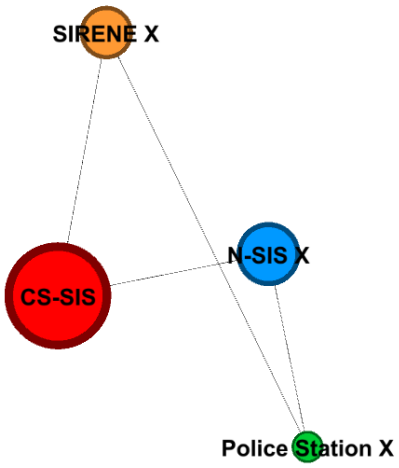

Figure 5. Sample representation of the SIS II network (for country "X").

To better exemplify this proportionality, Figure 5 represents a simplification of the SIS II network, with the only presence of the central SIS database (CS-SIS) and the SIS system components for country "X". What emerges is that each inputted node is backed by the same number of edges. Although the graph constitutes a simplified version, it can be derived that each actor gains power by means of being in a relational disposition to the exchange of data. While the C-SIS, N-SISs, SIRENE and Police Stations are all different technical and organisational units, it is the data that inevitably interrelate them by travelling from one unit to the other, thus producing a bundle of contingent practices – that is, "the SIS II network". It is important to underline that the resulting network can effectively be considered as an heterogenous 'assemblage' – 'composed of people, beings and objects' – that works as a single entity and gives performance to the circulation of data (Jeandesboz 2016: 295). What is central to its constitution and functioning is not the institutional arrangement of each individual unit,

[35] Conversely, the network of a decentralised architecture would necessarily result as more intricate, given the multiple connections that need to be established among its parts. This, in turn, would result in a higher number of edges vis-à-vis number of nodes in the graph. As I will show in Chapter 4 and 5, this is the case of both the Prüm framework, and the API and PNR systems.

but the relations, that is, the edges between them. As Crossley posits, "individuals are shaped by, and become social actors within, interaction" (2015: 66).

These observations foreground the value of applying visual network analysis to the study of networks in general, and digitally-mediated security in particular. Indeed, through the graphs it is possible to grasp how not only humans, 'but also things co-organize and co-produce the complex assemblages' […] of data practices (Glouftsios 2018: 189). In the resulting distribution, relations and agency as well as humans and non-humans are placed in the same flat, relational field (Payne 2017). This is better represented by Figures 6, 7 and 8 below. Although these figures present some differences with regard to the disposition of nodes, this is largely dependent on the inner workings and characteristics of the algorithms employed, that make sense of and highlight different qualities of the spatialized network. In Figure 6 and 7, for instance, the spatial disposition appears as random. Whereas in Figure 8, the forces of repulsion and attraction between nodes are stable, and thus create a more ordered data map. Yet hierarchy is absent from all the graphs, not much because it cannot be rendered visually, but because no one actor has power as a result of its status or positions. Rather, each actor gains power by means of being in a relational disposition to the exchange of data.

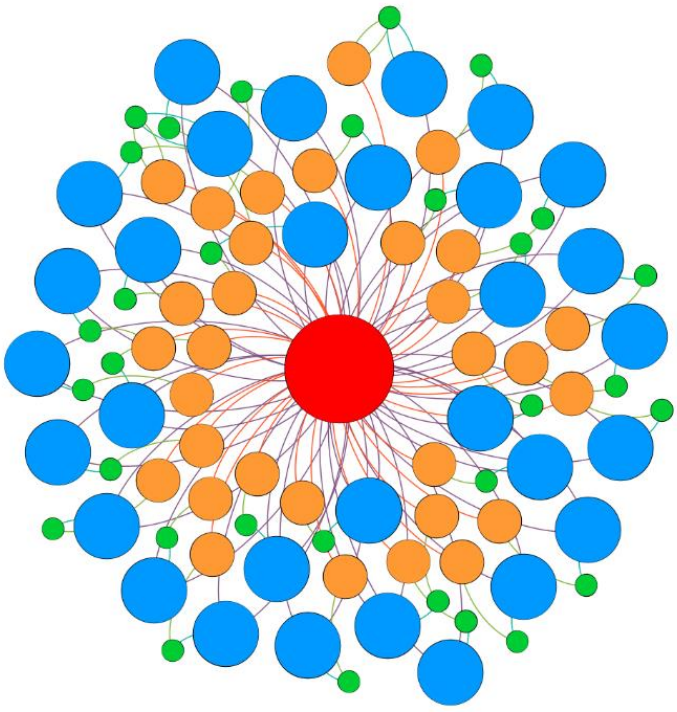

Figure 6. Graphical topology of the SIS II network (Force Atlas 2).

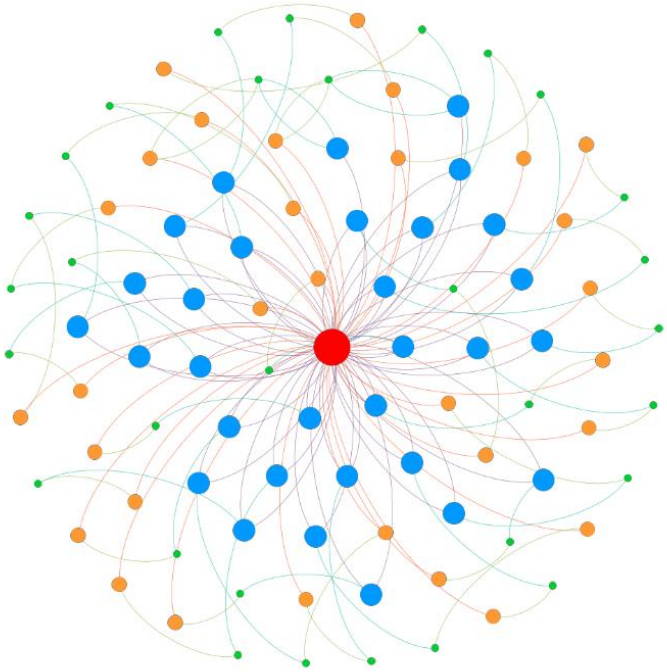

Figure 7. Graphical topology of the SIS II network (Fruchterman Reingold).

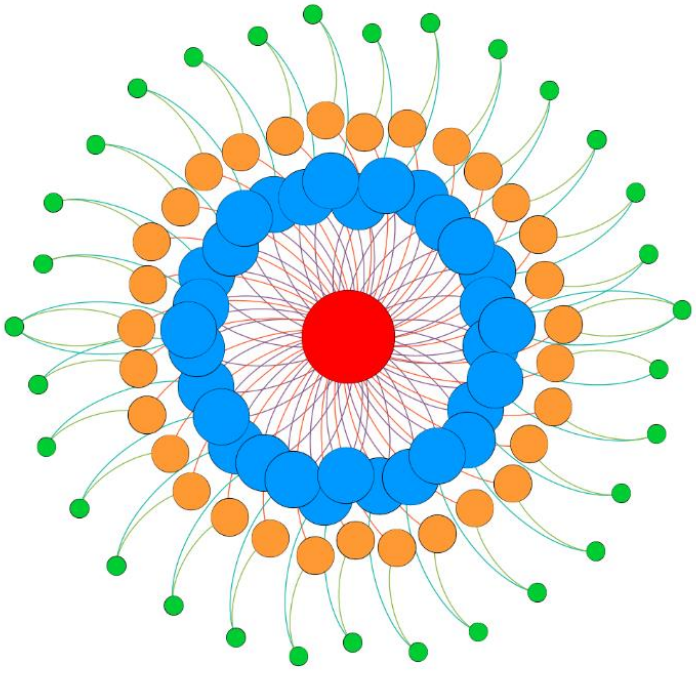

Figure 8. Graphical topology of the SIS II network (Yifan Hu).

Conclusion

I opened the empirical analysis of the Schengen Information System with the definition of information infrastructures as a 'shared, open (and unbounded), heterogeneous and evolving socio-technical system' of Information Technology (IT) capabilities (Hanseth and Lyytinen 2010: 4). In order to evoke this definition, I reconstructed the *socio-political*, *legal* and *technical* conditions that have shaped and driven forward the implementation and subsequent evolution of the SIS. By analysing each aspect separately, I was able to place the SIS technology back in the institutional, normative and organisational contexts of its development. This approach enabled to unearth the individual logics and policy processes that have established the SIS II as the most widely used information system in the EU AFSJ. The evolution of this large-scale EU database reveals striking parallels with the origins and development of subsequent EU schemes (e.g., the VIS, the PNR, etc.). While the EU Commission presented them as compensatory measures to the new terrorist threats, in reality they were 'forged' in the 'Schengen laboratory' (Parkin 2011: 1). The politics of emergency that generated a number of controversial features in the SIS II, such as the addition of biometrics and extended access to police authorities and intelligence services, has inherently set the stage for the development of subsequent expansions of the EU infrastructural basis through the implementation of large-scale multi-purpose (investigative) databases (Chapter 4 and 5).

What emerged from the analysis of the *socio-political* aspect is that the EU displayed an instrumental account to the development of the Schengen Information System. Information technology affects and in turn is affected by the implementation of the EU policy in the area of border controls and security. In case of the SIS, its evolutionary dynamics were given impetus by emergency-driven policymaking that conveniently exploited high-impact acts of political violence, such as 9/11 and the terrorist attacks in Paris and Madrid to introduce a number of controversial features (see also Bigo and Carrera 2004). IT systems are inherently controversial, and controversies are political. As shown in the analysis of its legal infrastructure, the development path of the SIS was marked by a series of internal controversies between different EU institutions. While the Commission has displayed a typically supportive attitude towards the new advanced features and functionalities, and indeed has pushed for their implementation by tabling a number of proposals, the Parliament (LIBE Committee) and the EU Data Protection Supervisor have often questioned their necessity and proportionality. The

emerging controversies have clearly impacted on the shape that the system would take, thus substantiating Hanseth and Lyytinen's definition of information infrastructures as an 'open (and unbounded) project' (2010: 4).

Another aspect of the SIS technical arrangement that further corroborates this claim is the possibility to activate "latent" functionalities. Essentially, this possibility reveals that the SIS information infrastructure was developed to be "sticky", that is, to be permanent. The finding that favours this assertion is related to the deployment of the logic of (in)security in order to drive forward the implementation of a number of controversial functionalities in the SIS, such as the AFIS system. As I have reported, both the AFIS and other newly-added features have been elaborated outside the typical development path, through agreements made between representatives of national police, interior ministries, and experts of security technology in non-binding Council conclusions, which are generally characterised by a profound democratic deficit. Consequently, the politics of emergency unleashed a dynamic by which the implementation and subsequent evolution of the legal and organisational components of the SIS were becoming increasingly dependent on technocratic expertise. This observation together with the instrumental use of the logic of (in)security suggest that the SIS not only is an unfinished project, but, crucially, it was never meant to be. In practice, it will be increasingly difficult to establish what form the system will take given its latent, flexible and adaptive architecture. Yet the costs of such institutional, normative and technical struggles over the system's configuration are high in terms of legal uncertainty and insecurity.

The SIS not only has evolved, but also is continuing to evolve as a result of the evolutionary dynamics that are directly built into the normative and technical arrangements of its architecture. Yet in the absence of proper oversight mechanisms the introduction of new features (e.g., the use of biometrics, inter-linkage of alerts and the use of SIS for discreet checks) pose profound ethical challenges regarding especially the EU principles of non-discrimination, data protection and privacy. Paradoxically, the development of the most innovative functionalities that have been intended to deliver more security, could serve to erode the freedoms and liberties of individuals, who will ultimately pay the price. By storing alerts on persons and objects it projects an understanding of security as concerned with the harm derived either from the movement of certain "illegitimate" categories of individuals (e.g., third-country national subject to a return decision, suspects of terrorism, traffickers, etc.) or from certain objects (e.g., stolen vehicles, misused documents, seized private property, etc.).

Effectively, the operation of inserting an 'alert' stigmatizes the person or object concerned as a threat to EU security. Once the 'mark' is inserted in the system, it assumes some action to be taken in the physical world. In this sense, the SIS transcends the boundaries between the digital and the physical world by eliciting multiple "cycles" of uses that have a direct effect on the individuals concerned by the inputted data.

Through network-like visualisations I sought to visualise these cycles in the form of the connections (edges) among the units that make up the SIS architecture (nodes). As we can observe, these connections are multilateral, never linear and potentially limitless since data travel through the SIS network as a result of the creation of multiple "cycles" of uses. Essentially, the power to "act" on the inputted data is the power to "make" security; this kind of power is socio-technical and socio-material since it circulates among an heterogenous set of actors (see Law 2008). These are human and non-human agents in the form of regulations and directives (materiality); software developers, engineers, legislators and security authorities (human agents); and, databases, cables etc. (technicality) (Ruppert and Scheel 2019; Glouftsios and Scheel 2021). Each of them have the power to re-compose the data in order to form the fabric of actionable security knowledge (see Bellanova and Fuster 2019). The side effect of going through multiple lifecycles is that an undefined number of investigative leads and thus more uncertainty is produced out of the inputted data, rather than less. These processes have been on-going since the setup of the SIS and are continuing to expand the data funnelled in processes of security governance.

Chapter 4

Towards EU Multi-Purpose Information Systems:

The Prüm Framework of Cross-Border Information Exchange

Introduction

In the absence of internal border controls, EU Member States had to address the issues of cross-border crime and irregular migration through the implementation of policies that would support pan-European cooperation in mobility controls. It was clear that traditional bilateral agreements and mutual legal assistance requests could no longer keep pace with the rapid movement of criminals across borders. This new scenario resulted in the adoption of several legal instruments that prescribed the development of technological infrastructures to continue ensuring security in the EU AFSJ. One of those instruments – considered in Chapter 3 – was the second-generation Schengen Information System (SIS II). SIS II paved the way for setting up a technological architecture designed to facilitate the exchange of information and to carry out law enforcement operations EU-wide. The politics of emergency that heralded the development of the SIS II information network has inevitably reconfigured transnational policing and has redefined the faces of security threats that were increasingly defined by the fault lines within societies. The interpretation of these risks by the EU has been accompanied by an aspiration for the expansive surveillance of individuals and by the promotion of science and technology in the mitigation of the risks derived from serious crime, terrorism and irregular migration (see Bunyan 2010; Dijstelbloem, Van Reekum, and Schinkel 2017; Jeandesboz 2010; Mitsilegas 2007; Van Dijck 2014).

The appropriation of science, and especially of forensic science, by political and police institutions was shaped by the "techno-scientific" imaginary related to the cross-border exchange of genetic information, specifically of DNA and fingerprints, as a way of solving crimes at the transnational level (see Amankwaa 2020; Machado and Granja 2020; Singler 2021). This imaginary was materialised through the implementation of another important instrument which further expanded the scope of the EU security apparatus: the so-called Prüm framework of cross-border information exchange. The Prüm framework sets out norms and procedures related to the automated searching and comparison of three categories of data: DNA, dactyloscopic (i.e. fingerprint) and Vehicle Registration Data (VRD). In particular, its development was framed by the increasing importance of the analysis of forensic data for investigating and preventing criminal offences, sustained by the belief in the infallibility of the scientific method (see also Amankwaa 2020; Butler 2006; Machado and Granja 2019; McCartney et al. 2011). To emphasise the convergence of science and technology, my main focus in this chapter will be on the genetic, DNA aspect of the Prüm instrument. This framing allows to make the analysis more narrowly focused and to demonstrate more clearly how the Prüm shapes policing across Europe in a special way compared to the SIS (Chapter 3) and the API and PNR systems (Chapter 5). However, in order to provide a complete picture of the data exchanged through the Prüm framework I also consider VRD data and include it in the network visualisations of the Prüm network.

The literature does not seem to provide a uniform definition of the Prüm, with some scholars conceiving it as a system or a set of systems (e.g., Machado and Granja 2020; Santos 2017; Santos and Machado 2017), and others as an information exchange framework (e.g., Johnson et al. 2015; Prainsack and Toom 2010). To obviate these differences, I use the term "framework" when referring to the set of legislative measures that regulate the cross-border exchange of information under the Prüm provisions; while I use the term "system(s)" – (plural) – only when referring to the decentralized set of national databases that exchange DNA, dactyloscopic or VRD data. There are two reasons behind the choice to favour the term "framework" and to use the term "systems" only in the strict technical sense. First, differently from the SIS which is an actionable centralised information system that contains alerts on wide categories of individuals and objects, the Prüm architecture has been conceived in the form of a sub-set of national databases arranged on a decentralised basis. Accordingly, referring to the Prüm as a "system" – (singular) – would obviate the core feature of its network arrangement. Second, given the absence of any central component at the EU level such as in the case of the

SIS, the Prüm can only be accessed through National Contact Points (NCPs) in the context of national criminal investigations and it is therefore loosely arranged. These features bring to the fore that the Prüm information infrastructure is held together by the legal framework for exchanging data rather than by any technical component.

Zooming in at efforts to reduce crime by fostering technical and scientific standardisation in the transnational exchange of genetic information, the Prüm framework constitutes the second case study in the composition of the puzzle of EU data-driven security governance. Addressing its development enables to examine how the fluidity of EU security governance has been extended to "techno-scientific" domains in the regulation of multiple aspects of everyday life. With the aim of controlling and monitoring "suspect bodies" (Haggerty and Ericson 2000; Janssen and Kuk 2016; Lyon 2016), the development of the Prüm is particularly representative of the concept of "assemblage" (Lanzara 2009) – already analysed in relation to the setup and functioning of the SIS II. Making the (criminal) body "visible" soon became the central preoccupation of the Prüm. The increased mobility in the Schengen area, combined with transnational threats to EU internal security, has culminated in the 'quest for visibility' (Besters and Brom 2010: 459) through DNA and biometric data. Behind this scope lies the assumption that 'collating and exchanging ever increasing volumes of data, including forensic bio-information, would automatically make the [EU] safer' (McCartney et al. 2011: 319). Accordingly, moving past the SIS, this chapter digs into the concept of 'assemblage' in relation to the use of the Prüm as a surveillant network for the identification and control of suspect bodies.

In line with the objectives of this research, the analytical efforts of this chapter are devoted to identifying the *socio-political*, *legal* and *technical* conditions that have led to the emergence of the Prüm framework. Yet much of the analysis is concerned with unearthing the specificities and challenges of using forensic DNA databases for criminal investigation purposes. The skeleton of this chapter largely resembles the structure of Chapter 3. The first part retraces the development of the Prüm, from the introduction of the Treaty of Prüm in 2005 to its transposition into the EU acquis in 2008. It examines the frictions that emerged during this policy process, together with the challenges faced by Member States in the operationalisation of DNA data exchanges (including the drafting, ratification and harmonisation of national legislation). Given that the implementation of the Prüm framework was concurrent with the EU political agenda for stepping up cross-border police and judicial cooperation, much of the

socio-political analysis reconstructs the history of moves towards the more systematic exchange of information for law enforcement purposes.

Bridging the *socio-political* analysis with the legal backbone of the Prüm, the second part examines more closely the central pillars that support the cross-border exchange of genetic information. In particular, it looks closely at the institutionalisation of the principle of availability in order to understand how it has lowered the barriers to the transnational exchange of DNA and biometric data. Accordingly, by addressing the *legal* conditions of possibility, this part aims to understand how agencies dealing with criminal activities like the police and the criminal justice system increasingly rely on forensic genetics in the detection and identification of offenders. To further dig into the relation between biology and technology, the third part examines the *technical* process that has shaped the implementation of the Prüm infrastructures. After outlining the procedures for transferring information cross-border, this part investigates how the resulting network of decentralised forensic databases aims at making the body a "site" of security vision by projecting identity from individual DNA fragments (see Maguire et al. 2018). Having addressed the *socio-political, legal* and *technical* specificities of the Prüm framework, the remaining of the chapter is dedicated to representing visually the Prüm (surveillant) network of data exchanges. The visualisations are sided by a description of the findings in relation to the discursive and visual reconstruction of the Prüm data lifecycle.

4.1. The "asynchronous" implementation of Prüm

The cooperation on the cross-border exchange of data between police and judicial authorities initially started as a multilateral Treaty, known as the "Prüm Treaty"[36], between only seven countries: Austria, Belgium, Spain, France, Germany, Luxembourg, and the Netherlands (Council of the European Union 2005). The Treaty was signed in the German town of Prüm on 27 May 2005 with a view to establish measures for stepping up cross-border police and judicial cooperation, and particularly to combat terrorism, cross-border crime and irregular migration. With the exception of Austria and Spain, it is not surprising that the other five countries initiated also the "Schengen Convention" (CISA) on 19 June 1990 (see Chapter 3). Especially, Spain had very little input into the first round of negotiations, that was mainly driven by Germany and the Benelux countries. In fact the Prüm Treaty is often referred to as "Schengen

[36] Also referred to as "Prüm Convention". These terms are often used interchangeably in the literature.

III" because of the same original intergovernmental grouping of Member States that set up the CISA (Belgium, Netherlands, Luxembourg, France and Germany) (Kierkegaard 2008). The link of the Prüm Treaty to the historical and political roots of the Schengen system also resonates in its preamble that states: "In an area with free movement of persons it is important for Member States of the European Union to step up their cooperation, in order to combat terrorism, cross-border crime and illegal migration more effectively" (Council of the European Union 2005, Ibid).

There are other instances that provide for the theoretical comparability of the two cases. First, although the Schengen system originally represented an effort to promote the free circulation of goods and services within the internal market, the political context of its development slowly began to converge with that of the Prüm. Especially, the history of Prüm can be traced back to a proposal made by the German Ministry of the Interior Otto Schily in 2003 (Luif 2007) in response to increasing concerns for EU security following the 9/11 attacks. Since its setup, the Prüm Treaty was motivated by an effort to develop an "Area of Freedom, Security and Justice" after the violent attacks in the USA (2001), as well as in Madrid (2004) and London (2005). Similarly, the evolution of the Schengen system, from SIS I to SIS II, was shaped by the politics of emergency after 9/11 (see Chapter 3). Second, the convergence towards an emergency-driven agenda soon resulted in the partial incorporation of both Treaties into the EU acquis. Originally, both initiatives were built around criminal databases which represented the so-called 'network goods'. Gaisbauer defines 'network goods' as 'club goods that create special incentives for incorporation (2013: 198). Once implemented, the so-called "network goods" fostered the transition from pure intergovernmentalism to advanced forms of cooperation[37] (Gaisbauer 2013).

Although the development of the Prüm framework bears the mark of the Schengen integration process, it did not go hand in hand with the evolution of the Schengen system. Balzacq and Hadfield defined their evolution as "asynchronous" (2012: 541), especially in relation to their institutional settings as well as to their temporal and functional differentiation. With the enlargement of the Schengen area, SIS I was expanded in terms of scope and functionalities, to accommodate its use by newly acceding Member States. This expansion resulted in the implementation of the second generation Schengen Information System (SIS II) which became

[37] The Prüm instrument was an international convention between seven EU Member States, before its integration into the EU legal framework in 2008.

fully operational on 9 April 2013. By contrast, the Prüm Treaty included a clause, leaving participation in such cooperation open to all other Member States in the European Union (Toom et al. 2019), but only few endorsed it. Between 2007 and 2008, ten countries (Bulgaria, Portugal, Sweden, Greece, Finland, Hungary, Italy, Romania, Slovakia and Slovenia) ratified the Treaty, followed by two non-EU Member States, Iceland and Norway (OJEU 2010b), that directly signed the so-called "Prüm Decisions" in November 2009. Under the Prüm Decisions (OJEU 2008b-c), parts of the Convention's agreements were formally transposed into EU law in August 2008, making the cross-border exchange of information mandatory for all the countries that had ratified the Treaty. However, at the time not all the signatories had taken the necessary steps to establish connections to other Member States and to develop an operational database with specific regulations (Costa 2020).

As a result, the path of implementation of the Prüm framework has been defined as "rocky" since 'it has not progressed smoothly or at the pace originally anticipated' (Sallavaci 2018: 225; see also Deloitte 2015). The signatory countries were given two deadlines to become fully operational: one year (26 August 2009), for the exchange of Vehicle Registration Data (VRD) and fingerprints, and three years (26 August 2011) [38], for the exchange of DNA data. However, by the time of the second deadline, only 11 Member States[39] were reported as being compliant with the legal and technical provisions for the exchange of DNA data under the Prüm Decisions.[40] By the end of October 2012, a total of 18 Member States met the operational requirements, although not all of them were exchanging data. Scholars have identified three main reasons to the "rocky implementation" of the Prüm Decisions: the lack of political prioritisation by new Member States as well as technical issues and financial limitations (see Sallavaci 2018). The state of affairs at the time of the operational requirements seemed to favour this explanation, as it revealed varying levels of national investment and political commitment across the EU as well as technical challenges related to the incompatibility of hardware/software components and connection issues (Sallavaci 2018; Topfer 2011). These difficulties inevitably undermined the development of a coherent infrastructure for transnational cooperation; however, they are only one part of the story.

[38] Council Decision 2011/472/EU on the launch of automated DNA data exchange in Portugal determined the deadline for implementing data exchange.
[39] From the initial group of 12, Portugal was the only country that, at the time, had not yet begun to exchange data, but was authorized to do so.
[40] States that were exchanging data in August 2011 were: Bulgaria, Germany, Spain, France, Luxemburg, the Netherlands, Austria, Romania, Slovenia, Slovakia, and Finland.

The reasons for the difficult implementation path should not be fully accorded to the technical and financial legacies of the newly acceding countries. At first sight the costs of operating the Prüm framework appeared to be significantly lower than in the Schengen case (Gaisbauer 2013). Nevertheless, becoming an operational member of the Prüm network is by far a more complex political and technical process that requires the setup of a decentralised network of national databases. Accordingly, before being capable of exchanging information cross-border, each Member State has to establish a bilateral connection with one or more countries. This means that 'the operability [of a country] is dependent on the readiness of the other Member States to participate' (Sallavaci 2018: 225). Accordingly, as the costs for establishing individual connections are high, not all Member States may be willing to extend their usage of the Prüm to all operational Member States (Deloitte 2015). This necessarily constituted a major hindrance to the development of a decentralised system of information exchange EU-wide. And, as a consequence, it favours thinking that the implementation of the Prüm framework was halted not only by endogenous factors but also by exogenous ones.

In the study conducted by Deloitte (2015) on behalf of the EU Commission, it has been reported that Member States did not feel legally bound to interconnect completely. Hence, partial implementation and the reluctance of some Member States to continue investing in creating connections affected the prospect for rapid expansion of the Prüm network of information exchange (Deloitte 2015). On this basis it is possible to distinguish two phases in the development of the Prüm framework: a fast-paced phase of ratification and a slow-paced phase of operationalisation. The first one is characterized by an initial impetus to join the Treaty, that produced rapid dynamics of inclusion of the newly acceded Member States. The ratification of the Convention by 12 countries only three years after the introduction of the Treaty supports this claim for rapid inclusion (Gaisbauer 2013). By contrast, the second phase was characterized by slow progress in the operationalisation of the provisions that have been ratified. Accordingly, the implementation of the Prüm was not only asynchronous vis-a-vis the evolution of the Schengen system, but it also suffered from the internal asynchronicity among the signatories countries. This asynchronicity regarded disparities in terms of the size of the national DNA databases, the volume of profiles exchanged and of resulting matches (Santos 2016). As a result, the initial enthusiasm that led 12 Member States to promptly embark on the Prüm project was not followed by the likewise willingness to operationalize it.

The 2016 report on the state of implementation of Prüm listed 22 countries as operational (Council of the European Union 2016). Besides non-EU members like Norway, Iceland, Switzerland and Lichtenstein, 6 countries were listed as non-operational: Denmark, Greece, Croatia, Ireland, Italy, and the United Kingdom. At the time that the second report was produced in January 2017, the same countries were reported as in the process of implementing the Prüm DNA system at the national level (Council of the European Union 2017). Reasons for not implementing the Prüm Decisions were diverse, and included that countries such as Greece, Italy and Ireland did not have DNA databases or dedicated legislation when the Prüm Decisions were adopted. According to the latest report by the EU Commission of December 2021, 26 signatory countries are now operational with regard to the automated exchange of DNA and fingerprints, and 25 have implemented the vehicle registration data (VRD) category (European Commission 2021a). Therefore, out of 29* Member States[41] that have joined the Prüm network, only Greece, Italy and Norway are not operational, yet they have either installed the national DNA database or are undergoing technical preparations to do so.

Early technical challenges involved in the "rocky" application of forensic databasing techniques to police and criminal justice cooperation meant that the initial development of Prüm took place within law enforcement bureaucracies such as national forensic laboratories and police agencies, in connection with the private domain (McCartney et al. 2011). Especially, the Prüm software was developed jointly by DNA and IT experts from the Bundeskriminalamt (BKA) in Germany, the Ministry of the Interior of Austria and the Netherlands Forensic Institute in the Netherlands (Toom 2018).[42] Subsequent deliberations over its utilisation required the involvement of a much wider set of actors, especially in support to the circulation of information (McCartney et al. 2011). Key stakeholders in the operation of Prüm are law enforcement and judicial authorities responsible for the prevention and investigation of criminal offences; national vehicle registration authorities; the custodians of the national databases interconnected by the Prüm framework; and forensic laboratories/institutes responsible for the forensic assessment of the results of automated matching of biometric data. Other important stakeholders include various EU bodies, organisations and networks, whose

[41] The number considers EU Member States as well as Schengen associated countries. The UK was part of Prüm when the Decision to implement it was taken in 2008, it then withdrew in December 2014 and it later sought to re-join, despite Brexit. It is now reported as operational with regard to the first two categories of data, but not with regard to VRD.

[42] See also Annex 1.
https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

expertise concerns mainly the data protection and oversight aspect of the Prüm initiative. These are national data protection authorities; the European Data Protection Supervisor (EDPS); the European Union Agency for Fundamental Rights (FRA); the Committee of Civil Liberties, Justice and Home Affairs (LIBE Committee); as well as non-governmental organisations.

4.2. Pillars of information exchange

Retracing the *socio-political* conditions that shaped the emergence of the Prüm framework inevitably implies to reconstruct the long history of moves towards the more systematic exchange of information for law enforcement purposes. The rationale behind the development of the Prüm finds its roots in the policy progress that has been made since the beginning of the 1990s to enhance police and judicial cooperation and increase the amount of information exchanged. The first steps towards this twofold objective were taken with the introduction of the 1990 Schengen Convention (OJEU 2000a), followed by the 1995 Convention on the establishment of a European Police Office (EUROPOL) (OJEU 1995b) and the 1998 Convention on mutual assistance and co-operation between customs Administrations (Naples II) (OJEU 1998). These acts of law legally grounded information exchange between law enforcement authorities of EU Member States with the purpose to detect, prevent and investigate criminal activities. The need to improve information exchange for law enforcement purposes was reiterated in the European Council conclusions of Tampere as early as 1999 (European Parliament 1999) and has been remarked ever since. The introduction of these resolutions was followed by a number of policy initiatives, justified by the rhetoric of "newly emergent terrorist threats" that were increasingly assuming a cross-border dimension (OJEU 2006b-c-d).

Post-9/11 justifications advanced by the EU for stepping up cross-border police and judicial cooperation revealed that the exchange of data, and especially of forensic data, was set to become the major asset in the fight against transnational crimes. And thus, technological systems were going to assume a central role in the process of exchanging information for security purposes. To this regard, the preamble to Council Decision 2005/671/JHA stated that 'it is important to promote the exchange of information as widely as possible, in particular in relation to offences linked directly or indirectly to organised crime and terrorism […]' (OJEU 2005b: preamble, para 10). This dramatic shift in the definition of the conditions under which

security had to be provided necessarily altered the relationship between the state, law enforcement authorities and the citizens. In what follows, I reconstruct the individual moments of policy expansion through which the EU sought to step up information exchange and cross-border judicial cooperation. I focus in particular on three pillars of information exchange: the "Hague Programme" (OJEU 2005a), Council Decision 2005/671/JHA (OJEU 2005b) and the "Swedish Initiative" (OJEU 2006d). For ease of reference I created a table (Table 2) which plots the policy pillars of information exchange and the political events that triggered the policy responses (by year of implementation/occurrence).

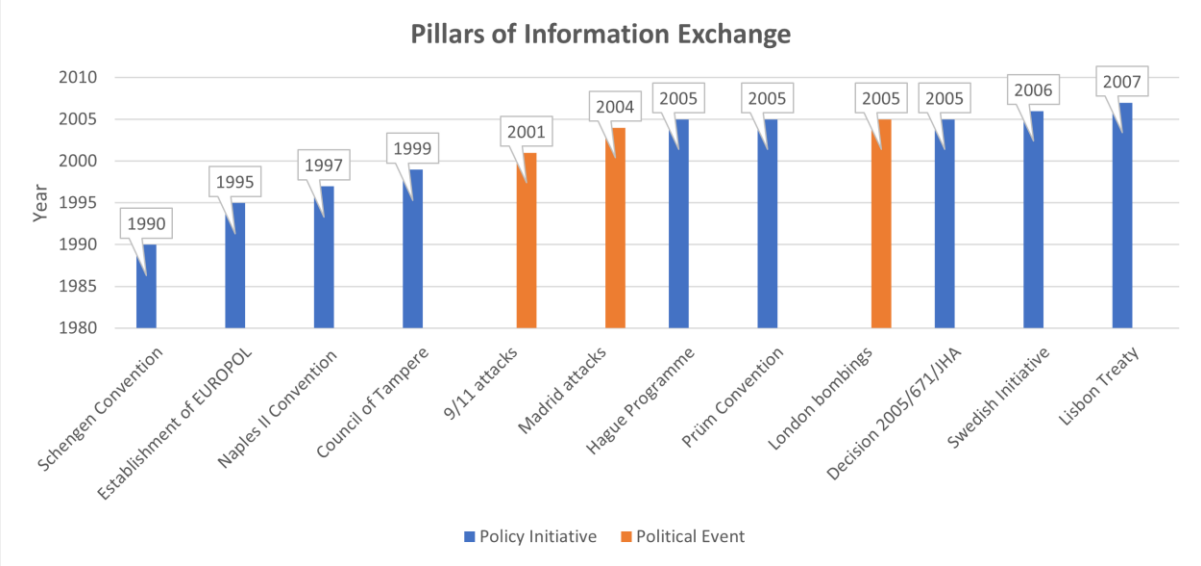

Table 2. Pillars of Information Exchange (Author's elaboration).

At the time when the Prüm Treaty was signed, two events were on top of the EU policy agenda (Balzacq and Hadfield 2012). On the one hand, the accession to the Schengen area of 10 new Member States on 1 May 2004 (see also Chapter 3). On the other hand, the European Council adopted a very ambitious programme in November 2004, the so-called "Hague Programme" (OJEU 2005a), as a result of the acts of political violence that threatened the development of an EU Area of Freedom, Security and Justice. The central tool of this initiative is information exchange (Balzacq and Hadfield 2012). The Hague Programme is not only the foundation of many schemes of cooperation between law enforcement agencies, but even more importantly, it is the foundation of the EU infrastructure for data management highly reliant on large-scale information systems. Law enforcement work is inherently an information-based activity. Investigators need to have fast, streamlined and systematic access to up-to-date information in order to prevent, detect and investigate crimes more effectively. The Hague Programme, and

later the Prüm framework, constituted one of these avenues, built specifically to step up the exchange of information. Since these Acts form the basis of cross-border information exchange, they are relevant also to the other AFSJ systems. Yet, the decision to include this information in this chapter is closely related to the understanding of the Prüm as a framework for exchanging information, rather than as a system – as explained at the outset.

The language used to justify the introduction of the Prüm was in fact imbued with the ideal of "free flow" of information initially promoted with the introduction of the "principle of availability" or "principle of equivalent access to data" through the Hague Programme. Under this principle, 'the mere fact that information crosses borders should no longer be relevant' (Ibid). This provision was designed to allow police and judicial authorities in one Member State to access information held by other Member States with as few procedural and judicial obstacles as possible. In a note, the Luxembourg Council Presidency stated that: "The aim is obviously that as large a list of information categories as possible is exchangeable with as little effort as possible" (i.e. requiring a minimum number of formalities, permissions, etc.) (Jones 2011: 6). Accordingly, the Hague Programme effectively triggered the promotion of a comprehensive inter-agency, cross-border approach to the exchange of information between police and judicial authorities. Since its implementation, it has contributed to enlarge the scope of information exchange beyond geographical boundaries and should therefore be regarded as the first step towards the consolidation of the European information infrastructure.

The policies that were implemented immediately afterwards were characterised by the same "cross-border" impetus. In particular, the second policy tool that supported the mobilisation of information beyond territorial jurisdictions was Council Decision 2005/671/JHA. The Decision was implemented after the violent event of the London bombings in 2005, whose overarching consequences were used to legitimise the extension of the scope of information exchange 'to all stages of criminal proceedings, including convictions, and to all persons, groups or entities investigated, prosecuted or convicted for terrorist offences' (OJEU 2005b: preamble, para 4). Since its introduction in 2005, each Member State is obliged to transmit information concerning criminal investigations, prosecutions and convictions for terrorist offences to Europol and Eurojust (Article 2(3)). Specifically, the Decision calls for Member States 'to ensure that any relevant information […] seized or confiscated in the course of criminal investigations or criminal proceedings in connection with terrorist offences can be made accessible as soon as possible […] to the authorities of other interested Member States' (Ibid,

Article 2(6)). This statement reiterates the need for 'equivalent access to data' and it thus constitutes a clear expression of the principle of availability.

The need to establish a smooth and secure channel for exchanging information cross-border was further promoted by the so-called "Swedish Framework Decision" (or "Swedish Initiative") (OJEU 2006d). Adopted in 2006, this measure aimed at setting the basis for a legally binding framework that would increase the effectiveness of data sharing between law enforcement authorities within the EU. The legislative provisions advanced therein constitute a reinforced version of the principle of availability. In particular, they establish that the conditions and procedures for cross-border data exchanges are not more restrictive than those applying at the national level ("principle of equivalent access", or "access on equal terms"); they also set out common rules regarding time limits and standard forms for the exchange of operational and strategic crime-related information held by law enforcement authorities. These provisions were predicated upon the principle of mutual trust between Member States. The successful operation of this principle, also known as "principle of mutual recognition", implies that judicial and police authorities in one Member State should trust the decisions of the authorities of another Member State when it comes to cross-border judicial co-operation.

However, the principle of mutual recognition does not automatically establish a regime of recognition and execution: mutual trust does not imply a removal of national barriers to the smooth and expeditious exchange of information, especially in the absence of a commonly accepted channel for information exchange. The Hague Programme and the Swedish Initiative were merely declarations of intent which required the implementation of dedicated databases and communication networks in order to ensure the transition from 'technological possibility to operational actuality' (McCartney et al. 2011: 320). In the context of the Prüm Convention the switch from intended scope to practice occurred in 2008 with the incorporation of the provisions of the 2005 Prüm Treaty into EU law. In particular, the cooperation that initially started as a multilateral Treaty was shifted to the EU level through two Council Decisions (2008/615/JHA and 2008/616/JHA), herein referred to as "Prüm Decisions" (OJEU 2008b-c). The Prüm Decisions include the obligation to establish databases for the automated search of DNA, dactyloscopic (i.e. fingerprint) and vehicle registration data, and set out procedures for the supply of information in relation to major events and in order to prevent terrorist offences.

The way in which the Prüm Treaty was forced through has been criticised for its circumvention of the normal consultative process (see Balzacq et al. 2006; Bellanova 2008; Bigo et al. 2009;

Kierkegaard 2008; McCartney et al. 2011). At the European Council of Ministers of Justice and Home Affairs (JHA) in Luxembourg on 12 June, the Council agreed to transpose substantial parts of the Treaty into the EU legal framework without the scrutiny of the European Parliament[43] and the judicial control of the Court of Justice. This manoeuvre was condemned by the European Data Protection Supervisor (EDPS 2007) in its 2007 Opinion for crucially lacking in democratic legitimacy. Despite this legacy, the incorporation was binding on the Member States that had signed the Prüm Treaty. Thus, what was first declared "on paper" provided the opportunity for setting up a hi-tech information infrastructure that conflated forensic science and IT systems for the effective and efficient exchange of information on "suspect bodies". The Prüm framework along with proposals to develop new systems were all framed in a way as to allow public authorities to gather, store, process and exchange large amount of personal data for a variety of purposes beyond criminal proceedings, such as for border management, asylum applications and law enforcement investigations. As a result, the principle of availability and of mutual recognition paved the way for the profusion of a vast number of different systems that consolidate science and technology for the facilitation of information exchange between different law enforcement bodies.

4.2.1. Towards "second-generation" Prüm ("Prüm II")?

Until 2018, that is eight years from their adoption, the Prüm Decisions have not undergone successive amendments to expand the scope of the Prüm exchange framework. This unaltered status partly derives from a decision taken during the meeting of the EU Council of Ministers of Justice and Home Affairs in 2007 when Ministers declared that the technical implementation of Prüm "must remain unchanged"[44] (Toom et al. 2019: 55). On the contrary, the SIS was conceived from the beginning with the view to build a 'flexible' technological architecture that, according to the EU Commission, would enable the incorporation of new functions as soon as this would become "technically feasible" (see Chapter 3). Although the implementation of the Prüm at the national level proceeded at a slower pace compared to the SIS, the initial impetus to step up and thus to expand the Prüm network of information exchange remained at the core of its development. Some scholars define the nature of Prüm as "aspirational" since its

[43] The European Commission should ensure that the European Parliament is fully included in the first phases of the evaluation process and its opinion is taken into due account when defining the political orientations of the policy framework, including a debate on technical details.
[44] See also https://www.parlementairemonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvij5epmj1ey0/vi3aqkaxuix2/f=/blg11264.pdf

rationales and objectives are future oriented (Wienroth 2018: 12). The aspiration of Prüm, however, was "neither deepening, nor widening" (Balzacq and Hadfield 2012: 541), but rather, I argue, to project the "techno-scientific" imaginary of the free flow of data into material infrastructures.

Essentially, the Prüm Treaty was primarily conceived as a shortcut to the implementation of the principle of availability as enclosed in the Hague Programme. On one hand, the principle of availability was aimed at diluting the national boundaries to cross-border exchanges by lifting the sovereign power of Member States over the collection, retention and use of data. Combined with the principle of mutual recognition, this principle prescribed to make full use of the available technology in order to ensure that there were no barriers to the reciprocal access to national databases (Kierkegaard 2008). On the other hand, the Prüm framework maintained the national prerogative over the manipulation of data (Balzacq et al. 2006) and can thus be understood as a minimal version of the principle of availability. In particular, the Hague Programme intimated that direct access to data should be the norm. Whereas, according to the Prüm Decisions, each Member State may identify the data (DNA profiles, fingerprints etc.) accessible to other Member States and determine the conditions for automated searching (OJEU 2008c: para 13 and 18). Yet, the process of streamlining information exchange under the Prüm framework proved to be extremely "complex, technically fraught and expensive", as concluded by the Polish Presidency (Council of the European Union 2011: 4; see also (Jones 2012: 1).[45]

Dyson and Sepos describe the trajectories by which European States implemented the Prüm as a form of 'differentiated integration' (2010: 4). This term denotes the movement at different speeds towards the achievement of common policies. Despite significant progress and evaluation visits being made, some Member States were still in the process of implementing the 2008 Prüm Decisions when consultations on launching the "next generation" Prüm were conducted ten years later (European Commission 2020e). The "rocky" implementation of Prüm (Sallavaci 2018) partly explains why its status remained unaltered for so long. With most Member States lagging behind in the operationalisation of the Prüm Decisions, the aspiration to expand the framework remained on hold. However, the orientation towards future goals, especially crime prevention, continued driving the development of and investment in techno-

[45] Presidency, 'Implementation of the Prüm Decisions – lessons learned', 20 December 2011 (EU Doc. No. 18676/11), p.4. http://www.statewatch.org/news/2012/jan/eu-council-prum-data-exchange-evaluation-lessons-18676-11.pdf

scientific infrastructures, closely related to software packages and innovative solutions in the field of biometric identification (see Jakubowska and Naranjo 2020). The opportunity to improve the functionalities of Prüm eventually came to the forefront with the Council conclusions of 18 July 2018 (Council of the European Union 2018c).

The Council invited the Commission to consider revising the Prüm framework "with a view to broadening the scope of the Decisions and, to that end, to updating the necessary technical and legal requirements" (Council of the European Union 2018b, Ibid). The reform was intended to remedy to the existing shortcomings in the Prüm architecture and to further enhance cross-border police cooperation. As stated in the 2020 Inception Impact Assessment (European Commission 2020c), the specific policy objectives were to review the efficiency of the exchange of current data categories; to broaden the scope of the automated exchange to additional data categories (e.g., facial images, driving licences, firearms[46]) available in the criminal databases of Member States; to speed up and streamline the "hit" follow-up procedure;[47] to allow Europol to feed the Prüm database with data received from third countries; to extend the scope of affected persons from suspects and convicted to missing and deceased persons; to align the instrument with the latest EU data protection rules (i.e. the General Data Protection Regulation (GDPR) and the Law Enforcement Police Directive); and to introduce a central router for search and comparison instead of the original decentralised network.

In relation to these objectives, the Council invited experts of the Council's Working Party on Information Exchange and Data Protection ("DAPIX") to evaluate the possible amendments and called upon Member States to continue the broadening of operational connectivity among themselves. From its establishment as an "Ad hoc Group" through to its current formal status, the tasks of DAPIX involved the oversight of the implementation and operation of EU-wide information exchange instruments, including the Prüm.[48] The DAPIX is also responsible for ensuring that information exchange between law enforcement authorities of Member States complies with the latest principles and rules on data protection. To evaluate this aspect, the EP LIBE Committee commissioned a parallel study (Toom 2018) in order to assess the ethical,

[46] See Council of the European Union (2021a) Proposal for the possible inclusion of national databases on firearms and their owners in the future Prüm framework, Brussels, 16 February 2021, 5787/21.
[47] The "follow-up procedure" is the process that happens after the automated search has produced a match (a "hit").
[48] Source: https://www.consilium.europa.eu/en/meetings/mpo/2017/4/working-party-on-information-exchange-and-data-protection-dapix-(255033)/

legal and social implications of forensic genetics in general, and in the context of the Prüm in particular. Discussions about the introduction of a new data category were prompted by the development of the AFIS functionality. The first Focus Group meeting for the feasibility of face recognition was hold in Vienna in April 2019 with the purpose to provide stakeholders with an overall analysis of the "next generation" Prüm.

Meanwhile, the Commission opened the consultation procedure (European Commission 2020e) on the reform by mandating the consultancy firm Deloitte to conduct a feasibility study, looking specifically at the possibility to integrate facial recognition technology. The final report was published in May 2020 (Deloitte 2020) and it identified opportunities for improvement in the following areas: improving automated data exchange; introducing new data categories; introducing a new IT architecture; exploring the possibility of linking Prüm to other information systems and to interoperability solutions; and lastly, integrating other stakeholders (Ibid). The LIBE Committee report (Toom 2018) is more critical than the Deloitte report (2015) and provides a series of policy recommendations on the implementation of potential new functionalities. As a result of the consultation procedure, DAPIX declared that the facial recognition technology was 'mature enough' to be implemented as an additional biometric tool. This is a clear example of 'technological development driving policymaking' (McCartney et al. 2011: 317). The Council also invited Europol to examine the possibility to become a partner in the Prüm framework so to enable the cross-matching of DNA and dactyloscopic data with third countries.

Despite already having access to a wealth of personal data under the existing Prüm rules, by doing so, the Commission wanted to enable access to even more data as soon as this became "technically" feasible. This commonality with the expansion of the SIS II testifies the EU Commission's effort to build "flexible" systems in order to make easier the introduction of new functionalities. In case of the Prüm, the main objective of such an application was the additional checking of images of unknown perpetrators of criminal offences against the national reference image databases (Council of the European Union 2019a). When these technical steps towards further technological harmonisation were tabled, differences in data protection provisions between the Member States continued to challenge the process of standardisation of information exchange at the EU level (Sallavaci 2018). The integration of new data categories into a decentralised network like the Prüm is indeed hard to achieve without some form of centralised accountability and oversight (Jones 2012; Sallavaci 2018). The duality between the

harmonization of technical procedures and the localities of the legislative understandings of proportionality and the right to privacy has inevitably created frictions in the implementation of Prüm (Prainsack and Toom 2013). At the same time, the differentiation in the degree of operationalisation between Member States, with some providing for larger databases and thus for a greater variety of offences being targeted, has contributed to the creation of inequalities at the level of fundamental rights as a result of the exposure of some citizens to searches for a greater number of offences, including minor ones (Sallavaci 2018).

These legal challenges have been remarked also by the European Digital Rights (EDRi), in response to the Consultation forwarded by the EU Commission. The EDRi strongly opposed the inclusion of facial images in the Prüm framework, as this would increasingly expand the surveillance powers of the police (EDRi 2020). Especially, the EDRi warned about the transformation of the EU area into a "police state" where the logic of transnational crime control would trump due process (Ibid). In this regard, the EDRi Policy Advisor, Ella Jakubowska, warned that: "these deployments of untargeted mass biometric processing systems - whether by law enforcement, public authorities (such as schools or local councils), or private actors – do not meet the required justifications or thresholds of necessity or proportionality to be considered lawful for the level of violation and intrusion they create" (Jakubowska and Naranjo 2020: 4). Despite the advancement of these concerns and the lack of a uniform data protection regime, the prospects for enlarging the scope and depth of Prüm were eventually tabled on 8 December 2021 with the EU Commission's proposal for a "next-generation" Prüm (nicknamed "Prüm.ng", or "Prüm II") (European Commission 2021b).

The expansion of the Prüm framework in the "Prüm II", rather than aiming to subvert its architecture and scope, was defined by the attempt to integrate further elements in the aspiration to realize the "techno-scientific" imaginary underpinning its development. Thus, legal fine-tuning and the introduction of more substantive provisions were but a means towards this future-oriented goal. Comparing the expansion of Prüm to the evolution of SIS I into SIS II would nevertheless be deceiving. The SIS II architecture was conceived as brand-new in order to cope with the EU enlargement and to equip the system with "latent" functionalities (see Chapter 3). Whereas Prüm II essentially builds on the existing framework, and seeks to reinforce it through the modernisation of the existing tools for cross-border information exchange. What Prüm II thus envisages is the achievement of the objectives originally laid down in the Prüm Treaty, that the "first generation" Prüm has yet failed to fully achieve.

4.3. From the *local* crime scene to the *transnational* exchange of forensic data

As remarked earlier, the stipulation of the Prüm Treaty had the objective of diluting the national boundaries of law that were preventing the cross-border exchange of specific categories of information. The materialisation of this "techno-scientific" imaginary occurred in 2007, when the Justice and Home Affairs (JHA) Council agreed to integrate the majority of the Treaty provisions into the EU legal framework. The incorporation of Prüm into the EU acquis in August 2008 resulted in the adoption of Council Decision (2008/615/JHA), along with an accompanying Decision (2008/616/JHA) related to the implementing measures. The so-called "Prüm Decisions" (OJEU 2008b-c) form the legal backbone of the Prüm framework and contain provisions for the regulation of four interrelated areas of cross-border information exchange. The first one concerns the automated search and comparison of three data categories, that is DNA profiles, dactyloscopic data and national Vehicle Registration Data (VRD); the second one concerns the transfer of data in the context of major events with a cross-border dimension; the third one regards the supply of information for the prevention of terrorist offences; and the last one concerns various measures, such as joint patrols, for stepping up cross-border police cooperation. These legal pillars effectively mirror the "techno-scientific" imaginary of the original Prüm Treaty which sought to dilute national boundaries of information exchange through the confluence of biology and technology in the investigation and prosecution of suspects and unsolved crimes at the pan-European level.

Indeed the preamble to Decision 2008/615/JHA refers to the need to introduce procedures for promoting fast, efficient and inexpensive means of forensic data exchange for the investigation of criminal offences, particularly terrorism and cross-border crime. To this regard, it establishes that 'Member States grant one another access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data' (OJEU 2008b: preamble). The promotion of the transnational exchange of forensic data through the Prüm framework has two important dimensions: scientific and technological. Scientific because it relies on the use of DNA and dactyloscopic data (i.e. biological traits) as means for ascertaining identity. This procedure promotes the confluence of biology in the application of genetic profiling databases that, for long, have been a consolidated forensic technique deployed within the domain of law enforcement bureaucracies such as national forensic laboratories, police agencies or Interpol (Matos 2019). Technological because the comparison and evaluation of

DNA sequences or of dactyloscopic data requires the use of algorithmic analysis tools and databases (i.e. technology) mostly dedicated to the storage of DNA profiles of convicted offenders or profiles of unidentified stains collected during criminal investigations. Clearly these two dimensions are interrelated. Yet, what initially were meant to be local procedures in the setup of the Prüm infrastructures, slowly began to be employed as a neutral method for solving serious crimes transnationally (Prainsack and Toom 2010, 2013).

4.3.1. Legal harmonisation

The removal of national legal barriers to information exchange inevitably projected the forensic information collected from the "local" crime scene to the "transnational" screens of all EU Member States. Nevertheless, in order to take part to the transnational exchange of forensic information, Member States had to fulfil numerous legal and technical requirements. Within the EU there are different types of judicial systems, with different laws and criteria for the operation of genetic databases (Costa 2020). The greatest inconsistencies mainly regard different understandings of the criminal justice system, and thus different domestic regulatory frameworks for the exchange of data and their use as evidence. For instance, the national DNA database of a country may include suspects, convicted profiles, crime stains, unidentified persons and other categories of files, while another may include only profiles of convicted or missing persons. A country can also have different criteria regarding the removal of such files, the police practices for collecting and storing forensic data, the criminal typology, and the attributed penalty (Costa 2020). Another issue concerns the understanding of what constitutes a "serious crime". Some countries decide to exchange information regardless of the crime, while others may exchange information only on crimes considered "sufficiently serious" to justify the exchange (Matos 2019: 156).

This narrower understanding inevitably results in a narrower conception of the data that must be entered, searched and be made available for comparison (Matos 2019). The Prüm Decisions were intended to overcome these differences and to ensure greater harmonisation in the circulation of data. Therefore, the adjustment of domestic regulatory frameworks was the first requirement towards this objective. However, at the time of their adoption, the legal provisions regulating data processing for law enforcement purposes were missing, as Framework Decision 2008/977/JHA had not yet been adopted, let alone its successor, Directive 2016/680/EU ("Law

Enforcement Directive") (OJEU 2016b)[49]. In the absence of a uniform data protection regime at the EU level, the fundamental rights aspect of Prüm exchanges was difficult to supervise and be attained in practice. The data protection rules included in Chapter 6 of the Decisions deal specifically with data exchange within the scope of Prüm, thus effectively transforming the national monopoly on the collection, retention and use of data into an EU-wide right under the principle of availability (Balzacq and Hadfield 2012).

Under the Prüm Decisions the obligation to establish forensic databases available to other Member States replaced any voluntary mechanisms for cooperation on the cross-border exchange of information (Bellanova 2008). Accordingly, compliance with harmonised rules was the first step towards the creation of a framework that would permit the cross-border exchange of highly sensitive information, regardless of the presence of significant safeguards at the EU level. Especially, the projection of the Prüm infrastructures was instrumental to the creation of 'administrative artifacts' that would enable to operationalize the transnational exchange of forensic data (Costa 2020: 564). In this way, the Prüm framework was intended not only to manage the exchange of data, but also of judicial mechanisms, where the national boundaries related to different legal systems and legislations were effectively diluted. The new configuration of "legal borders" has in turn created a European space where the movement of "suspect" bodies was increasingly controlled and managed through forensic databases. Based on unique biometric identifiers, the Prüm infrastructure was directed at the creation of an apparatus in which different actors collaborated not only in the transnational exchange of data, but also in the internal surveillance of the European territory (Costa 2020).

In addition to conforming to these legal requirements, prospective Member States were also required to undergo an evaluation procedure, as foreseen in Decision 2008/615/JHA (Article 20). This requirement imposes an obligation to fill in and submit a data protection questionnaire, to conduct a pilot run and to pass an evaluation visit (OJEU 2008b). The questionnaire indicates the data category (i.e. DNA files, fingerprints or VRD) that the Member State was seeking to start exchanging. The evaluation visit consists in inspecting the infrastructures and the techniques implemented in each country for the operational exchange of DNA, dactyloscopic or VRD data. Finally, the pilot run involves carrying out the simulation

[49] Directive 2016/680 on the protection of natural persons with regard to processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data repealing Council Framework Decision 2009/977/JHA.

of a data exchange exercise with another country. At the end of these three steps, an evaluation report is submitted to the Council, which after consultation of the Parliament unanimously decides whether the conditions have been met (Jones 2012). Once the Council adopts the implementing decision, the Member State concerned can start the operational exchange of data with the Member States with which it has established a bilateral connection.

Yet, the establishment of a decentralised network of bilateral connections is a complex process that requires Member States to satisfy also a number of technical requirements. In particular, the Prüm Decisions include the obligation to set up databases related to automated DNA analysis files (forensic DNA databases), automated dactyloscopic identification systems (AFIS), and national platforms for the exchange of vehicle registration data, as well as modalities for mutual access to the national databases (OJEU 2008b-c). Accordingly, in the absence of any central component at the EU level, the Prüm framework organises the cross-border exchange of information on a decentralised basis. The result is a complex technical architecture of bilateral connections that varies in the degree of connectivity between operational Member States. For instance, a Member State may undertake a large scale exchange of data against every other operational Prüm database; or rather, it may decide to connect with only one or two neighbouring countries, and exchange data only on one data category. For the purposes of supplying data, the Prüm framework stipulates a series of other technical requirements, related specifically to the modalities of mutual access.

Each Member State shall first designate the authorities that will act as National Contact Points (NCPs) (OJEU 2008b, art 6) to facilitate and manage the exchange of forensic data. Once appointed, the designated authorities become central actors in the Prüm network (Costa 2020). Their powers are governed by the applicable national law, and generally involve the conduct of the necessary procedures to perform automated exchanges on a daily basis. These tasks include the organization and implementation of the connections with other databases for the purpose of receiving and sending information; the performance of tests with partner countries; and, most importantly, the management and reporting of DNA matches. The signatory countries have attributed this role to different entities, ranging from judicial authorities to police forces, whose responsibilities vary according to their organizational structure (Machado and Granja 2018 and 2019). Despite national differences, in general, the NCPs are in charge of carrying out the routine work that enables DNA data to be exchanged transnationally. Member States must first ensure the availability of their national databases for the automated search and

comparison of DNA, fingerprints and vehicle registration data. Access to information held at the national level is then achieved by recurring to NCPs that are tasked with overseeing the transmission procedure.

4.3.2. Techno-scientific harmonisation

The Prüm Decisions establish norms and protocols related to the transmission procedure for the automated searching and comparison of DNA profiles and dactyloscopic data. As observed, given that the architecture of the Prüm does not contemplate a centralised computer server, the exchange of data is carried out on the basis of an "any-to-any" communication model: the transmission of data runs through a decentralised infrastructure of databases and is achieved in two steps, commonly referred to as Step 1 and Step 2. Step 1 is a techno-scientific process that concerns the cross border exchange and comparison of DNA data and fingerprints, based on a "hit"/"no hit" principle. This stage is governed by the rules stipulated in the Prüm Decisions and subscribed by each operational Member State. Accordingly, the procedures followed for the automatic exchange of information relating to DNA, fingerprints and VRD are highly standardised. Whereas Step 2 regards the actions taken by the requesting country following the result of Step 1 in a positive "hit". This stage is dependent on the successful outcome of the first step and is governed by national legislation. Hence, this two-step approach varies in the degree of harmonisation of the rules, from the highly standardised procedures of Step 1 to the local norms of Step 2.

In conformity with the rules established under Decision 2008/615/JHA, each operational Member State makes its data available to be exchanged with and/or searched by other Member States by creating a copy of its forensic database. Step 1 starts once a country has fully implemented the Prüm Decisions and is then allowed to commence exchanging DNA or dactyloscopic data with the operational Member States with which it has established a connection. However, once operational, a country does not automatically exchange all the data or profiles retained at the national level. The cross-border exchange is first subjected to the selection, evaluation and prioritization criteria of each Member State, resulting in the drop-out of potential reported hits. For instance, a country may decide not to create a copy of a certain profile category such as victims or volunteers, thus limiting the scope of the data available for the automatic exchange. Only the DNA profiles or dactyloscopic data filtered for search or comparison are fed to the Prüm database. DNA profiles are typically obtained from crime scene samples and contain a letter or number code which represents a set of identification

characteristics of the noncoding part of the DNA sample. Whereas dactyloscopic data refers to fingerprints, palm prints or images of latent fingerprints or palm prints.

In order to assure that no personal information is exchanged during Step 1, only reference data[50], including a unique identification number, are uploaded to the Prüm database, without any information immediately identifying the data subject. Once inserted, the technical procedure followed to compare the data is highly scientific. The data retained in the Prüm database is sent to the "Request and Response" database of the requested country for verification of a potential "match". For the purpose of techno-scientific harmonization, signatory Member States are required to observe common technical specifications[51] in connection with all requests and answers related to searches and comparisons of DNA profiles and dactyloscopic data. Specifically, Council Decision 2008/616/JHA lays down a minimum set of requirements regarding data format. A request for a search or comparison shall include the following information: the code of the requesting Member State; the date, time and indication number of the request; DNA profiles and their reference numbers; and the types of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles). The answer to the request (i.e. "matching report") shall contain: an indication as to whether there were one or more matches ("hits") or no matches ("no hits"); the date, time and indication number of the request and of the answer; the codes and reference numbers of the requesting and requested Member States; the type of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles); and lastly, the requested and matching DNA profiles.

The comparison of a particular DNA trace against the Prüm database relies on the examination of the loci[52] of the submitted sample to find the highest comparability possible. Butler (2006: 235) defines loci as "a single currency in a financial sense" that permits the cross-border comparison of genetic traces at the EU level. A DNA profile[53] sent out for comparison or made available to the other Member States for searching must contain at least six of the seven designated loci[54]. According to forensics experts, given that the probability of a true match is

[50] The DNA reference data are composed of a DNA profile and the non-DNA specific data. They shall only include DNA profiles established from the non-coding part of DNA and must not contain any data from which the data subject can be directly identified.
[51] These technical specifications are laid down in the Annex to the Council Decision 2008/616/JHA.
[52] The "locus" is a specific, fixed position on a chromosome where a particular gene or genetic marker is located.
[53] In general, a DNA profile contains 24 pairs of numbers representing the alleles of 24 loci which are also used in the DNA matching procedures of Interpol.
[54] According to Article 7 of Council Decision 2008/616/JHA, Member States shall use existing standards for DNA data exchange, such as the European Standard Set (ESS) or the Interpol Standard Set of Loci (ISSOL).

only 40% with six loci, a DNA profile may contain all the available alleles in order to raise the accuracy of matches (Toom et al. 2019). For a "full match" all values of the compared loci must correspond. If only one value is different, the "hit" is classified as a "near match". This result is accepted only if there are at least six full matched loci in the two compared DNA profiles. In this case, notification of a positive "hit" is provided to the requesting country through the common communication network called "TESTA"[55]. The TESTA network is a form of virtual tunnelling system that is used to directly send requests and to receive replies among the Member States. Access to TESTA occurs either through individual national access points located at different sites or by setting up a direct link from the data centre of a Member State.

In general, requests for DNA data are processed within 15 minutes, for dactyloscopic data within 24 hours and for vehicle registration data in 10 seconds, by a fully automated procedure. In the first case, the exchange requires the installation of the Combined DNA Index System ("CODIS") (Santos and Machado 2017), a software produced and sold by the USA Federal Bureau of Investigation that "blends forensic science and computer technology into an effective tool for solving crime."[56] Whereas for the comparison of dactyloscopic data, Member States must install the Automated Fingerprint Identification Systems (AFIS) – discussed also in Chapter 3 in relation to the updated functionalities of SIS II. Lastly, information related to VRD are exchanged through national platforms by means of established search criteria. The items declared as necessary for the refinement of the search are the licence plate, vehicle identification number (VIN), country of registration, commercial type of the vehicle, and EU category code. The national platforms are linked to the online application EUCARIS. Similarly to TESTA, the EUCARIS application connects all participating Member States in a mesh network where each Member State communicates directly to another Member State.

4.3.3. Local discords

In the case of DNA and dactyloscopic data, the comparison that results in a binary "hit"/"no-hit" response (Costa 2020) is then reported back to the requesting country. This means that for every profile submitted for verification a result should be available. However, only in the case of a positive "hit" the cross-border exchange proceeds to Step 2. If it reaches this stage, the

[55] Trans European Services for Telematics between Administrations.
[56] Further information available at: https://www.promega.es/-/media/files/resources/profiles-in-dna/103/codis-program-overview.pdf?la=en

requesting country has the opportunity to access more precise information such as personal data relating to the matching DNA profile or fingerprint data. Technically, therefore, the consultation launched by the requesting country gives way to a response revealing the identification of the person to which the matching data belongs to. Under these circumstances, Decision 2008/615/JHA does not stipulate harmonized rules with regard to the purpose and means by which information should be requested and exchanged. Neither does it specify what kind of personal data can be provided. Compared to the high degree of harmonisation of Step 1, the second step of the exchange process is governed by national legislation, with discretion for a country to decide the procedures for the follow-up request. In general, the request for further information is placed through mutual assistance procedures (MAP) or mutual legal assistance (MLA) requests. When a Member State receives a report of a "hit", the established National Contact Points (NCPs) are responsible for validating and checking the evidential value of the matching profile.[57]

At this stage, matches reported to criminal investigative authorities are subject to further selection, evaluation and prioritization, resulting in higher drop-out rates compared to Step 1. Potential drop-outs occur when the assessment criteria of a "hit" are not aligned due to the diverging rationales of the various national police agencies and prosecutors in relation to crime control (e.g. priority of a case). For instance, matches between a known individual abroad and DNA profiles from domestic unsolved crimes may be prioritized over a national reference profile that matches a DNA profile of an unsolved crime in another country. Similarly, matches potentially linking a suspect to a severe crime like rape and murder may be considered more important than petty or high-volume crimes. Given the lack of a uniform procedure to follow up a match, different practices emerge when submitting or responding to mutual legal assistance procedures (Machado and Granja 2019). Consequently, only a percentage of the hits generated in Step 1 may be followed up and ultimately be used as evidence in a court of law. These inconsistencies contribute to the lack of equality in the level of speed and in the amount of information exchanged through the Prüm network (Toom et al. 2019).

Among the persistent problems found, inherent differences in the national organization of criminal investigations and forensic data seem to have the greatest impact on cross-border exchange. As stated by Johnson et al. (2016: 28), '[i]n Requested Country, DNA-based information might be judicial evidence and must achieve higher standard of validity (hence the

[57] For validation purposes, national contact points can contact each other directly.

stricter reporting rule), whereas in Requesting Country, DNA-based information might be law-enforcement investigative evidence and is exploited differently than in Requested Country'. Additionally, technical differences in terms of formats, messaging standards and message exchange technologies can further hamper the techno-scientific harmonisation of Step 2. Hence, the cross-border exchange of information has as its main challenge the legislative diversity of the signatory Member States. These divergences show that European countries have different techno-scientific imaginaries about the personal information that should be exchanged cross-border, and also have different conceptions of the notions of privacy and data protection (Matos 2019).

As a result, from the automated exchange of forensic data in Step 1 to the forensic re-analysis in Step 2, the process of cross-border police cooperation is not evenly harmonised. During the first stage, DNA data and fingerprints are compared in "bulk" in conformity with the multilateral regulations of the Prüm Decisions. After notification of a positive hit, the investigation shifts to the bilateral level, pursuant to the existing national legal and organisational regulations of the respective Member States. The recurrence to traditional channels of mutual legal assistance, prescribed by the so-called "Swedish Initiative", inherently breaks with the "transnational impetus" for replacing the lengthy bureaucratic bilateral procedures through the setup of Prüm. Essentially, if the ultimate goal of the Prüm network is to materialize the EU "techno-scientific" imaginary of the free flow of data by neutralising legal, cultural and organisational differences (Prainsack and Toom 2010, 2013; Matos 2019), the infrastructures in place are fraughted with the "techno-scientific" reality of each operational Member State. Similarly to the "principle of ownership" in the SIS II, the Prüm signatories retain the ownership of their profile data and control its submission, access by other countries and destruction in accordance with their national laws. Only Step 1 projects the local forensic information to the transnational stage. Whereas Step 2 inevitably affects the prospect of a highly harmonized cross-border data transfer.

4.4. Visualising the Prüm network

The interconnections that make up the Prüm network are much more difficult to plot given the complex technical and organisational aspects of its configuration. However, the reliance on visual network analysis has rendered the arrangements of its constituent parts more intelligible.

In order to visually reproduce the topology of Prüm I recurred once again to the Gephi software. In terms of methodology, I followed a similar procedure to the one described for SIS II in Chapter 3. However, rather than starting by indexing the data in Excel, I inserted it manually in the blank tables provided on Gephi. The first column of each table listed the actors, and the second column listed the relations between the actors. Based on the contextual information inserted, such as the number of actors belonging to a category or the type of relation between them, Gephi spatialized the relational distribution of the various components in a graph. Given that the Prüm framework provides for the exchange of three types of data, that is DNA, fingerprint and VRD data, I spatialized them individually. This operation resulted in the creation of three distinct visualisations, each displaying the central features of the operational exchange of that type of data. To simplify the work I have included only the countries that were listed as "fully operational"[58] in the Annexes (see Annexes I, II and II)[59] to the latest report of October 2021 on the Prüm "State of Play" [60] (Council of the European Union 2021b).

Then, I labelled each node indexed in Gephi through an acronym. The nodes corresponding to the national databases for the exchange of fingerprints and VRD data appear simply as "N DB"; whereas those corresponding to the national DNA databases as "N DNA DB"; the nodes related to the Prüm interfaces figure as "Prüm"; and lastly those corresponding to the Request and Response databases as "R&R Database". Each label is followed by the ISO country code of the Member State to which it refers to (e.g., N DNA DB LT – for Latvia; Prüm AT – for Austria; R&R Database HU for Hungary, etc.). After labelling them, I have arbitrarily assigned a colour to each node category: light blue for "N DB" and "N DNA DB", yellow for "Prüm" and orange for "R&R Database". This procedure ensures that each constituent part of the network is differentiated from the others, and additionally it permits to quickly grasp the trajectories that data follow from one actor to another. Like in the resulting graphs of the SIS II (Chapter 3), the size of each node is determined by the number of connections that cross it. The smallest nodes are the national databases ("N DNA DB" and "N DB") since they provide only for one connection (edge) – from their server to the server of the Prüm database of their

[58] I have excluded for example Italy, Greece, Norway and the United Kingdom from the network of exchange of VRD data since they are either in the production/testing phase or there is no report on their status of implementation, such as in the case of the UK.
[59] The Annexes reflect the current state of implementation for each type of data exchanged through the Prüm framework. Annexes I and II list as operational 26 Member States in the exchange of DNA and fingerprints. Annex III lists as operational 25 Member States in the exchange of VRD data.
[60] The state of play does not provide information about Schengen Associated States (Iceland, Norway, Switzerland and Liechtenstein). Limited information on Norway, which is not operational yet.

country. Whereas the Prüm databases are connected also to the R&R databases of the other countries (depending on the number of national connections established). The nodes of both "Prüm" and "R&R databases" are thus automatically bigger.

The journey of the data exchanged through the Prüm network starts from the national database of an operational country, labelled as National DNA database ("N-DNA-DB") (for the exchange of DNA data), or simply as National Database ("N DB") (for the exchange of fingerprints and VRD data). Here the profiles that meet the Prüm inclusion rules are copied from the national database to the Prüm database ("Prüm") of that same country. The Prüm database can either contain a physical copy or a view of the national database. This first step creates a (directed) edge between the two databases of each country. Then, once inserted into the (national) Prüm database, the data (DNA or fingerprints) can be sent to other countries for comparison. Note that a country can decide to verify the data for a match by sending it to one or more selected countries, or to all operational countries to which it is connected. This form of exchange is done by relying on the secure European network called TESTA. As explained, TESTA functions as a communication tool that encrypts the data before sending it to the server of the country of destination. Once the encrypted data arrives at the server of the selected country, the communication tool transfers it in the corresponding Request and Response database ("R&R Database).

Depending on the number of connections established, this second step creates a further edge, between the Prüm database of the requesting country and the R&R database(s) of the receiving country(ies). In order to then compare the data received, the matching tool of the receiving country picks up the data from the Request and Response database and compares it with the national Prüm database. The result of the comparison is then reported back in the Request and Response database, where it can be viewed via the Graphical Use Interface[61]. Once compared, the data travels back to the requesting country via the secure European TESTA network. By travelling backwards the data crosses the same edges, but in the opposite direction. This process results in a number of overlapping edges that cannot be directly visualised in the visualisations of the Prüm network. Yet tracing the flow of each type of data was essential to determine the specific trajectories that data follow from one database to another. Although there are not

[61] Note that the results of a comparison can be viewed by both the requesting and requested country.

substantial differences in the visual features of the visualisations, I decided to include all three in order to focus the attention on the high number of resulting edges (Figures 9, 10 and 11).

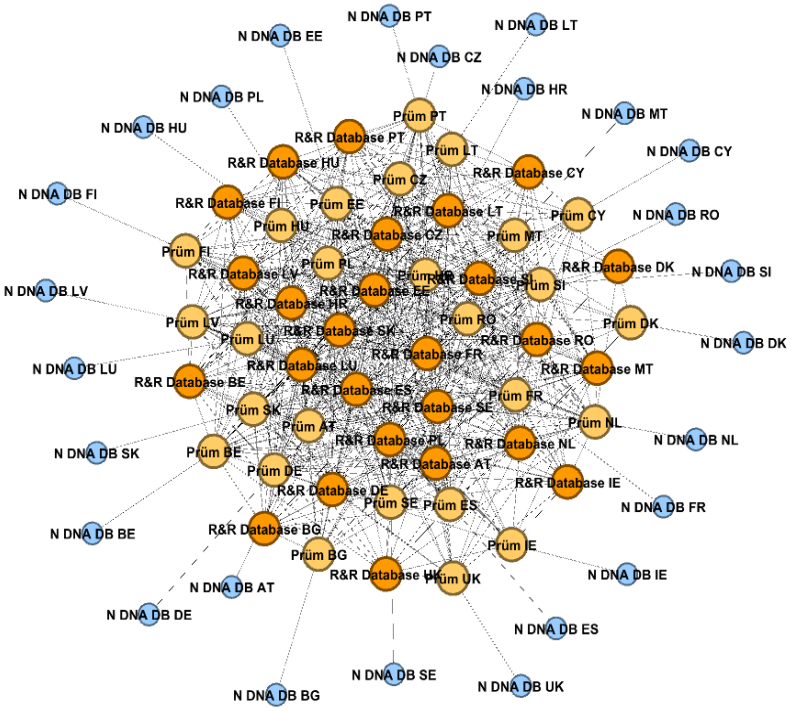

Figure 9. Force-directed layout of DNA data exchange (Force Atlas 2).

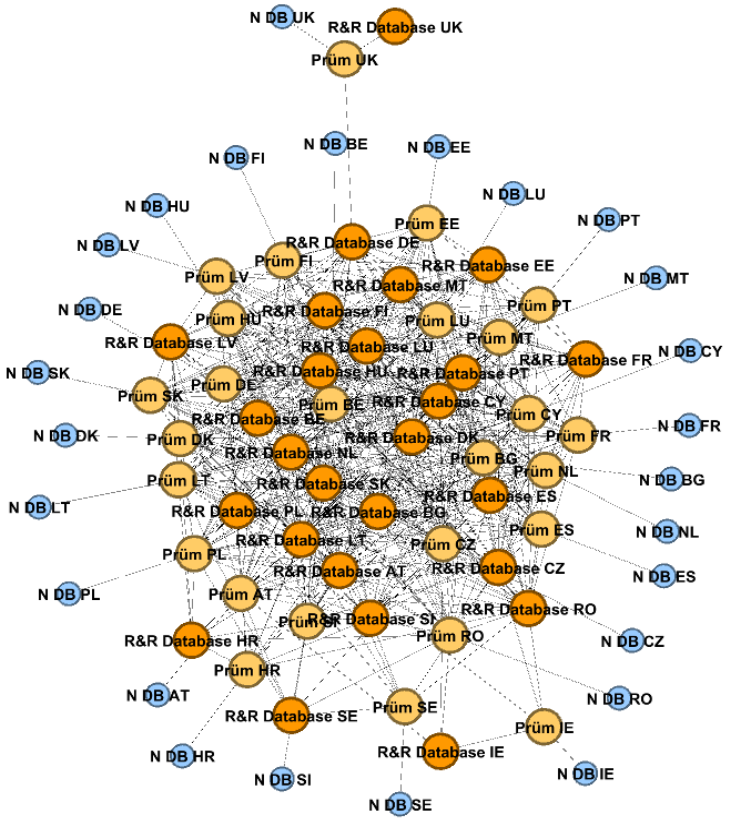

Figure 10. Force-directed layout of dactyloscopic data exchange (Force Atlas 2).

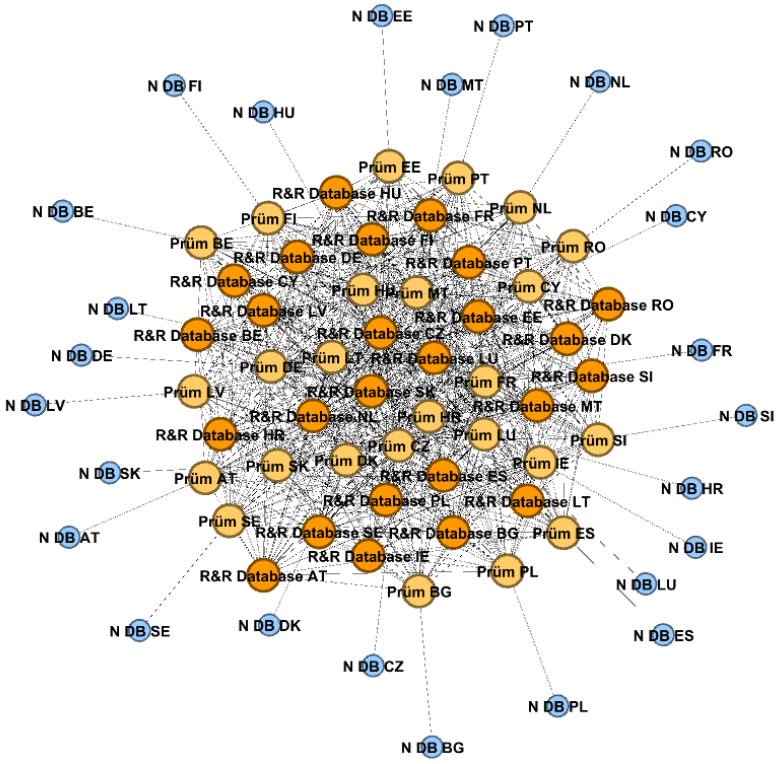

Figure 11. Force-directed layout of VRD data exchange (Force Atlas 2).

This visual characteristic reflects the configuration of the Prüm as a decentralised network of national databases. The high number of edges is indeed the direct result of this configuration. . In order to provide a model of exchange, I took the case of Belgium (BE). For the exchange of DNA data, Belgium has established 23 out of 26 possible connections[62] with the other operational Member States (Figure 12). Santos (2017: 316) considers that "[t]he factors that may influence the decision to connect two countries can be associated to the perceived relevance in terms of cross-border crime, but also to simple matters of convenience, interpersonal relations between NCPs and political decisions." In order for one Member State to be able to undertake exchanges directly with every other operational Member State, 26 bilateral interfaces would be required in the case of DNA and dactyloscopic data and 25 in the case of VRD data. This ideal configuration would currently equate to over 700 interfaces across the EU. However, as reported in the 2021 State of Play, the Prüm framework has not yet reached its full potential regarding the possible number of connected databases (Council of the European Union 2021b). This depends on the fact that not every operational Member State have established the same number of connections. Some exchange data with over 20 Member States, others with only four or five.

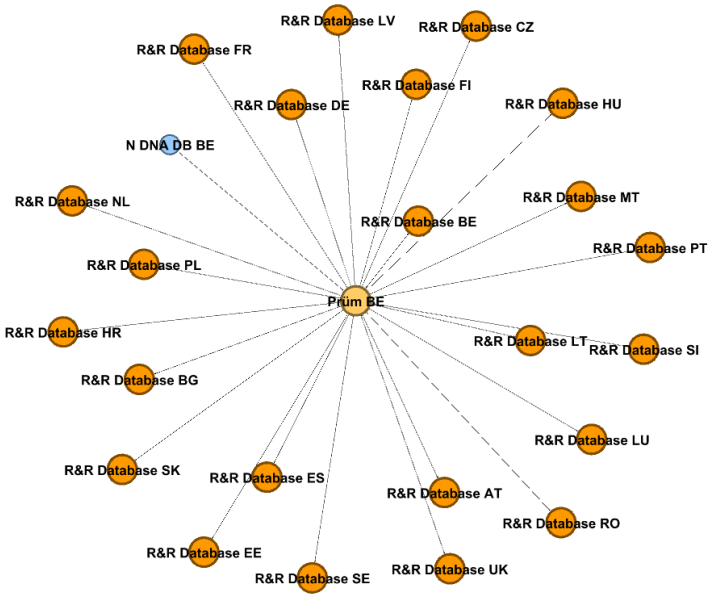

Figure 12. Force-directed layout of DNA exchange (Belgium).

In total the connections established (by category of data) resulted in 617 edges for DNA data, 562 for dactyloscopic data and 562 for VRD data. Obviously, in the visualisations it is almost

[62] It does not exchange DNA data with Denmark, Ireland and Cyprus.

impossible to spot the differences in the numbers. However, every graph appear highly crowded in the centre where most of the exchanges between the Prüm databases and the R&R databases are concentrated (Figure 9, 10 and 11). As expected, given that the national databases are connected exclusively with the Prüm database of their country, the limited number of connections resulted in the disposition of the corresponding nodes in the outer circular frame. Furthermore, although each Member State has established a different number of connections, the gap is not too big. For example, Germany and the Czech Republic are operational with 23 countries in the exchange of DNA data; France, Hungary and Romania with 24, Latvia and Croatia with 22. Accordingly, due to these similarities most of the nodes related to the Prüm and R&R databases are located in the inner circular frame. The only difference regards the second visualisation (Figure 10), that represents the operational exchange of dactyloscopic data. It is not surprising that the UK is left out from the central spatialization of the network. According to Annex II, the UK is operational only with Germany. This huge gap vis-à-vis the number of connections established by the other countries resulted in its exclusion from the core of the relational distribution of dactyloscopic data exchange.

Another visual feature that stands out regards the spatialization of VRD data exchanges. In order to better visualise the central feature of this network I have created another visualisation by running Yifan Hu. Yifan Hu is a multilevel algorithm that reduces network complexity by balancing the forces of repulsion and attraction in the connections between nodes (Hu 2005). As shown in Figure 13, the disposition of the nodes is ordered in a circular fashion, with the national databases occupying the outer circle, the Prüm databases the intermediate one, and lastly, the R&R databases the inner one. The proportionality in their disposition is the result of the equivalent number of connections established. All Member States are in fact equally operational, meaning that they exchange VRD data with all the other Member States in the Prüm network. In general, the visual characteristics of Figures 9 to 11 are an indicator of the asynchronous implementation of the Prüm framework in the EU. Some countries have been more proactive in establishing connections and have thus succeeded in starting exchanges with a higher number of countries (Santos and Machado 2017).

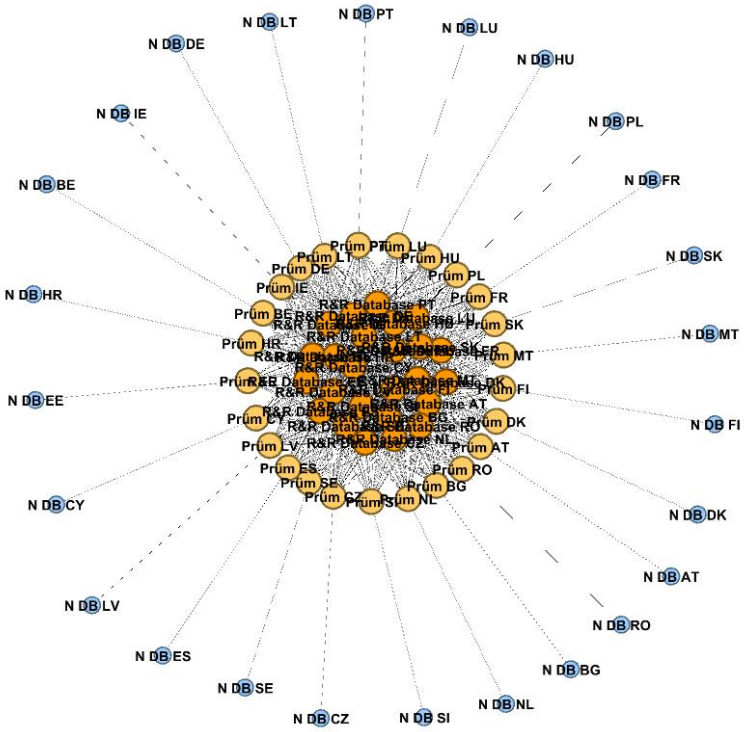

Figure 13. Force-directed layout of VRD data exchange (Yifan Hu).

In this regard, the main highlight is the development of a core group of countries sharing a high volume of data between them (Santos and Machado 2017), contrasting with a small southern peripheral group who is left out from the central relational disposition of the Prüm network. The overview of the 2021 state of implementation confirms that most of the volume of exchanges occurs in West and Central European countries that have taken leading roles in the implementation of Prüm (Council of the European Union 2021b). Consistently, the top countries for the volume of DNA data exchanges include the Netherlands (25); Austria, France, Poland and Romania (24); Germany and Slovakia (23); Belgium and Luxembourg (22). These figures validate the claim about the rapid implementation of Prüm in the Northern and Eastern European countries vis-à-vis the slower development in the Southern European countries (Santos and Machado 2017), such as Greece, and Italy, which are still in the piloting phase but are not operational yet; as well as Portugal, Malta and Cyprus, which have established a relatively small number of connections in all three categories of data. This group is currently having very little impact on the transnational exchange of data through the Prüm network. As a result, the asymmetries in the observed fluxes of data can potentially generate hierarchisation and fragmentation in the operation of Prüm (Balzacq and Hadfield 2012; Santos and Machado 2017: 311).

Conclusion

Because of the confluence of science and technology, the political interest in setting up the Prüm required an investment of a quite different order compared to the Schengen Information System (McCartney et al. 2011). In order to illuminate the uniqueness of Prüm vis-à-vis the SIS as well as the other AFSJ systems considered, this chapter has sought to analyse its implementation in relation to larger debates about the use of forensic genetic technologies as means for identifying individuals. By unearthing the specificities of the Prüm framework, I managed to reconstruct the scientific and technological trajectories followed in the co-construction of a highly decentralized architecture of multilateral exchanges of forensic information at the EU level. In the Prüm, the EU "techno-scientific" imaginary related to the belief in the infallibility of forensic science has found direct application as a strategy to solve crimes not only at the national level but also at the transnational one (see Amankwaa 2020; Butler 2006; Machado and Granja 2019; McCartney et al. 2011). What indeed emerged from the empirical analysis is that the Prüm initiative resulted from the projection of criminal concerns from the "local" level to the new "transnational" reality caused by the demise of the EU internal borders and in turn by the increased mobility of persons in the wake of the Schengen Agreement (Matos 2019).

In line with the politics of emergency that shaped the evolution of the SIS, the origin and development of the Prüm framework endorsed the view that terrorism, cross-border crime and irregular migration were the central threats to EU security (McCartney et al. 2011). Assuming that the threats faced by Member States were objective constituted an effective political shortcut for advancing transnational visions of desirable futures driven by science and technology (Prainsack and Toom 2010, 2013). In particular, the setup of Prüm was framed by the increasing importance of forensic DNA databases for criminal investigations and the ascendance of DNA profiling (Santos 2016). As a result, the "quest of visibility" through unique biometric identifiers, such as DNA and dactyloscopic data, effectively became the distinguishing trademark of the Prüm. In a quite peculiar way compared to the SIS, the Prüm was developed as a security infrastructure of cross-border information exchange, that projects the "body" (Maguire et al. 2018) – and, even more singularly, genetic identifiers (Machado and Granja 2020) – as the object of security. However, while the Prüm aspired to become an efficient scheme for cross-border information exchange, this aspiration has been constantly curtailed by technical and scientific issues as well as legal and ethical concerns.

The harmonisation and standardisation of the automated operations under Step 1 served the objective of overcoming the great heterogeneity of the legal regimes that regulate forensic and police practices at the national level (Costa 2020). As shown, Step 1 effectively diluted these barriers by allowing Member States to directly access the depersonalised sub-sets of national criminal DNA and fingerprint databases of all connected Member States for search and comparison. Nevertheless, these differences inevitably reappeared during Step 2 (Matos 2019), due to the existence of highly heterogeneous practices in the conduct of bilateral exchanges of information through National Contact Points (NCPs). Accordingly, far from the prescriptions of the principle of availability, the findings demonstrate that data remain the property of the state under the Prüm Decisions, 'not constitutive of a common Area of Freedom, Security and Justice' (Balzacq and Hadfield 2012: 554). The failure to align Prüm with the principle of availability has been commented by some scholars as creating a hierarchy within the EU (Balzacq et al. 2006) through a "border" between those Member States cooperating via Prüm and those yet to implement the Prüm infrastructures (Balzacq et al. 2006; McCartney et al. 2011).

The unfolding of the two-step procedure further highlighted that while the "hit"/"no hit" response (Step 1) is provided within seconds or minutes (depending on the data category), it may take weeks or even months to receive a response to the follow-up request via mutual assistance requests (Step 2). This further confirms that the Prüm network is yet to materialize the "techno-scientific" imaginary related to the efficient and fast free flow of data. Rather than an actual medium for the exchange of information then, the Prüm provides an index that can be queried through the "hit"/"no hit" procedure in the search for the existence of the desired information. The transformation of the Prüm into a criminal database has simultaneously transformed bodies as "sites" of security decisions. Omanovic warns about the danger of transforming the Prüm into a pan-European face database used for politically motivated surveillance instead of standard police work (Campbell and Jones 2020; see also Jakubowska and Naranjo 2020). This idea is reinforced by the fact that the Prüm instruments for information exchange were developed outside the democratic accountability of the EU Parliament and the oversight of the Court of Justice, and were thus mainly driven by law enforcement needs.

The possibility to project identity from individual data fragments, such as DNA genetic information through the Prüm, is promoting a politics of population control (see also Amoore 2013; Bigo and Carrera 2004; Bunyan 2010; Jeandesboz 2010; Kierkegaard 2008). Especially,

the techno-scientific standardisation element introduced with the Prüm that was intended to facilitate transnational cooperation between police and judicial institutions, eventually produced a surveillance mechanism that allows for the projection of old forms of suspicion (Costa 2020; see also Lyon 2003; 2016; Murakami 2007; Van Dijck 2014). Accordingly, through the confluence of biology and technology, the EU managed to forge a powerful instrument not simply for exchanging data cross-border, but, crucially, for redistributing power from criminal investigators to forensic technocracies (Prainsack and Toom 2010). However, techno-scientific politics is problematic because this mode of governing is increasingly concerned with the individual, and specifically with "suspect bodies" that have become the core of highly intrusive policymaking provisions under Prüm. At the same time, this mode of governing increases concerns about the legitimacy and acceptability of the rise of the EU as a policing state (Bunyan 2010).

Chapter 5

Towards EU Multi-Purpose Information Systems:

Advance Passenger Information (API) and Passenger Name Record (PNR) Systems

Introduction

After the analysis of SIS (I and II) and the Prüm framework, this empirical chapter focuses on the provisions that regulate the collection, processing, and use of identity and travel data from air passengers in the form of Advance Passenger Information (API) and Passenger Name Record (PNR). API data are basic biographic information about passengers and crewmembers. This information is usually retrievable from the machine-readable zone of travel documents (i.e. passports) and includes elements such as the name, date of birth, gender, citizenship, as well as elements related to the travel document (e.g., passport number, etc.). Unlike PNR, API data are not required for air carriers' commercial and operational purposes and are therefore collected only for governmental ends. Such legal requirement has been established by Council Directive 2004/82/EC, also known as the "API Directive" (OJEU 2004), and is valid for air carriers operating flights to EU Member States from a third country and vice versa. By contrast to API, Passenger Name Records (PNRs) contain a wide array of information about air passengers, ranging from their names, addresses, the means of payment for the flight, or any travel-related preferences, such as wheel-chair requests. This information is generated by passengers, travel agencies, or air carriers at the moment of booking, checking-in, or boarding a flight.

Essentially, PNR is an umbrella term that encompasses information about the whole itinerary of passengers,[63] far beyond basic identity attributes or travel document information, such as in the case of API. The collection of PNR data is set to work for law enforcement purposes through the implementation of Council Directive 2016/681 ("PNR Directive") (OJEU 2016c). At its inception, the PNR Directive was conceived as an emergency policy following 9/11 that has later been toned down to a proportionality assessment and eventually has been normalised in the EU. In contrast to the API Directive which mandates the collection of API data mainly for identity verification, the collection of PNR data is directed at targeting traveller behaviour. The combination of API and PNR has become paramount not only to the airline industry and border community, but also to states who seek to identify travellers "of interest" and perform targeted risk assessment along the traveller journey. By vetting all available passenger-related data prior to boarding, governments aim to prevent the cross-border movement of individuals who might represent a threat to aviation and internal security.

The aim of this chapter is to uncover how commercial datasets created by airlines are turned into sources of security knowledge and are then mobilised for a wide range of law enforcement purposes, including for counter-terrorism and the investigation, detection and prevention of serious crimes. Yet rather than discussing Advance Passenger Information (API) systems and Passenger Name Record (PNR) systems separately, in what follows, I provide a joint analysis that covers all aspects related to the lifecycle of "passenger data" (as one category of data), including the collection, transfer and processing of API and PNR, as well as their employment by law enforcement authorities. The added value of analysing them jointly is the possibility to juxtapose their legislative frameworks and technical setups, to acknowledge potential asymmetries in the modes API and PNR are generated and then transferred – following different protocols and organisational procedures, and again, to understand how these similarities/differences impact on the lifecycle of passenger data at large. The presence of the comparative element provides an empirical contribution to previous work that have sought to address how these systems – as well as other implemented in the AFSJ – reconfigure the power of states to govern international mobility and the threats (i.e. terrorism, serious crimes)

[63] Including hotel and car reservations (if booked with the flights), contact information such as addresses, email- and IP-addresses, phone and mobile phone numbers; payment information (credit card details), dietary information, information on disabilities, etc. Note that this information may vary between PNR systems implemented in the EU/US, as well as between countries within the EU.

associated with it (see Bellanova and Duez 2012; Bigo 2014; Broeders and Dijstelbloem 2016; Glouftsios 2018; Glouftsios and Leese 2023; Hall 2017; Mitsilegas 2007).

Questions about the (disproportionate) uses to which API and PNR data could be put take place against the wider shift towards preventive, intelligence-led law enforcement. In particular, I consider three distinct stages – data collection, transmission and processing – in order to understand how the generation and use of passenger data vary in the level of targeting: from the "indiscriminate" gathering stage to the "targeted" practice of mining data in the assessment of the risk level of travellers. Being less about the size of the "haystack" (Aradau and Blanke 2015; Logan 2017; Lyon 2014) – that is, the universe of data collected – the nature of the tension points to a differentiation in the degree of discrimination behind the quantity of data sought. Especially, the term "bulk", which stands for the whole universe of records (Gellman and Soltani 2013), is in sharp contrast with the narrower algorithmic querying process which promises the detection of the so-called "needle" among the "haystack" of data (Aradau and Blanke 2015: 6; Kris 2014; Logan 2017). Accordingly, as the performance of bulk collection programmes – like API and PNR – shifts from the indiscriminate gathering stage to the targeted practice of data mining, a trade-off emerges. For instance, personal data collected to ascertain the identity of travellers at borders can contribute to draw up typologies of "risky" individuals through profiling techniques, and to assess the behavioural patterns even of those individuals devoid of any suspicion (see Aradau and Blanke 2017a).

This chapter is organised as follows. The first section describes the context in which passenger-related information is collected by the travel industry for identity management purposes. It focuses specifically on the identity verification approach that characterises the processes behind passenger authentication. The second section provides the framework for evaluating the API and PNR Directives by presenting the policies that regulate the collection of passengers information at both the international and European level. Here I focus on the differences between API and PNR, especially in terms of scope of the data elements sought. The third section outlines the distinct stages and modes by which API and PNR data are first transferred and then processed according to the purposes set out in the respective Directives. Lastly, I proceed to uncover the underlying technical processes by which the set of inputs (i.e. passenger data) are transformed into pre-determined outputs ("risky" travellers) for law enforcement authorities. In order to emphasise the relationality between data inputs and resulting outputs, in this section I report the findings from the visual network analysis of both API and PNR.

Lastly, I weave the thread of the analysis by discussing how passenger data contribute to encoding security-related decisions as part of the wider demands for suspicion-less mass collection-, retention- and analyses of data.

5.1. Passenger information landscape

The API and PNR systems are embedded within a broader political context characterised by discourses that frame mobility as an inherently threatening phenomenon (e.g., Broeders and Dijstelbloem 2016; Dijstelbloem and Broeders 2015; Leese and Wittendorp 2017). These discourses are often put forward by EU institutions and the industry in order to justify investments in hi-tech projects. Since the routine examination of passengers and their possessions is no longer considered a suitable instrument to enforce security, current techniques for passengers identification have shifted to a more selective approach based on risk assessment, intelligence analysis and behavioural patterns (see Amoore 2013; Kaufmann et al. 2019). The typical logic here is that for every security issue there is a technological 'solution' (see Bigo and Carrera 2004; Martins and Jumbert 2020; Singler 2021). Especially, the reason why API and PNR data are transferred from the private to the public sector is to grant national police authorities bulk access to identity data and travel itineraries. Establishing and verifying an identity to a high degree of confidence is nevertheless a complex task that requires to assess the risk behind each piece of available information (Amoore 2013; Aradau and Blanke 2017a; Aykut et al. 2019). This procedure has become the precondition for undertaking security-related decisions concerning an individual, such as granting or refusing access to a Member State.

The ICAO Traveller Identification Programme (ICAO TRIP) Strategy (ICAO 2013a) establishes a comprehensive framework for the identification of travellers that relies on the implementation of Advance Passenger Information (API) systems – (or, alternatively, interactive API (iAPI) systems in more technologically-advanced jurisdictions) – and Passenger Name Record (PNR) systems. These are not mere border control tools, but also law enforcement instruments. Traditionally, the physical inspection of the traveller and of the associated travel document were practices related to border security. However, a great bulk of the identity verification process which is relevant to law enforcement now relies on the secure transmission of electronic data obtained even before a journey starts. The preventive approach

behind the collection of passenger-related information has resulted in the increasing merge of border controls, homeland security and the airline industry (see Abrahamsen and Williams 2010). Even in the Schengen area where mobility is constantly promoted, border crossings can assume a negative connotation when they are illegitimate and can generate a potential risk for internal security (e.g. Balzacq and Hadfield 2012). Hence, identity verification has become the first line of defence against the cross-border movement of terrorists and of illicit goods (see Amoore 2008).

The assessment of data beforehand is of critical concern, especially to border control authorities (BCAs) that need to know early and reliably who is coming to the border. BCAs are better placed to mitigate the risk that terrorism and organized crime (domestic or transnational) disperse into national territories since they are front line in managing the circulation. Traveller identification programmes (ICAO 2013a, 2016), such as API and PNR, serve this purpose, by principally permitting to verify identities and assess risks. As stated in the ICAO TRIP Magazine (2016: 23), to establish an identity 'the first and fundamental requirement involves identity proofing and verification to assess the level of certainty that a person asserting an identity is in fact that person'. In this context, passenger data contribute to integrated border management by enabling a risk-based, data-driven approach to security. By exchanging API and PNR data in advance, customs and border authorities aim to carry out secure checks and identify suspect passengers *ahead of* travelling. Specifically, their task is to balance the risk of irregular border crossings against the provision of efficient services to low-risk travellers. According to the ICAO TRIP Guide, the risk-based approach to traveller identification is built on four pillars: identity management in the border continuum; advance checks; individualised risk management; and facilitation services for legitimate travellers.

To validate and corroborate a person's claimed identity authorities rely on two types of evidence: core identity attributes (e.g. alphanumeric or biometric data) and secondary identity-related information. The former generally includes name(s), surname, date of birth, place of birth, nationality, or even fingerprints data. This type of information can be retrieved from national identification documents or machine-readable passports. Whereas secondary identity-related information, such as address, phone numbers and email address, are generally found in visa records, utilities, bank or tax records, health records, employment records or even on social media. The collection of these two types of evidence from passengers broadly occurs in two instances: when border guards verify passengers' identity (API) or when a new travel

reservation is made and/or amended (PNR). Accordingly, API and PNR data are used by public authorities for border control purposes and shared for law enforcement finalities. However, enforcement authorities do not exchange information linearly, because personal data are dislocated across agency records and airlines' reservation systems. Therefore, the exchange of passenger information creates an intricate system, which makes personal identification challenging.

Information is shared between a variety of public and private actors, including border guards, police and migration authorities, as well as the transportation industry that are joined up in an inter-agency, cross-border approach in the identification of "suspicious" or "wanted" persons. In the context of API and PNR systems the use of the word "identification" is yet ambiguous. The purpose of these systems is to indicate that there is a certain likelihood that the person thus identified *may* commit a crime or a terrorist offence in the future; or even more vaguely that that person *may be* "of interest" on grounds of suspicious patterns indicating the "potential" intent to commit a crime (Korff 2015). Here, the matter is not simply one of matching the details of a convicted or wanted criminal with the generalities provided by a traveller, as for instance in the case of the SIS II. The functioning of API and PNR systems imply quite different meanings of the words "identify" or "identification." In the case of the SIS, the aim is to match a certain person against existing records in order to find previously-identified individuals. In the case of API and PNR, the aim is to mine vast amounts of disparate data to create profiles and label people as "more or less likely" to be involved in terrorism or other forms of serious crime.

Yet, neither the API nor the PNR Directive are clear about the way in which the terms "identify" or "identification" are used. As a result of this semantic confusion, the danger is that information on airline passengers can be collected for a range of rather different purposes, traditionally associated with surveillance mechanisms (Korff 2015). As I will further discuss in consideration of the technical aspects of PNR systems, these now include "rule-based identification" of individuals through computerized means, in order to label them according to their risk level. Yet in the case of PNR systems, rule-based targeting is used not only to "identify" known terrorists or suspects in the traditional sense, but also to mine big data mountains to label *unknown* individuals as "suspected terrorist" on the basis of risk indicators and algorithms (e.g., Amoore and Raley 2017; Aradau and Blanke 2017b; Bellanova and De Goede 2020; Lahneman 2016). Rather than tackling the narrower legal and ethical concerns

about rule-based targeting in the context of API and PNR, in the section that follows, I look closely at the legal frameworks that have engaged the term "identification" in relation to the purposes for which API and PNR data are used.

5.2. Regulating traveller identification

The obligation for passengers and airlines to provide identity and travel data is regulated at both the international and European level by provisions for the collection, use and storage of such information, together with measures to protect their integrity and safeguard privacy. Early efforts to broaden the collection and sharing of API and PNR data globally have been advanced during the United Nations (UN) Security Council through the adoption of a number of Resolutions – Resolutions 2178/2014, 2309/2016, 2396/2017 and 2482/2019. Since their introduction, the UNSC (2014; 2016; 2017; 2019) Resolutions have driven a significant increase in the implementation of traveller identification programmes, like API and PNR. At the same time, they have developed processes and standards for sharing and transmitting personal data cross-border. Resolution 2178/2014 encourages UN Member States to employ an evidence-based traveller risk assessment and screening procedures for the collection and analysis of travel data. In particular, it requires that

> "Airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from […], or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee".
>
> (UNSC 2014: par 9).

Resolution 2309/2016 further emphasises the need for UN Member States to strengthen information-sharing, border control, law enforcement and criminal justice, in light of the more diffuse terrorist threat. One year later, Resolution 2396/2017 makes first mention of PNR systems by establishing a requirement that all States

> "Develop the capability to collect, process and analyse […] PNR data and to ensure that it is used by and shared with all their competent national authorities, with full

> respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses and related travel […]."
>
> (UNSC 2017: par 12).

This mandate resulted in the development of new standards and recommended practices at the international level. One of these provisions is the Organization for Security and Co-operation in Europe (OSCE) (2016) Decision No. 6/16 that commits OSCE participating States to establish national advance passenger information (API) systems in line with Annex 9 to the Chicago Convention (ICAO 2017b) and the WCO[64]/IATA[65]/ICAO[66] Guidelines on Advance Passenger Information (API) (2014).[67] More recently, Resolution 2482/2019 remarked the need to enhance the exchange of API and PNR data between public authorities and private sector airlines due to increasing linkages between terrorism and organized crime (UNSC 2019, par 15(c)).

At the European level, the collection and transmission of passengers data are governed by two legal instruments – Directive 2004/82/EC ("API Directive") (OJEU 2004) and Directive 2016/681 ("PNR Directive") (OJEU 2016c). Both Directives set out operational standards, procedures to follow for processing and analysing passengers data and for transferring them from air carriers operating on the European territory to the competent national security authorities of EU Member States. The following analysis focuses on the parameters that regulate the scope of data collection and that in turn determine the desired output of API and PNR systems – that is, to flag and recommend travellers or suspicious travel patterns for additional scrutiny. How data are generated and by whom, for which purposes, and how they are used in the law enforcement context are the questions at stake. In order to address these questions, three main aspects of the two Directives are considered: first, the categories of data collected; second, the modes by which they are transmitted to law enforcement authorities (i.e.

[64] World Customs Organization - http://www.wcoomd.org/en.aspx
[65] International Air Transport Association - https://www.iata.org/
[66] International Civil Aviation Organization - https://www.icao.int/Pages/default.aspx
[67] The API Guidelines were initially developed in 1993 by the WCO in cooperation with the International Air Transport Association (IATA). Subsequently, the International Civil Aviation Organization joined the process and a Contact Committee comprising the three organizations was formed. In order to help their respective members to implement API systems, the three organizations jointly published the WCO/IATA/ICAO Guidelines on Advance Passenger Information in 2003, as well as updated versions in the following years. Source: https://www.icao.int/Security/FAL/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards.aspx.

data formats and transmission protocols); third, the purposes for which API and PNR data are processed.

The API Directive regulates the collection and transmission of biographic data and flight details in all EU Member States[68] and Schengen associated countries (Norway, Iceland, Liechtenstein[69], Switzerland). It was introduced in 2004 (with the transposition deadline of 5th September 2006) in a period when Spain was dealing with high immigration flows from South America, for the purpose of combatting illegal migration and improving border controls. Only later, the scope of the Directive has been expanded to include under Article 6 the use of API also for "law enforcement purposes" (OJEU 2004: 26). Once implemented, the Directive imposed an obligation on air carriers to transmit advance passenger data to the border control authorities (BCAs) in the Member State of destination for flights inbound from a third country (i.e. extra-EU flights). By receiving data *prior to* the departure or arrival of the aircraft, BCAs can identify persons "known" to be a security risk (e.g. people included on national/international watchlists), and declare them to be "inadmissible" for boarding. According to the latest evaluation[70] of the API instrument (European Commission 2020d), almost all Member States that have since transposed the Directive in their national legislation collect API data with the aim of combating irregular migration and for improving border control. Out of 31 Member States, 21 collect it for law enforcement purposes, and 15 for the fight against terrorism.

Compared to the API Directive, the scope of the PNR Directive is much wider to encompass the collection of passenger data and itinerary information from all flights entering, leaving or travelling to/within the EU. In this respect, the Court of Justice of the European Union (CJEU 2017) acknowledged in Opinion 1/15 that such broad coverage is necessary since 'the exclusion of certain categories of persons, or areas of origin' (Ibid) would otherwise hinder the

[68] Including those Member States applying the Schengen acquis in full and those which did not yet – as of 2020 – apply the Schengen acquis in full, such as Bulgaria, Cyprus, Croatia and Romania. Denmark, by virtue of Protocol 22 to the Treaties, is allowed to decide whether or not it will participate (opt in) in measures proposed pursuant to Title V of Part Three TFEU, including the PNR Directive. Denmark notified the Commission of its willingness to participate in the implementation of the API Directive in 2006. Therefore, "implementing Member States" should be understood as referring to all EU Member States, including Denmark. The United Kingdom, as a Member State, was bound by the PNR Directive until 31 January 2020.

[69] Despite being a Schengen associated country, Liechtenstein does not feature among the "implementing countries" because it does not have an airport, and thus an API system in place.

[70] The Evaluation has been carried out 15 years after the adoption of the Directive in 2004, with the objective of providing an understanding of whether its provisions are still "fit-for-purpose". The Final Report assesses whether and how the API Directive still addresses the needs of border control and law enforcement authorities, airline carriers, passengers, and other stakeholders.

achievement of the Directive's intended objectives – that is, the prior identification of persons who may represent a risk to public security. PNR data must then be handed over from air carriers to the central authorities responsible for handling PNR data transfers, that is, the so-called Passenger Information Units ("PIUs"). The tasks of PIUs include cross-checking PNR data against relevant law enforcement databases; processing them against 'pre-determined criteria' in order to identify persons *potentially* involved in a terrorist offence or serious crime; and, disseminating PNR data to national competent authorities, Europol, and the PIUs of other EU countries, either spontaneously or in response to 'duly reasoned requests'(OJEU 2016c: 139). The PNR Directive does not impose an obligation on air carriers to collect and retain PNRs beyond the categories of data that they normally collect for their own commercial and operational purposes; nor does it force passengers to provide additional data beyond those already provided to air carriers.

The European Commission presented a first proposal for the introduction of PNR systems in November 2007 (see Article 29 Data Protection Working Party and Working Party on Police and Justice 2007). The proposed directive was negatively received by the EU Fundamental Rights Agency, the EU Standing Committee of Experts on International Immigration, Refugee and Criminal law (The Meijers Committee), the EU Article 29 Working Party on Data Protection, the European Data Protection Supervisor, academics and civil society groups. After the European Parliament refused to vote on the issue in November 2008, the Commission advanced a second proposal in February 2011 (European Commission 2011a), together with an impact assessment document (European Commission 2011b). The new proposal eventually became effective in 2016 with the adoption of the current EU PNR Directive (OJEU 2016c)[71]. The 2011 proposal is notable for the introduction of the concepts of 'risk assessment' and 'automated processing' for purposes of assessing the degree of risk presented by passengers. When comparing the 2011 and the 2007 proposals the Article 29 Working Party has expressed the opinion that:

> "The new proposal does not really narrow the scope of its application, nor does it provide extra safeguards. On the contrary, instead of limiting the goals for which member states may use PNR data, the current proposal extends the purpose of this instrument further."

[71] The current text of the PNR Directive has been effective since 24 May 2016 and had to become law in the Member States by 25 May 2018.

(Article 29 Working Party 2011, section 2).

The 2007 draft on the use of PNR data was limited to the purpose of "preventing and combating terrorist offences and organised crime" (see Article 29 Data Protection Working Party and Working Party on Police and Justice 2007). The 2011 proposal has considerably extended this scope to encompass "the prevention, detection, investigation and prosecution of terrorist offences and serious crime" (European Commission 2011a)[72]. Two main issues emerge from this framing. The first regards the wide range of purposes (-plural) covered by the text that has become binding under the 2016 PNR Directive. As the FRA and the EDPS have noted, the current framing provides for the dilution of the purpose limitation principle. Especially national authorities are left with a wide margin of discretion as to what constitutes a "serious crime" to be "prevented, detected, investigated and prosecuted." This loose definition can result in large differences in the crimes sought among the Member States that have implemented the PNR Directive. A similar issue emerges in relation to the broad framing of what constitutes "law enforcement" under the API Directive (OJEU 2004: 26). Although the re-use of API data in the law enforcement context appears as a secondary aspect, Article 6(1) does not exclude this possibility, leaving it at the discretion of Member States. As further stated, the national implementation of this purpose can range from enhancing internal security and public order, to the fight against terrorism (OJEU 2004)[73].

Under these circumstances, it becomes much more contentious to establish whether API and PNR constitute a tool for border control or counterterrorism. The PNR Directive is more straightforward in defining the threat that it seeks to counter, that is "preventing, detecting, investigating and prosecuting terrorist offences and serious crime" (OJEU 2016c: 137). In the text there are many other indicators that suggest that the PNR is used mainly as a counterterrorism instrument for preventive purposes, rather than as a tool for border control. For instance, border guards do not appear in the list of competent authorities having access to PNR data (Article 7) (OJEU 2016c). Whereas Article 6 of the API Directive imposes an obligation on air carriers to transmit API data directly to the authorities responsible for carrying out checks on persons at external borders (OJEU 2004). This requirement suggests that it is

[72] With the adoption of the PNR Directive in 2016, this scope was encompassed under Article 1(2) (OJEU 2016c).
[73] According to the 2020 Evaluation of the API Directive, a number of countries have made use of the possibility offered by Article 6(1)(5) to collect API data for law enforcement purposes. The evaluation lists Cyprus, Austria – where API data can be transmitted to another law enforcement authority in case of suspicion of a criminal offence – and Slovenia. The national transposition in the UK goes even beyond the scope of the API Directive by including law enforcement and intelligence as one of the ultimate goals (European Commission 2020d).

part of the narrative that the purpose of API is to improve border control, yet the latest developments in this field seem to tell a different story. In December 2022 the Commission tabled two proposals for two new Regulations, covering the use of API data for enhancing and facilitating external border controls (European Commission 2022a) and for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (European Commission 2022b). Although at this stage they are not binding, future advancements may create further uncertainty for both data subjects and national authorities with regard to the specific purposes and contexts (i.e. border controls or law enforcement) for which API and PNR data can be used, especially when API are collected as part of PNR data.

A second issue closely related to the future evolution of the API Directive and, more crucially, to the current framing of the PNR Directive emerges. This issue regards the increased police powers derived from the possibility to *prevent* terrorism and other forms of serious crimes. The idea that the police possesses intrusive powers to prevent a criminal act not yet committed, is particularly problematic (see Aradau and Blanke 2017a; Egbert and Leese 2020; Kaufmann 2019; Kaufmann et al. 2019). This is because the very concept of "predictive policing" – that has reversed the temporality by which evidence about a criminal activity is sought after (McCulloch and Pickering 2009) – is inherently incompatible with the basic principles of a democratic society. The acquisition of information in 'bulk', such as in the case of API and PNR, has created a bureaucratic incentive to 'over-collect' the data (Donohue 2014; Forsyth 2015; Lyon 2016) in order to deal with people who have not (yet) committed any wrongdoing, but who are "predicted" to "potentially" commit a crime or terrorist act. Nevertheless, problematizing the size of the haystack of data is actually misleading. The preference for the terminology "bulk collection" as opposed to the uneasiness which "mass surveillance" generates is an attempt to subsume the indiscriminate and untargeted acquisition of data "en masse" under the more targeted and discriminatory practice that the search for the "needle" among the ocean of data intimates (Aradau and Blanke 2015; Donohue 2014; Logan 2017).

Essentially, the attempt to identify possible future perpetrators of crimes, even before any concrete act is carried out, postulates the "bulk" collection of PNR data as a necessary stage to achieve a distinction between *who is* and *who is not* a terrorist/criminal. At this initial stage no discrimination occurs, given the impossibility to establish a discriminant between the categories of "legitimate" and "illegitimate" suspects before processing the data. Accordingly, the haystack created through the collection of data "en masse" conflates potential, would-be

terrorists, along with categories of the innocent and the guilty. The manifestation of this preventive rationale in the collection of PNR data reveals a reversal of suspicion in the approach by which data are sought after by the police. By consequence, the shift from chasing and reporting crimes 'post-facto', to anticipating the materialisation of a criminal act has inherently eroded the principle of presumption of innocence (McCulloch and Pickering 2009). Under the rule of law it cannot be acceptable that the police are granted increased powers to target people devoid of any suspicion. Yet such "predictive", "preventive" action is increasingly promoted through bulk collection programmes like the PNR, as not just legitimate but somehow necessary.

5.2.1. Scope of data collection

Article 3(2) of the API Directive provides for the collection of two categories of data: flight data and passenger data. The first category ("header" data) includes information relating to the flight, such as the code of transport, departure and arrival dates/time, total number of passengers carried and initial point of embarkation. The second category of data ("item/footer" data) generally includes biographic information relating to each passenger, namely, surname, given name(s), nationality, date of birth, place of birth, gender, type of travel document, travel document number, name of issuing state/organisation, expiration date of the travel document. Passenger data, that largely correspond to this second category of items,[74] are retrievable from the Machine Readable Zone (MRZ) of the travel document (e.g. passport), except for the "place of birth" which is available only from the Visual Inspection Zone (VIZ) (ICAO 2015). Additionally, airlines may collect other data components[75] related, for instance, to a secondary travel document (e.g. when a visa is required for travelling), or generally found in airline systems (e.g. information specifying the seating arrangement of passengers) (ICAO 2015). Accordingly, the structure of individual API messages and the amount of data they contain can vary. Table 3 and 4 provide a summary of the core and additional data fields mandated under the API Directive.

Header data	**Footer data**
Airline code	Surname

[74] Ibid, see Section 8.1.5(a) for a complete specification of data items.
[75] Ibid, see Section 8.1.5(b) and 8.1.5(c) for a list of additional data elements available in airlines reservation systems and those not normally included.

Flight identification number	Given name(s)
Scheduled departure date	Nationality
Scheduled departure time	Date of birth
Scheduled arrival date	*Place of birth*
Scheduled arrival time	Gender
Last place/port of call for aircraft	Type of travel document
Place/port of initial arrival for aircraft	Travel document number
Subsequent place/port of call within the country	Issuing state or organization
Number of passengers/crew members	Expiration date of travel document

Table 3. List of API data elements (Header and Footer data) (Author's elaboration).

(Additional) Header data	**(Additional) Footer data**
Seat assignment	(Visa) number
Baggage information	Issue date
Traveller status	Place of issuance
Place/port of original embarkation (passenger)	Primary residence (country, address, city, etc.)
Place/port of clearance (immigration)	Destination address
Place/port of onward foreign destination	Other document number used for travel
Passenger name record locator number	Type of other document used for travel

Table 4. List of additional API data elements (Header and Footer data) (Author's elaboration).

In the case of the PNR Directive, the scope of data collection is much wider than the sole identity data contained in passengers' travel documents. From an individual PNR record, authorities can infer information about when and how reservations were made, as well as other details about the traveller and the intended journey. In particular, the collection of PNR data complements biographic information with travel route details provided by passengers at the moment of a flight reservation, then stored into air carriers' reservation systems. Accordingly, individual PNRs are created by many intermediaries (e.g., travel agencies, online booking systems, etc.) at the time of travel intent, and are then collected by airlines for their own operational and commercial purposes in the provision of air transportation services. Depending on the moment when the journey is booked, data can be captured many days or months in advance of a flight, and up to a year. Given that the nature of PNR data is declaratory, the quality and specificity of information provided for each journey vary from passenger to passenger. Yet, in contrast to Article 4 of the API Directive, the PNR Directive does not foresee any sanctions when air carriers transmit incomplete or false data.

The ICAO document 9944 (ICAO 2010) contains a list of data elements that may be present within an individual PNR. These elements consist primarily of basic biographic data (e.g., surname, given name, gender, date of birth, nationality, place of birth etc.) – which largely overlap with API data – and address details (e.g., contact address, billing address, email address, home address); supplemented by information related to the reservation (e.g. contact and payment details, meal selection, seat and baggage information, frequent flyer number etc.) and the travel itinerary (e.g., origin city/board point, destination city, active itinerary segments, cancelled segments, layover days, flight departure date etc.). Therefore, the list of data elements can be extensive. Table 5 identifies the 18 items that are generally required by States, with the 19th item being the historical data of the previously identified 18 items.[76] The categories of data mandated by the two Directives constitute the basic inputs into data-driven processes that aim to verify travellers' identity (API) and predict their behaviour (PNR). For instance, API and PNR can be used for risk-based targeting and to complete watchlist checks – either manually or automatically – since they contain the full biographic details of all passengers and crewmembers on a flight.

[76] Information around these 19 items is found in ICAO Document 9944 (ICAO 2010).

19 PNR Data Elements
PNR record locator code
Date of reservation / issue of ticket
Date(s) of intended travel
Name(s) on the PNR
Available frequent-flyer information (free tickets, upgrades, etc)
Other names on PNR, including numbers of travellers on the PNR
All available contact information
All forms of payment information and billing information
Travel itinerary for specific PNR
Travel agency and Travel agent
Code share PNR information
Split/divided PNR information
Travel status of passenger
Ticketing information including ticket number, one way tickets, and automated ticket fare quotes
All baggage information
Seat information include seat number
General remarks including OSI and SSR information
Any collected APIs information
All historical changes to the PNR listed in data types 1 to 18 Above

Table 5. List of PNR data elements required by States (Author's elaboration).

Yet it is possible to spot partial overlaps between the data fields mandated by the two Directives. If combined, the scope of API and PNR data collection amounts to approximately

106 data elements[77] (See Table 6). Nearly all API elements (approximately 38 out of 106) may be present within a PNR. Of these, ten primary data elements are taken from MRTDs (i.e. surname, given name, gender, date of birth, nationality, place of birth, type of travel document, travel document number, name of issuing organization, expiration date of travel document). Five additional elements may be added to both records when Machine Readable Visas (MRVs) are used (i.e. visa number, date and place of issuance), or other secondary travel documents are provided by passengers (i.e. the type of document, and its number). However, not all the above listed items may be required by a State or may be applicable to all passengers (in the case of the PNR system). Leaving this option at the discretion of Member States creates several inconsistencies in the collection, processing and use of passenger data.

PNR and API Data Elements	Number
MRTD details	10-15
Contact details	6
Passenger/crew flight details	66+
Payment details	~4
Other information	~4
Data related to aircraft flight	9
Total	~106

Table 6. Total number of API and PNR data elements (Author's elaboration).

For instance, API data are generally lacking for intra-EU journeys. While in the case of PNR, the choice to apply the Directive within one Member State or between two Member States (i.e. inside the Schengen area) is voluntary, in which case the European Commission must be notified (Article 2). Therefore, each Member State has the power to require PNR data for intra-EU flights if they find it necessary, and indeed most of them do so. According to the list published by the Commission (OJEU 2020: 7), 10 out of 13 Member States[78] that had implemented the PNR Directive before the transposition deadline of 25 May were making use

[77] 102 out of 106 elements concern PNR data. 38 out of 106 are composed of API data.
[78] The following Member States apply the Directive to intra-EU flights: Belgium, Germany, Croatia, Italy, Lithuania, Hungary, Malta, Poland, Slovakia, UK.

of this option. At the same time, this extension inherently contravenes the principle of "freedom of movement" that forms the backbone of the Schengen zone. The Schengen border code establishes that only minimum controls apply to EU citizens crossing the EU external border vis-à-vis third-country nationals entering, exiting or transitioning on the EU territory. However, when data are collected in bulk, such as in the case of PNR, enforcing a distinction between extra-EU and intra-EU travel is relatively more difficult due to the impossibility to establish a discriminant unless stopped at borders for further investigation. This in turn can result in the potential infringement of the rights of individuals, not when they are stopped, but when their data are collected and then processed.

The PNR Directive does not exclude the possibility of extending the scope of data collection also to other modes of transportation, such as maritime, rail and road carriers (Recital 33). This possibility was discussed within the Council Working Party on Information Exchange and Data Protection (DAPIX) in the second half of 2019 and eventually it was implemented on 2 December 2019 (Council of the European Union 2019b). So far it has been used only by a few Member States, yet the crux of the controversy lies in the fact that any such extension of the scope of the Directive is foreseen by its legal basis. The possibility to do so with no prior discussion of its necessity and proportionality potentially amounts to a permanent, on-going investigation into all possible future criminal acts (Vladeck 2014; Donohue 2014). I have already stressed the legal and ethical questions, including considerations on their impact on fundamental rights, in relation to the concept of "latent development" as built into the SIS infrastructure (see Chapter 3). Similarly to the SIS, the PNR instrument constitutes another case of "flexible" and thus "latent" technology whose functionalities can be expanded without the need to priorly update its legal basis.

5.3. From data inputs to security output(s)

The following analysis unfolds the various stages of data structuring that transform the set of inputs (i.e. passenger data) identified in the API and PNR Directives into pre-determined outputs (i.e. "risky" travellers) for law enforcement authorities. As advanced in Chapter 1, how data are set to work within different security sites – in this case for law enforcement – depends on the underlying processes by which they are generated, composted and ultimately computed in order to be rendered governable (Bellanova and Fuster, 2019). Thinking in terms of

relationality between data inputs and resulting outputs invites to move beyond investigating the obscure process that encodes security-related decisions. Through this alternative approach I seek to examine how the transfer and subsequent processing of the data categories collected under the API and PNR Directives determine the security processes to be applied before departure or after arrival of passengers. While the final section focuses on their processing, in what follows, I look specifically at the transmission of passenger data through electronic means, which yet makes use of different modes and analytic procedures that inevitably condition the trajectories of the data exchanged. The scope of this section is therefore twofold: first, to look at the provisions that regulate the transfer of API and PNR data from the airline industry to the competent authorities responsible for their processing; second, to visualise such transfers in the form of a network of data exchanges by employing visual network analysis.

5.3.1. Visualising the transfer of passenger data

The technical arrangements of API and PNR systems are substantially different from other centralised, pan-European databases like the SIS II (see Chapter 3). In the case of API and PNR, there are several such systems (-plural) in Europe (and across the world)[79], with no centralised components. Each Member State is bound by the API and PNR Directives to develop and implement its own systems. This is why, rather than focusing on their internal technical arrangements, I look more broadly at the configuration of API and PNR as two separate networks of systems – each with different modes for transferring data and separate sets of actors participating in the exchange. In order to display the central features of the operational exchange of API and PNR data, I followed a procedure similar to the one applied to create the network visualisations of the SIS II and the Prüm framework. However, instead of remarking the steps of the visualisation technique employed (i.e. software used, etc.), I move directly to the specificities of the network design. In consideration of the Member States that participate in the API and PNR networks, I have included only those that at the end of the review period (as of 2019) had "fully transposed" the API and PNR Directives and were declared as having "fully functioning" systems in place (European Commission 2020b; 2020d).

[79] Although it goes beyond the scope of this research, which takes place on the EU level, it is important to note that PNR data may be transferred to non-EU countries under certain specific conditions. Part Three, Title III of the EU-UK Trade and Cooperation Agreement deals with the issue of the transfer, processing and use of PNR data in relation to flights between the EU and the UK. The EU has also signed agreements specifically on the transfer of PNR data with Australia and with the United States of America. Source: https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lb8zp

This number amounts to 25 out of the 31 implementing countries[80] in case of API; and 24 out of 26 Member States[81] in case of PNR.

To transmit and receive passenger details electronically, air carriers, border control authorities and PIUs need to have their automated systems connected to one or more data transmission networks. In order to ensure the security and reliability of the electronic transfer, the European Commission requires that Member States abide to recommended practices with regard to the transmission procedure. Specifically, the transmission of API and PNR data is regulated at the international level by a set of internationally agreed standards, and guidelines developed by the World Custom Organisation (WCO), the International Air Transport Association (IATA) and the International Civil Aviation Organisation (ICAO). This set of regulations has been in place since the 1990s and governs the electronic interchange of structured data, related to trade in goods and services between independent, computerised information systems. In the context of API and PNR, the aim of these regulations is to establish trusted mechanisms and uniform measures – including a list of common protocols and supported data formats – in order to ensure a certain degree of alignment among air carriers in the transfer and subsequent handling of the data collected.

The journey of API data begins when passengers arrive at airports' desks for checking-in and release their flight and biographical information to the departure control system of the airline which they are travelling with. Given the high number of airline companies operating in each airport[82], to simplify, I labelled the whole universe of nodes corresponding to their departure control system simply as "DCS", followed by the ISO country code of the Member State in which the airport is located (e.g., DCS HU). Once captured, API are transmitted to border control authorities either as a single data file ("batch message") listing all passengers and crew members on a flight ("batch API"),[83] or individually, on a passenger-by-passenger basis ("iAPI"). The first version of iAPI was developed in 2009 in order to provide a more interactive

[80] Two implementing countries still were running pilot systems (Belgium and Slovakia) and four implementing countries (Cyprus, Greece, Iceland, Norway) did not have an API system but were planning to establish one post 2019.
[81] Of the two remaining Member States, Slovenia has notified partial transposition and Spain, which has not notified any transposition measures, was referred to the Court of Justice on 2 July 2020 for failure to implement the Directive.
[82] According to the latest evaluation of the API Directive (European Commission 2020d), the scope of API data collection in terms of air carriers regards all air carriers in 19 countries, whilst in 12 implementing countries API data are being requested from for selected air carriers only.
[83] Traditional (batch-style) API is still the most common and widely recognized mode of transmission in the airline industry (European Commission 2020d).

request/reply type of application for the positive acknowledgement and response back to air carriers' system. Interactive API systems indeed allow for a two-way communication between air carriers and border control authorities in near real-time. Yet they are more costly to implement compared to batch-style API, because their operation requires authorities to perform multiple actions in a matter of seconds in order to vet the information of all inbound passengers and crew members.

Regardless of the mode used, the transmission occurs shortly after flight departure – and not earlier than 30 minutes before – or even after take-off, to ensure a complete list of passengers on board. The standard format[84] used for the transfer of API data is the UN/EDIFACT PAXLST message (WCO/IATA/ICAO 2013b). The transmitted data then reach the server of the national border control authority in the country of destination or departure. In the graphical representation, I labelled the server as "Server BCA". This first step in the API network creates a (directed) edge between "DCS" and "Server BCA" in each implementing country. After having distinguished between "legitimate" travellers and travellers "of interest", border control authorities return a response to the carrier by issuing a "board/no-board" advisory message pending approval. According to the API Guidelines (WCO/IATA/ICAO 2014) the standard format for returning a response to an air carrier is the UN/EDIFACT CUSRES (Customs Response) message. This type of response functions as an official acknowledgement by border control authorities for the receipt of a PAXLST message. This creates a further (directed) edge – yet in the opposite direction – between "Server BCA" and "DCS".

Note that in reality the edges between the two are more numerous because border control authorities may be sending API data for verification purposes to one or more designated authority entitled to request or receive API data in each implementing Member State. Therefore, in order to account for these connections, at least partially, I labelled the nodes corresponding to the whole universe of the national authorities as "NA", followed by the ISO code of the relative country (e.g. "NA HU"). Depending on the number of requests, this second step creates a further edge, between the national server of border control authorities – "Server BCA" – and the national authorities in the receiving country(ies) – "NA". These trajectories result in a high number of overlapping edges that cannot be directly visualised in the graphical representation of the API network. Yet, in terms of visual features, it is not surprising that what

[84] States implementing API systems should conform to common standards, developed and jointly maintained by ICAO, the International Air Transport Association (IATA) and the World Customs Organization (WCO).

prevails is the concentration of edges, compared to the inputted number of nodes (Figures 14 and 15). For 75 inputted nodes (3 nodes category for 25 implementing countries), the resulting number of edges – and thus of interconnections among the actors participating in the API network – amount to 1250.

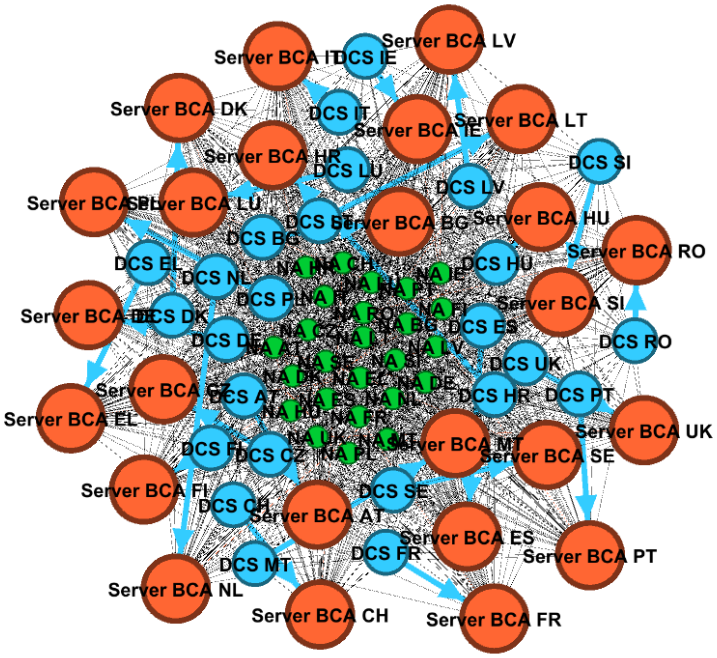

Figure 14. Force-directed layout of the API network (Force Atlas 2).

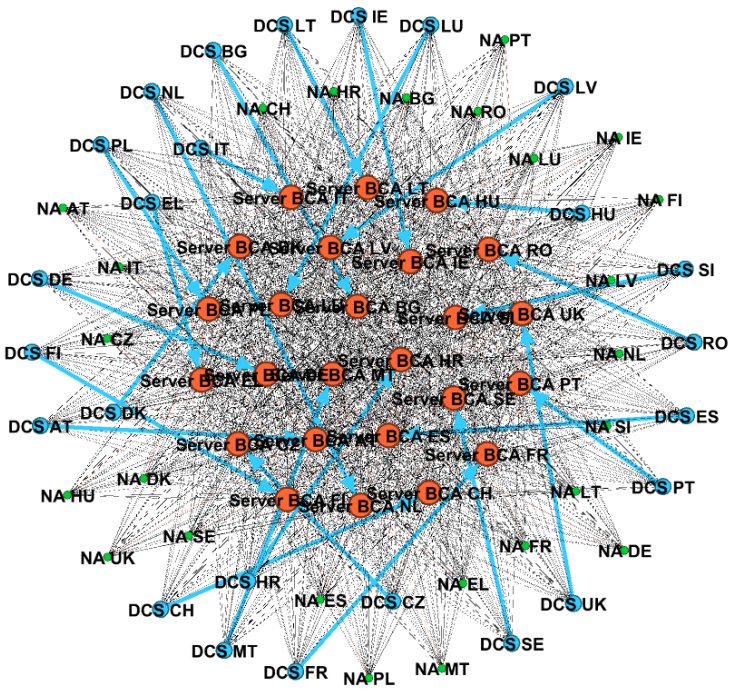

Figure 15. Force-directed layout of the API network (Fruchterman Reingold).

Moving on to the PNR, the Directive sets out two methods for transfer: the "push" and the "pull" method (Article 8 and 9 respectively). Through the "push" method, aircraft operators transmit (i.e. "push") electronically the collected data elements into the database of the national authority that requests them. While through the "pull" method, competent authorities can directly access air carriers' reservation systems and extract (i.e. "pull") a copy of the required PNR from their database. The push method is generally preferred since airlines remain in control of the data provided, and is thus considered less privacy-intrusive compared to the "pull" method. In this case, PNR are generally sent by air carriers as a single message from their reservation system to the Passenger Information Unit (PIU) of the Member State concerned. To account for these two actors in the network visualisations, I labelled the node category corresponding to air carriers' reservation systems as "RES" and the category corresponding to the servers of PIUs as "Server PIU" – followed by the ISO code of the relative country (e.g., RES ES, Server PIU ES).

The transfer of PNR between them represents the first stage in the PNR journey. In the graph, this creates an edge that connects each "RES" to each "Server PIU". In order to ensure a certain degree of standardisation in the transfer, air carriers are bound by Article 16(2) of the PNR Directive to adopt one of the data formats and transmission protocols listed in points 1 and 2 of the Annex to the Commission Implementing Decision 2017/759 (OJEU 2017). This Decision is based on globally agreed standards, in particular the PNR ICAO Guidelines and the UN/EDIFACT based PNRGOV message developed by the WCO/IATA/ICAO (2013a). Alternatively, air carriers can use XML PNRGOV as transmission mode which requires the use of Internet Web services, yet this standard is still under development. To acknowledge the receipt of a PNRGOV message, governments recur to "ACKRES" as a response for two types of events: to acknowledge that a State has received the carrier's message (or interchange) for processing; or, to indicate that a State has processed the carrier's message. Governments can also recur to "GOVREQ" to make an ad-hoc request for a PNRGOV (e.g., for a specific airline, flight number, date or for a specific record locator). Under these instances, the data travel backwards and thus cross the same edges, but in the opposite direction – from "Server PIU" to "RES". This process results in a number of overlapping edges that cannot be directly visualised in the graph.

The sole entity responsible for handling the transfer of PNR data (and its subsequent processing) is the so-called Passenger Information Unit (PIU). Each Member State is

responsible for designating the national body that hosts the PIU (generally run by law enforcement authorities) along with the required equipment and personnel (Article 4.1); and for adopting a list of competent national authorities entitled to request and receive the PNR data processed by the PIU (Article 7). According to the latest report on the implementation of the PNR Directive (European Commission 2020b), the totality of Member States have established fully operational Passenger Information Units, and have designated the authorities entitled to request and receive PNR data from them. Given the centrality of PIUs, their node category appears as bigger than the others. Indeed the PIUs initiate the second stage by handling all PNR transfers with the PIUs of other Member States as well as with Europol (Article 4.2). To account for the participation of Europol, I have assigned a node and labelled it as "EUROPOL". Such transfers create multiple edges that interconnect "Server PIUs" with one another as well as with "EUROPOL".

The last stage concerns the transfer of PNR from the PIUs to the national authorities entitled to request and receive them. Like for API, I labelled the category of nodes corresponding to the whole universe of the national authorities as "NA", followed by the ISO code of the relative country (e.g. "NA ES"). In this case, the transfer occurs through any existing channels for cooperation – that is, through bilateral or multilateral agreements or through the so-called "Secure Information Exchange Network Application" (SIENA).[85] This interconnection creates further edges between the nodes of each "Server PIU" and the nodes of each "NA". Figures 16 and 17 report the resulting graphs for the network visualisation of the PNR. In Figure 16, it is not surprising that the "EUROPOL" node is left out from the main cluster of nodes – that is, where most of the connections between groups of nodes are concentrated – given the marginal role of Europol in the PNR network. Similarly, the limited number of edges that target national authorities ("NA" in the graphs) resulted in their marginal disposition around the periphery of the relational distribution. In Figure 17, the various stages that build up the PNR network are clearly represented, as one reads the graph from the outer circular frame, where all the "RES" nodes are located, to the centre, where most of the transfers between "Server PIUs" take place.

[85] SIENA has been developed for the secure exchange of information between Europol and the Member States and has been operational since 2009. It functions as a central management system for case handling, cross-comparisons, and the exchange of structured data. In more recent years, SIENA has also become the default information exchange channel for specialised law-enforcement units, such as the case of passenger-information units (PIUs). Source: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena

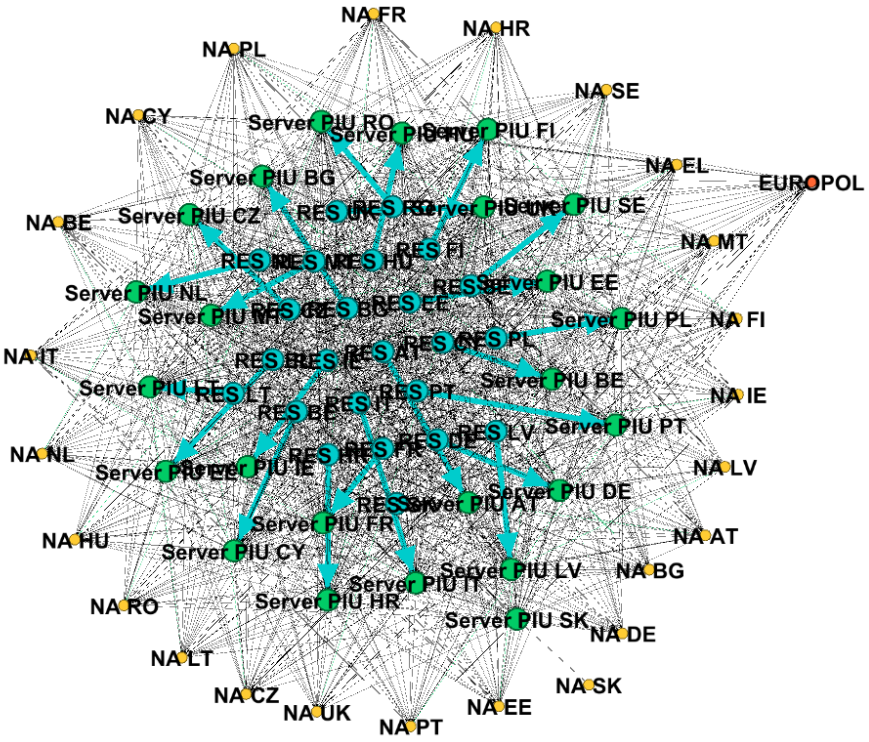

Figure 16. Force-directed layout of the PNR network (Force Atlas 2).

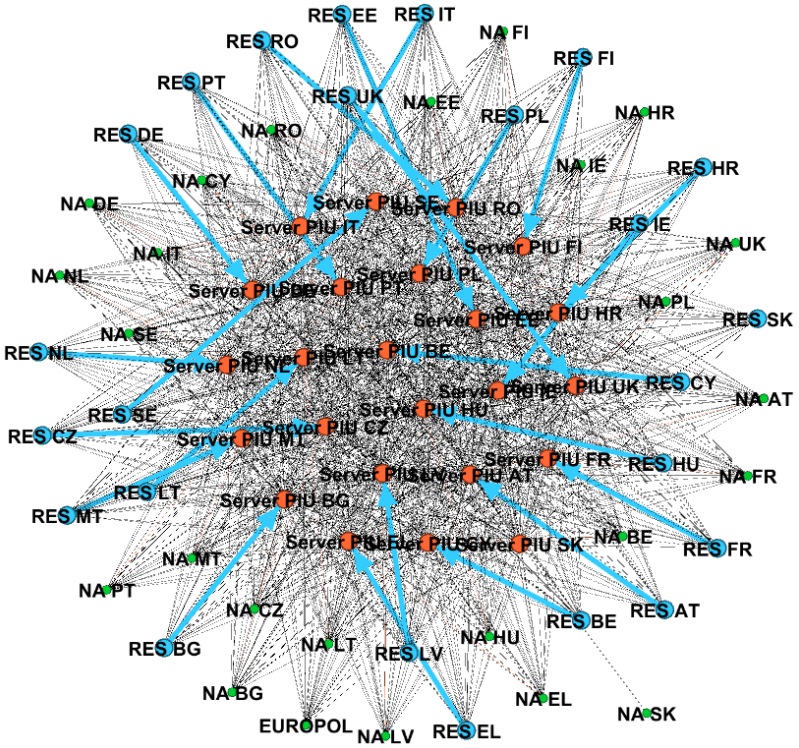

Figure 17. Force-directed layout of the PNR network (Fruchterman Reingold).

In total, the number of edges for the PNR network amounts to 1153, based on 73 inputted nodes (3 nodes categories, for 24 countries participating in the PNR network, plus Europol). This proportion between number of nodes and edges is not so dissimilar from the API case (75 inputted nodes and 1250 edges). To understand the significance of this proportionality, we have to observe more closely the relational disposition of the nodes in the API and PNR networks. Both networks appear more crowded in the centre where the core group of nodes is located. In the PNR network, the core group is represented by "Server PIUs" (green nodes in Figure 16, and red in Figure 17), while in the API network, it is represented by "Server BCAs" (red nodes in Figures 14 and 15). These clusters contain a higher density of edges, that in turn signals a higher volume of data transfers. Accordingly, the proportionality in their disposition is the result of the number of connections established. All nodes belonging to the core group are in fact equally operational, meaning that they have a similar stake in the exchange of API and PNR data with the other nodes in the group. By contrast, the peripheral group featuring "NAs", "RESs" and "DCSs" (Figures 15 and 17) is left out from the central relational disposition, meaning that the lower number of connections has little impact on the transnational exchange of data through of the API and PNR networks.

This visual characteristic is the direct result of the decentralized nature of their network arrangement and validates the claim about the relevance of the difference between centralised and decentralised systems when reproducing the data lifecycle visually. The most significant finding indeed emerges from the comparison between the Prüm visualisations and the API and PNR network visualisations (Figures 18, 19 and 20). What these three have in common is that their infrastructures are arranged on a decentralised basis. Therefore, in the absence of a central component, each actor that participates in the network has to establish individual connections with the other operational actors. This inevitably results in the high number of edges that traverse the respective graphs (Figures 18, 19 and 20). Additionally, it further substantiates the claim about the technical complexity of developing a decentralised infrastructure of information exchange. The connections in a centralised infrastructure are in fact necessarily lower, since all the actors exchange data via the central system rather than among each other. Yet the main takeaway from their visual juxtaposition concerns the importance of the relations between the actors (edges) above the assumed relevance of these actors themselves (nodes). What this entails at the level of practice is that the trajectories of data multiply as more "cycles" of uses, and thus of relations, are established. This observation further strengthens the value of plotting the data lifecycle as a network of practices.

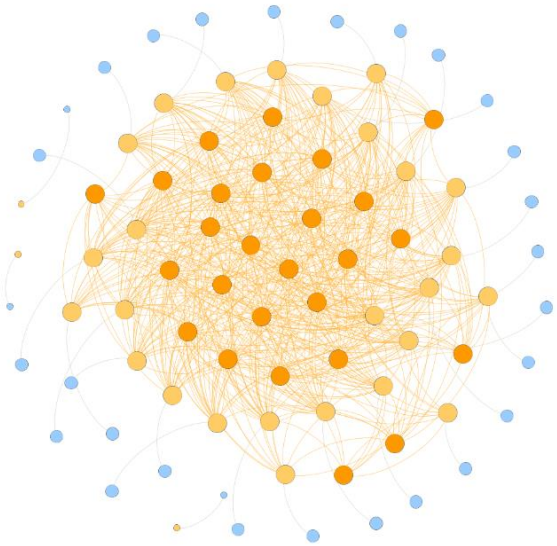

Figure 18. Graphical topology of the Prüm network.

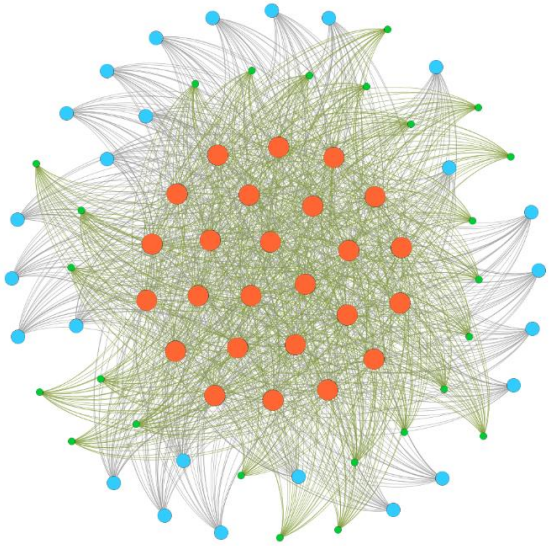

Figure 19. Graphical topology of the API network.

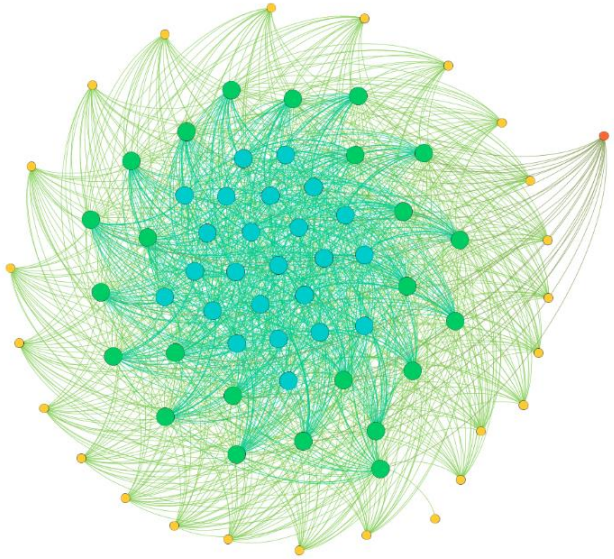

Figure 20. Graphical topology of the PNR network.

5.3.2. The production of "risky" outputs

Once PNR and API data are transferred from air carriers to the competent national authorities, the next stage in their lifecycle concerns their processing, by means of specific analytic techniques. This section looks specifically at how the protocols that regulate the transfers of

API and PNR as well as the technical arrangements observed through the network visualisations mediate sovereign decisions of arrest and exclusion by filtering out those circulatory elements that are considered "unwanted" (e.g. irregular migrants) or "risky" (e.g. individuals suspected of terrorism and other forms of serious crime). Article 3 of Directive (EU) 2016/680 defines 'processing' as:

> "Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".
>
> (OJEU 2016b, art. 3)

The API Directive mandates the electronic transmission of API to BCAs in order to carry out the advance screening of passengers that potentially present a risk to aviation and internal security. The verification procedure is performed against various national, EU and international databases, including national records or watchlists, criminal investigation registers, the Schengen Information System (SIS), the Visa Information System (VIS) and international watchlists. Annex 9 to the Convention on International Civil Aviation ("Chicago Convention") recommends States to limit the query by using only those elements located in the Machine Readable Zone (MRZ) of the travel document, since they provide a higher threshold of reliability (ICAO 2017a). These consist of basic biographic attributes that apply uniquely to a person. Accordingly, API data are processed mainly for identity management purposes, with the objective of combatting illegal immigration. By obtaining data beforehand, border guards have enough time to examine whether there are "high-risk" passengers on board (e.g. passengers included on watchlists), who may require secondary checks before being allowed to enter the country of destination. Article 6(1) of the API Directive provides also for the processing of API data for law enforcement purposes, subject to the national laws of those Member States that require them.

Yet this aspect appears as secondary compared to Article 6 of the PNR Directive that clearly states the risk assessment purpose behind the processing of passenger data – that is, for: "carrying out an assessment of passengers *prior to* their scheduled arrival in or departure from the Member State to identify persons who require further examination by the competent

authorities (…)" (OJEU 2016c: 139). The PNR framework distinguishes two modes for processing PNR data. The first one concerns the 'pro-active' use of PNR to create and update pre-determined criteria that allow for the identification of persons who were previously unsuspected of involvement in terrorist offences or serious crimes (Article 6(2)(c)) (OJEU 2016c). This type of risk assessment requires constant update as the database is fed with new information directly from airline reservation systems and results in the emergence of new travel patterns. In practice, the detection of atypical travel behaviours – such as tickets booked at short notice and paid for in cash, indirect travel routings, and short stays following long haul journeys – is achieved through the employment of rule-based algorithms (see Hall 2017; Rouvroy and Berns 2013; Yeung 2018). What is targeted is an alleged modus operandi that is generally associated with smuggling, trafficking of people or drugs. At the operational level, this kind of analysis provides for a risk-based approach to the identification of *unknown* travellers whose combination of attributes against pre-determined risk indicators (see Amoore and Raley 2017; Aradau and Blanke 2015) suggests that they pose a threat to aviation security.

The result of this mode of threat assessment is the possibility to prevent travellers from commencing their journey, if deemed suspicious, or, conversely, to the facilitation of their entry, if legitimate. The second mode of risk assessment concerns matching passenger data against relevant databases (e.g., SIS, Eurodac,[86] ECRIS,[87] etc.) or national and international watchlists in the identification of *known* suspects (Article 6(2)(a)) (OJEU 2016c). In this case, the assessment happens in near 'real-time', that is prior to passengers' scheduled arrival in or departure from a Member State. Rather than generating new criteria that inform traveller risk assessment, this 'passive' use of PNR data relies on the analysis of pre-existing information in the identification of *known* suspects. Therefore, the parameters for identifying individuals are already known. In order to check for matches, the data elements collected (e.g., credit card used for the booking or associated telephone numbers) are entered as a targeting rule against pre-existing records that contain biographic information (name, date of birth, sex, nationality, etc.) or other secondary identity attributes for a wanted person, depending on what is known.

[86] Eurodac is a large-scale IT system that helps with the management of European asylum applications since 2003, by storing and processing the digitalised fingerprints of asylum seekers and irregular migrants who have entered a European country. Source: eu-LISA, https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac

[87] The European Criminal Records Information System (ECRIS) is a decentralised system established in April 2012 for exchanging information on previous convictions between EU Member States. Source: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en

From the operational, analytical and technical point of view the use of pre-determined criteria is more demanding since it requires advanced software and algorithms in the performance of rule-based targeting. This explains why, according to the latest review of the PNR Directive, the first mode of risk assessment is still at an early stage of implementation in most Member States, whilst the second mode of processing is more widespread (European Commission 2020b). The second mode concerns the comparison of PNR data against databases already implemented for the purpose of 'preventing, detecting, investigating and prosecuting terrorist offences and serious crime' (Article 6(3)(a)) (OJEU 2016c: 139). Most Member States comply with – what is supposed to be – a purpose limitation requirement and limit the processing of PNR data to only those databases regarded as "relevant". Yet the wording of 'relevant databases' is way too vague and can therefore be understood to encompass a wider range, not strictly related to the "law enforcement context". In general, the reference database most widely used is the SIS – the largest information sharing system for security and border management in Europe. Yet querying PNR data against the SIS is often challenging due to the discretionary nature of PNR, combined with the lack of sufficient detail concerning the type of offence underpinning a specific SIS alert (see Chapter 3).

As PNR data are unverified for travellers' identity and are often limited or incomplete due to their discretionary nature, significant risk analysis is required in order to reliably match PNR with the records contained in the reference system, such as the SIS. Accordingly, the best operational results are often achieved by the joint processing of API and PNR data. The availability of verified API data elements – and in particular the date of birth – directly from the machine-readable travel document enables the processing to be more targeted and specific. Hence, in order to boost the reliability of PNR, the PNR Directive established an obligation (Article 8(1)) for air carriers to transmit API data (in addition to the richer PNR reservation data) 'if collected during the normal course of their business' (OJEU 2016c: 140). In this case, API data must be treated as PNR data and should therefore conform to the provisions contained in the PNR Directive. The latest revisions of the API and PNR Directives (European Commission (2020d; 2020b) have evidenced the usefulness of combining API and PNR in order to strengthen the reliability and effectiveness of these systems as law enforcement tools.

Nevertheless, the presence of several discrepancies concerning the purposes for which API and PNR can be used may hinder their efficient processing in the context of law enforcement. In case the passenger's date of birth is lacking – that is, when airlines are not required to collect

API data for intra-Schengen flights – the ability to perform exact matches against the SIS database is affected. This in turn creates uncertainty as to whether any positive result obtained by vetting API data concern a person subject to a SIS alert. Even more crucially, having two legislations regulating the use of passenger information creates security gaps and legal uncertainty as to which categories of data can be used for border management, and which ones for law enforcement. This is especially the case when API constitutes an element of PNR data and is then transferred to the PIU – either together with PNR or separately. In terms of data protection, both the API and PNR Directives contain some legal guarantees against the misuse of data. These rights concern for example, the right of natural persons to access and request the correction and erasure of data, and the right not to be subject to solely automated decision-making. Simultaneously, data controllers – that is, the users that determine the purposes and means for data processing – have to comply with a number of principles, such as data minimization, purpose and storage limitation, transparency, fairness, accuracy, confidentiality and accountability.

More broadly, the protection of natural persons against the adverse effects of automated processing falls within Article 22(1) of the EU General Data Protection Regulation (GDPR)[88] which states that: 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces adverse legal effects concerning him or her or, similarly, significantly affects him or her' (OJEU 2016a: 46). However, since the API Directive pre-dates the adoption of this legislative proposal, it does not include up to date procedural safeguards as found in "new generation" legal instruments like the PNR. The current version of the text only refers to Directive 95/46/EC ("Data Privacy Directive") (OJEU 1995a) and as such it is outdated.[89] While the PNR Directive is in line with Article 22 of the EU GDPR which provides that the final decision concerning the automated processing of data shall always be taken by authorized competent authorities, and not from a machine or processing system (OJEU 2016a). The inconsistency between "first-generation" and "new generation" legal instruments in the passenger information landscape can expose data subjects to potentially disproportionate and unlawful data processing activities.

[88] The GDPR has significantly reviewed the EU data protection framework by seeking to strengthen the obligations of data controllers and the rights of data subjects in relation to the processing of personal data, while ensuring the free movement of such data within the Union.
[89] The Data Privacy Directive was applied until 25 May 2018, and it was then replaced by Regulation (EU) 2016/679 ("General Data Protection Regulation").

In addition to this legal gap between the API and PNR frameworks, there is another element that causes uncertainty in their application – namely, the period of data retention. The ability to conduct risk-based assessments is promoted by the possibility to retain API and PNR data after their initial transfer. Article 6(1) of the API Directive provides that, for border control and migration purposes, authorities shall delete API data within 24 hours after transmission (OJEU 2004). This measure appears as proportionate in relation to the time allowed for the performance of pre-vetting screening procedures. However, the Directive does not establish any data retention requirement when API data are transferred for law enforcement purposes, leaving such matter to the competence of national laws. Similarly, the PNR Directive allows security authorities to retain PNR data for "as long as it is necessary for and proportionate to" the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and serious crimes (OJEU 2016c: 135). It further provides that 'where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, the retention of such data by the competent authority should be regulated by national law, irrespective of the data retention periods set out in this Directive' (Ibid: 135).

In the case of the PNR, the length of the retention for data provided by air carriers to the PIUs of relevant Member States should not exceed five years, after which data should be deleted (Article 12(1)) (OJEU 2016c). Accordingly, it is possible for law enforcement authorities to conduct a future query since the Directive allows for the creation of an historical database which contains five years' worth of information. The need to retain PNR data for five years, compared to the very short time allowed for processing API data, stems from the different nature of these systems. API is mainly directed at identifying known individuals in the border control context. While the PNR is mainly used as an analytical tool aimed at uncovering the associations between known and unknown (suspect) individuals. By definition, the identification of risk patterns demands for long-term risk analysis through the pooling of a sufficient amount of data, and hence, for a longer data retention period. Under such circumstances, the PNR Directive provides for the 'depersonalisation' of data after an initial period of six months by 'masking out' data elements (OJEU 2016c: 135). Yet the use of undefined terms such as 'anonymization', 'depersonalization' and 'masking out' adds further uncertainty as regards the length of data retention.

'Anonymisation' means the removal (i.e. masking out) from a dataset of direct identifiers (e.g., name, date of birth, ID number, contact and payment information etc.) that would allow direct or indirect identification of a person. 'To depersonalise through masking out of data elements' means to render those data elements which could serve to directly identify the data subject invisible to a user (OJEU 2016c: 138). This is generally achieved by replacing in the dataset such identifiers with an 'encrypted' one (e.g. a serial number instead of the full name of an individual). When reference to such terms is made in the API and PNR contexts, there is the somewhat implication that it is no longer possible to link anonymised or masked out data back to an identified or identifiable individual (Korff 2015). In reality, there is no legal guarantee that ensures anonymity, especially if the data in the dataset are linked to or combined with data in other datasets. The main problem with effective anonymisation is the size of the anonymised dataset – that is, the set of individuals to whom data might relate. This is the case of API and PNR. As more and more data are piled in the active search for identities, any attempt to achieve anonymisation through anonymised datasets is rendered meaningless by the possibility for 'retrospective identification' (Jakubowska and Naranjo 2020: 15), by mining other large datasets to which API or PNR data have been transferred or checked against. The unworkable attempt to ensure anonymity – in particular for data related to individuals unsuspected of any involvement in terrorist offences or serious crime – is particularly problematic from the data protection perspective.

As noted in the opinion of the Consultative Committee on data protection (Korff 2015), it is difficult to see how data protection safeguards can be applied to anonymised datasets, and especially in the context of the untargeted retention of API and PNR. Both cases provide for the search and disclosure of data – even depersonalised or anonymised data – […] '"just in case" the data might be helpful later in some future police or secret service inquiry' (Korff and Brown 2011: 184). The practice of "re-using" data is foreseen – and indeed is incentivised – by the latest developments at the EU level in matters of data retention[90]. Article 2(2) of the so-called "Data Governance Act" defines 're-use' as 'the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced (…)' (European Commission 2020f: 23). This definition attends to the design and implementation of technical solutions –

[90] See, for example, the imposition under the "Data Retention Directive" (OJEU 2006a) to retain communications data "just in case" those data might be helpful later in a criminal investigation. This practice basically provides an incentive for the untargeted, suspicionless retention of data.

like API and PNR – that render data transferable and meaningful in different security contexts across geographical, temporal, organizational and legal boundaries (Bellanova and Fuster 2020). Accordingly, once implemented, the API and PNR Directives create numerous cycles of use for pre-existing data by enabling passenger information to become re-usable entries in the investigation and prevention of criminal activities.

In reference to the purpose for which data can be processed, Article 4 of the GDPR states that:

> "For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected".
>
> OJEU (2016a: 27)

The possibility of "re-using" data *beyond* the context for which they were initially produced (just in case they *might be* helpful in a future investigation) constitutes an example of function "creep" (Innes 2001) and a major departure from the basic principles of the rule of law. Especially, such framing undermines the fundamental data protection provisions of purpose limitation, data minimisation and data retention. Repurposing data for law enforcement investigations and criminal proceedings raises accountability and transparency issues because of the particular legal framework in which national security agencies operate and the moves towards preventive, intelligence-led law enforcement. As stated by the Council of Europe (2018: 15): 'the main concern of using data from profiles for different purposes… is that the data loses its original context'. Whereas the use of personal information needs to be fit for purpose in order to ensure that fundamental rights and data protection safeguards are respected. The overall result is that risk assessment can be carried out multiple times as more API and PNR records are created. Therefore, national authorities, that are responsible for storing, processing and exchanging API and PNR data, are active contributors to the reinvention of the life of data.

Conclusion

Although from the API and PNR Directives it may appear that the gathering, transfer and processing of identity and travel data are rather smooth processes, in reality there are multiple

problems and frictions emerging. Most of the tensions that I have highlighted in this chapter arise in the context of private sector collection and public sector use. The often conflicting interests of airlines and law enforcement authorities result in the transfer of information that either lacks quality or is incomplete. Warnings about issues relating, among others, to the quality and completeness of data and the cooperation between private companies and law enforcement authorities have been advanced in the 2020 Review of the PNR Directive (European Commission 2020b). The Review is wary of the non-observance of the standards by some air carriers, which renders API and PNR systems not fully effective. These tensions matter since they puzzle the very discourses that justify the implementation of these systems – as well as of the other AFSJ schemes, more broadly. They demonstrate that information exchange is not always smooth, efficient, quick and accurate as it features "on paper".

In the API and PNR contexts, the fact that data are collected by air carriers and not by law enforcement directly creates an accountability issue which is magnified by the enmeshment between the state and the private dimensions of surveillance. The demands for API and PNR data are indeed part of the wider demands for the *preventive* collection, retention and processing of multiple categories of data sources – including health data, financial data, communication data and phone data (see Amoore 2008; Aradau and Blanke 2015; Aykut 2019). These demands combined with the possibility of linking passengers data to other massive bulk datasets, that are held especially by the police and intelligence agencies, represent the natural outcome of the trends towards *suspicion-less*, *intelligence-led* law enforcement (see Donohue 2014; Egbert and Leese 2020; Kaufmann 2019). Debates about the disproportionate uses to which API and PNR data could be put must therefore take place against this wider context. As Korff (2015: 8) puts it, "[the] "PNR" is not an isolated issue, but a new symptom of a much wider disease."

More specifically, the functional characteristics of API and PNR systems have been built on a whole new edifice of police and criminal law procedures that is increasingly concerned with detecting and apprehending those who have not yet broken the law – but are "predicted" to do so on the basis of "suspicious" patterns (Amoore 2013; Aradau and Blanke 2017a; Leese 2014). API and PNR systems thus feature as a medium for translating the security logics of prevention, pre-emption and traceability into operational interventions on individuals flagged as "risky". As Aradau and Blanke note, 'data-driven predictive policing technologies promise to be proactive rather than reactive' (2017a: 383). In such context, proactivity can be understood as

the capacity to purposely create an evidence-base through the aggregation of data in bulk. While the terms that refer to how passengers data are handled suggest benign administrative procedures (e.g., facilitation of legitimate travel and border crossings, smoothing out passengers flows, etc.) it is the use of API and PNR, resulting from their processing, that is instrumental to the mass surveillance of citizens (Lyon 2014, 2016).

These matters touch upon key legal and political issues which are not limited to the right to data protection, but are related, more broadly, to the repurposing of data in the AFSJ domain. Sharing passenger-related information – either in the form of API or PNR – already occurs as a matter of routine and with such high frequency that put the control of their exchange well beyond the jurisprudence of national oversight bodies.[91] In the case of PNR systems, data extracted by searching the database of a PIU in a Member State can be entered into the database of another PIU for further processing and thus be subjected to a different data protection regime. This causes accountability and legitimacy gaps, which in turn threaten the effectiveness of data protection principles. The identified inconsistencies between API and PNR systems and the lack of adequate safeguards create the need for an intervention at the EU level in order to ensure a degree of harmonisation and standardisation between these instruments (and the other schemes in the AFSJ area) and the legislative developments concerning data protection.

This intervention, in turn, may require more robust obligations in the way airlines and competent national authorities process personal data and in the way the repurposing of API and PNR data is achieved. In relation to this objective, this chapter has aimed to show how the scope of data collection and the desired outcome behind the implementation of API and PNR systems direct the processing and analysis of passenger data in specific ways. Whether the risk assessment of travellers is performed through the proactive processing of API data or by matching PNR data against pre-existing records, the input and the output that inform the assessment remain unaltered. Both instances require identity and travel data in the form of API or PNR (inputs) in order to identify suspicious patterns or flag potential risky individuals (output). Therefore, risk analysis simply acts as a means to achieve the law enforcement's desired objective of targeting suspicious people and identifying travel patterns that authorities were previously not aware of.

[91] To this regard, the EU Commission launched a series of consultations to address the technical and operational challenges derived from the cross-border exchange of electronic information, See European Commission (2010); European Commission (2015); and European Commission (2017).

The question remains of whether it is still possible to define the implementation of API and PNR systems in relation to a specific AFSJ purpose. While there is undeniably a link between the data fields mandated by the API and PNR Directives and the policy area concerned – border management for API and law enforcement for PNR – this link is preferential, not exclusive. Both instruments enable the collection of passengers-related information for purposes related to the identification of air travellers. However, the provisions contained in the respective Directives permit the transfer of such data from air carriers to competent law enforcement authorities for purposes (i.e. crime prevention) unrelated to the context of their initial collection (i.e. airline security and border management). Accordingly, in addition to the SIS and the Prüm framework, this analysis has showcased how the lifecycle of API and PNR systems is instrumental to the prevention, detection and investigation of terrorist offences and other serious crimes.

Chapter 6

Conclusion:

EU AFSJ Information Systems as Tools for Data Re-Purposing

Introduction

This research set out to identify whether the "making" of security in the EU AFSJ could be explained by reconstructing the socio-political, legal and technical conditions of possibility that have sought to facilitate the re-use of data in the context of the investigation and prevention of criminal activities. In the empirical chapters I have outlined the trends that I have found to be important determinants in the production of security knowledge through the (un-)making of a variety of data sources. I have thus mobilized the concept of "data lifecycle" throughout, in order to conceptually and methodologically substantiate how security is multiple and context-dependent on the design and implementation of different information infrastructures. By bringing together previous insights from IR, technology studies and infrastructural geopolitics, I examined the politicality of these more or less visible infrastructures, which are now so firmly embedded in mundane administrative processes to the point that our perception about them is altered. Yet many of these technologies are exerting influence not only on our digital selves, but, even more crucially, on our mobility across borders as well as on our likelihood to be targeted by preventative security interventions. In what follows, I continue this debate by examining the point of convergence of these trends, namely, what I have qualified as a move towards AFSJ information infrastructures as law enforcement tools for data repurposing.

6.1. Towards multi-purpose data and information exchange schemes

The empirical analyses of the SIS II (Chapter 3), the Prüm framework (Chapter 4) and the API and PNR systems (Chapter 5) have evidenced several instances under which personal data (in the form of fingerprints, DNA, biographical data, etc.) are collected from individuals for a different range of purposes, such as for ongoing criminal investigations, for predicting crimes, for the facilitation of border crossings, and not least, for air travel-related purposes. These are not one-time acts, but they are repeated instances that place individuals in a mechanism of constant scrutiny. For example, every time we cross the external border of a Member State, we need to re-claim and thus re-establish our identity by providing the information contained in our passport to border control authorities (including fingerprints provided when the passport was issued). Therefore, the generation of data – that largely corresponds to the first stage in the data lifecycle – is dependent on multiple administrative processes involving both the private and public domain. Indeed we have observed that from the circumspect collection and processing of data to their use for law enforcement ends, multiple actors, institutional arrangements and legal frameworks are involved in the composition of the SIS II, Prüm, API and PNR as networks of data exchanges.

Data are first captured and stored within different databases, at different moments, and across different spaces. They are then processed, analysed and transferred for different ends, in accordance with the purposes set out in the respective regulatory frameworks. As data pass through these different stages, they enter in a relational disposition with the informational environment in which they are materially embedded. Such environment is made of both infrastructures and humans that together have the capacity to "act on" the data, by bringing them to life, refining them through analytic techniques and repurposing them in order to inform various policing practices (Kaufmann and Leese 2021). The exposition of data to multiple interventions illustrates two aspects of the data lifecycle: first, it underlines that data are vulnerable but durable. Once data yield their productivity, they permeate the environment which they enter. Even data that in the first place are considered incomplete or lacking quality – and are thus not meant to be analysed – become "piled up" nonetheless. Through analytic practices, data are thus constantly reassembled, recombined and repurposed. Repurposing means that the data gathered and stored away can be extracted, either in toto or only partially, and then be used to initiate other "cycles" of uses.

Arguing that data are subject to a security judgement reiteratively underlines the second aspect of the lifecycle: data which have already been mobilized can be re-used as inputs into new analytic processes. Data are in this sense never verified, but rather, they are ascertained once and then stored away in "latent" databases. In other words, data become "redundant". In relation to the information infrastructures considered in the empirical analysis (i.e. SIS II, the Prüm Framework, the API and the PNR), the term "redundant" draws attention to the way in which each category of data circulates across the respective networks, which is far from occurring in a "circular" fashion (as the term "lifecycle" would suggest). As we have observed in the network visualisations produced for each case study, the lines (edges) that connect one actor to another constitute the trajectories that data leave behind when a new cycle initiates. These trajectories are multiple, never linear and potentially limitless since data travel back and forth from one actor to another. So data are in this sense "unsettled" because their life never repeat itself in the same order, or by following the same trajectory. This finding is crucial as it serves to illustrate the main advantage of the application of visual network analysis to the study of the lifecycle of data: transcending the orientation to replicate through writing the power dynamics that underlie the SIS II, Prüm, API and PNR networks of data exchanges.

VNA has provided the means not only for mapping these networks but also for making sense of the entanglements between security and technology by looking at their intertwined function in the lifecycle of data. Even more crucially, VNA allowed me to unlock our academic praxis from the disciplinary boundaries that were preventing a more profound engagement with the meaning of "making" security through the "(un-)making" of data. In the resulting graphical representations, digitalization functions as the precondition for guaranteeing security, and data are the means for delivering it. Yet by striving for a theoretical and methodological approach that would encompass the shift of policing towards technological practices (Austin and Leander 2021), we, as social scientists, are actively contributing to promote a vision of security as subsumed to technology. The graphical representations of the SIS II, Prüm, API and PNR networks indeed illustrate the argument that data undergo multiple transformations and repurposing processes throughout their lifecycles and are thus seen to fit the production of multiple security logics (Kaufmann and Leese 2021): they can be mobilized for the identification of suspicious patterns, such as in the case of the PNR; or to draw inferences about the occurrence of crime in retrospect, such as in the case of SIS II. Therefore, visual network analysis did not just substantiate what I already knew, but it also offered a few notable revelations.

6.2. Comparative overview

Before examining more closely the findings from visual network analysis, I turn to what constituted the crucial task of this investigation, that is, the identification of the *socio-political*, *legal* and *technical* conditions of possibility that allow for the exchange of data for criminal purposes at the pan-European level. In what follows, I adopt a comparative approach to discuss the results from the empirical analysis and address the research question. In brief, to deal with the socio-political conditions, I began with an understanding of the institutional context that shaped the development of the SIS II, the Prüm framework of cross-border information exchange, the API and the PNR through policy-making. To address the legal conditions, I examined the regulatory frameworks that form the normative backbone of these initiatives. Finally, to deal with the technical conditions, I considered the technical cases related to the possible consultations and uses of the systems, their architecture, as well as the modes for exchanging data. The results of these three tasks have evidenced the individual acts of power that "(un-)make" data in order to produce re-usable entries across different information infrastructures and in turn enact different modes of "making" security. Specifically, the first act concerns the structuring of the security vision at the political level through the design of policy initiatives. The second act concerns the translation of the security vision into a series of material requirements through legislation. And finally, the third act concerns the embedment of these material requirements into the design and functional characteristics of information systems.

6.2.1. *Socio-political* conditions of possibility

The reconstruction of the socio-political conditions of possibility has exposed the EU Commission's 'untested belief in information technologies as the ultimate solution for any security threat that the EU might face (Guild et al. 2009: 3; see also Besters and Brom 2010). Yet, at the beginning, the establishment of the Schengen area was hardly concerning aspects of police and security. With the introduction of compensatory security measures to the lifting up of borders – from the set-up of large-scale information systems and the digitalization of external border controls (now "smart border" controls) (see Dijstelbloem and Broeders 2015; Glouftsios 2019; Jeandesboz 2016) to the strengthening of police cooperation, etc. – this picture began to change. The assumption that the uncontrolled circulation of persons would produce

an inevitable increase in crime began to gain traction and gradually led to the informatization of the Schengen structures. The SIS, the Prüm framework and later the API and PNR systems were all born under the umbrella of the logic of (in)security. The *socio-political* conditions that drove forward and shaped the implementation of these contested security measures was thus emergency-driven. Paradoxically, the development of the most innovative systems that were intended to deliver more security, served to erode the freedoms and liberties of individuals through the routinization and the embedment of data practices into administrative processes of life.

Another interesting finding that emerged from the empirical analysis is that the sense of emergency was exploited not only to justify the establishment of the AFSJ information infrastructures (Parkin 2011), but also to advance the introduction of a number of controversial features, such as the AFIS functionality in the SIS II and in the Prüm framework, or again, the extension of the scope of the PNR Directive to intra-EU flights. These evolutionary dynamics were given impetus by high-impact acts of political violence, such as 9/11 and the terrorist attacks in Paris and Madrid (see Bigo and Carrera 2004). The exceptional justifications professed in light of the "new terrorist threat" were thus carefully deployed by the EU in order to frame discussions on the expansions of the scope of the SIS II, the Prüm, the API and PNR systems. Nevertheless, the essentially administrative nature of these technologies is in sharp contrast with the emergency-driven approach to policymaking that has shaped their evolution. This trade-off demonstrates that the EU has sought to normalize the logic of (in)security through mundane administrative processes that require the transfer of data for purposes other than forecasting and anticipating the next security event. The logic of emergency then, is now firmly embedded in the SIS II, in the Prüm, and in the PNR and API systems that relentlessly collect our personal information to investigate and predict suspicious criminal activities, to facilitate border crossings, or again for travel-related purposes.

Although the implementation of these technological solutions was underpinned by the same politics of emergency, the findings have shown that each system purports a different mode of "making" security. Specifically, the SIS II (Chapter 3) projects an understanding of security as concerned with the harm derived either from the movement of certain "illegitimate" categories of individuals (e.g., third-country national subject to a return decision, suspects of terrorism, traffickers, etc.) or from certain objects (e.g., stolen vehicles, misused documents, seized private property, etc.). The operation of inserting an alert in the SIS II indeed stigmatizes the

person or object concerned as a potential "threat" to EU security. The Prüm (Chapter 4) understands the body as the site of security decisions. In this system, the quest of visibility (through DNA and biometric data) becomes the quest for security. The rationality that informs the Prüm is yet more prone towards drawing inferences from the past. Finally, the API and PNR systems (Chapter 5) problematise movement, and hence the traveller, as a form of security risk that needs to be countered by appealing to the logic of prevention. Therefore, while the SIS II is concerned with the identification of individuals and the consultation of related alerts for both the investigation and prevention of criminal activities, and while the Prüm is more focused on forensics, the API and PNR are more about travel intelligence. Rather than being directed to the past, the logic inscribed in the API and PNR systems is pre-emptive and future-oriented.

The comparative analysis of the socio-political conditions has thus emphasised that security is multiple and dependent on the technological context in which it is enacted. This argument clearly supports the value of studying technologies in a situated manner in order to reconstruct the logics, rationalities, and different practices at stake in the constitution of multiple "spaces" of security. Indeed by placing the information infrastructures considered in their respective institutional and organisational contexts, I was able to scrutinize how the different security "imaginar(-ies)" that underpinned their implementation were first translated into material requirements through legislative acts and then into functional characteristics. In particular, the security solution envisaged at the political level has created an imaginary of how the system should look like and what it should or should not do, such as the possibility to collect and process certain categories of data (e.g. dactyloscopic or biometric data), or to access certain alerts (e.g. in the SIS II). Accordingly, by addressing the socio-political conditions I managed to unearth the first act of power that structures the field of security governance. This act is *political* and concerns the definition of a certain activity/object, such as the movement across borders, as a form of security risk.

6.2.2. *Legal* conditions of possibility

By placing the SIS II, Prüm, API and PNR systems in their respective normative contexts, I sought to unearth the *legal* conditions of possibility and thus the second act of power in the "making" of the security vision. The second act largely corresponds to the translation of the object to be "securitised" – as it has been defined at the political level – into a series of binding documents (e.g. regulations, directives etc.) that regulate what is expected of the information

infrastructure to be implemented, what are its technical requirements and functional characteristics, what type of data are sought to be collected, stored and processed through it and for which purposes. This process results in the incorporation of the proposed policy initiative into EU law. Specifically, the nature of the legal conditions of possibility that underpinned the implementation of the SIS II, Prüm, API and PNR is *material* and derives from the institutionalisation of a "flexible" technological architecture that could be re-arranged, expanded, or updated in response to political considerations. In this regard, the empirical analysis has shown that the systems displayed comparable evolutionary dynamics that resulted not from a direct "threat" to security, but from hegemonic "threat-defined" strategies – carefully thought out at the political level. The perceived increase of the threat level – for instance, as a result of an act of political violence (e.g. Paris attacks) – was instrumentalized in order to call for a higher security threshold (through policymaking), and thus for tighter measures (i.e. subsequent expansions of the systems).

These comparable findings led me to advance the notion of "latent technologies" in reference to the way in which their legal frameworks have been re-arranged without the need for lengthy renegotiations (Parkin 2011). These re-arrangements offered the possibility to add intrusive features, such as the interlinking of alerts in the SIS II, the addition of the AFIS functionality in the Prüm framework, and again the extension of the scope of the PNR Directive to intra-EU flights. What is even more peculiar in the way in which these systems were expanded is that the necessity for major updates was justified by the EU Commission and the Council by appealing to the logic of (in)security which shaped their original implementation (i.e. socio-political condition). The transformation of fear into an instrument of governance thus allowed for the implementation of highly politicized infrastructures for security governance. The costs of such institutional, normative and technical re-configurations are high in terms of legal uncertainty and insecurity as remarked across the studies conducted by the LIBE Committee, the EDPS and the FRA, among others. Indeed the possibility to activate "latent" functionalities and thus to redefine the purpose of these systems further erodes the distinction between tools used for law enforcement and immigration control. The inherent risk is to shield the legitimacy of this dual function behind latent infrastructures that codify the intrinsic legal and political arrangements, and in turn to increase the chances of negatively impacting on innocent persons.

As the legal and technical architecture of these systems is in flux, the major consequence is that the data funnelled in processes of security governance can be increasingly expanded, with

the associated danger to open up the way to indiscriminate data processing practices. It is not surprising then that the EU Commission has recently launched a number of initiatives[92] to facilitate the "re-use" of data in the context of police cooperation. These initiatives are part of a broader package called "the European Data Strategy" (European Commission 2020a), that promotes the implementation of AI-driven innovations in the field of police and criminal intelligence. According to Article 2 of the Data Governance Act (European Commission 2020f), the term 're-use' refers to 'the use by natural or legal persons of data held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the data were produced (…).' The vision purported is that of a common European data space in which data are used irrespective of the storage location. Yet by expanding the area of data exchanges beyond established territorial jurisdictions, technological innovations are producing new forms of political authority that are altering the nature of national borders. When data are exchanged and processed in the context of borders, crime or fight against terrorism, the thin line between jurisdictions as well as between different policy areas is constantly crossed. This in turn raises a number of legal issues related more broadly to the move towards multi-functional, multi-actor and multi-purpose information schemes.

In the context of data processing through large-scale databases, the notion of "purpose limitation" is indeed central for limiting the function creep built into EU databases. The notion of function creep (Innes 2001) can be seen as a virtual line between a lawful and justified data processing system and a surveillance tool – crossing that line entails going away from the original purpose of the system. In the case of AFSJ databases, three developments can be seen as resulting in the erosion of the purpose limitation principle: the possibility for Europol to enter alerts in the SIS II and to become a partner in the Prüm framework; the addition of the AFIS functionality, and thus the permission to identify individuals on the basis of fingerprints and facial images; and the possibility of extending the scope of the PNR Directive to intra-EU flights as well as to other modes of transportation. A corollary to the question of purpose limitation is time limitation: how long should the data be stored? What happens to personal data after the period of data retention has expired? The question of time limits reveals a lack of common standards in the context of AFSJ databases. Even more crucially, through the

[92] See, for example, OJEU (2018b) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 28 November 2018, L 303, pp. 59-68.

institutionalisation of "latent infrastructures" which yet are meant to be permanent, the EU is attempting to "introduce a surveillance regime that is continuous, untargeted and systematic" as ruled by the European Court of Justice (2022: 47).

6.2.3. *Technical* conditions of possibility

The regulatory frameworks analysed in relation to the legal conditions of possibility not only contained rules and procedures for operating the systems, but also the specifications concerning their architecture and functioning. Together these specifications form the *technical* conditions of possibility that can be observed in the making of a certain technology (means), and thus of a certain mode of "making" security (end). Specifically, the third act of power concerns translating the security logic packed in the form of material requirements, into the design and functional characteristics of an information system. These include, for instance, the data elements collected, the communication network for transmitting the data, or again, the analytic techniques for processing them. In this third phase, the line between designers (e.g. software engineers) and users (e.g. IT analysts) is not always straightforward. The design of an information system is in fact an heterogenous and collaborative process that requires multiple interventions (see also Glouftsios 2019). Fundamentally, the power that is accorded to a technology by "overwriting" their script is the power to produce the security vision. The output(s) can range from risk categories, potential hits in the system, and lists of suspects. This type of power is perhaps the most obscure since it concerns the possibility to process and analyse data through digital tools (e.g. algorithms) whose inner workings are often unintelligible (see Amoore and Raley 2017; Bellanova 2017; Bellanova and De Goede 2020).

To make sense conceptually of this third act of power, I recall two concepts that I discussed in Chapter 1 – "composting" and "computing" data – first proposed by Bellanova and Fuster (2019). Visualising the relational composition of each network in the form of a graph favoured thinking of data in their process of becoming "actionable" elements through computing techniques (Bellanova and Fuster 2019: 346, 358). The juxtaposition of the SIS II, Prüm, API and PNR network visualisations reflected the distinct technical configuration of each infrastructure. With the more or less equal number of inputted nodes (91 – SIS II; 83 and 84 – Prüm; 75 – API; 73 – PNR), the resulting edges in the Prüm, API and PNR network visualisations were by far more numerous compared to the ones in the SIS II (150 SIS II; between 562 and 617 – Prüm; 1153 – API; 1250 – PNR). As already noted in Chapter 5, this finding substantiates the claim about the technical complexity of developing a decentralised

infrastructure of information exchange (Prüm, API and PNR) vis-à-vis a centralised one (SIS II). In the absence of a central component, each actor that participates in the Prüm, API and PNR networks had to establish individual connections with the other operational actors, thus resulting in the higher number of edges that traverse the respective graphs. Conversely, in the SIS II this number was necessarily lower since all the actors are connected directly to the central system rather than among each other. The process of setting up a decentralised architecture then is necessarily more complex and in terms of economic investment the burden is higher at the national level.

However, by remarking such a distinction between centralised and decentralised infrastructures we may be deceived to think that the technical arrangement impacts on the movement of data across the network. Yet data circulate by means of the cycles of uses to which they are subjected, regardless of the differences in the technical arrangement of the infrastructures. Such movement occurs through the connections (edges) that bind each component either to the central system or to other (decentralised) components. What is really crucial in the circulation of data then is their end-use. A specific category of data may be exchanged more than another, and more than once across time. Even the data that have been anonymised, depersonalised or that have decreased in value as a result of risk assessment continue to circulate and thus to cross repeatedly the same trajectories. This characteristic in the circulation of data cannot be rendered through network-like visualizations since tracing the movement across time would require a different kind of software, and thus of visual method, in order to avoid the reproduction of a number of overlapping edges. What is yet crucial is that the movement of data is not unidirectional, from one node to the other. Rather, data move multi-directionally as a result of the creation of multiple cycles of uses. This assertion further validates the application of visual network analysis to the study of the lifecycle of data as a network.

In investigating the role of data across different security infrastructures (e.g. for border and migration management) CSS scholars have devoted much attention to questions about the constitution of data – that is, what is data before and when does it become data? However, on the basis of these findings, it is also crucial, I believe, to understand what happens to data after they are inputted, extracted and used throughout their lifecycles (e.g. as evidence in a court case or in an on-going criminal investigation). Assuming that the cycle of data begins with its "birth", through the collection and entry of data in a database, and ultimately ends with its "death" once it is used would be misleading. The main questions to ask then are: is it possible

to talk about the "death" of data? Are data simply "buried" within information systems, or do they continue to exist but in a different form? What happens to the data that is not transmitted or used, but is yet retained in an information system? These questions are inherently linked to the provisions regarding the depersonalisation, anonymisation, and deletion of data. The regulatory frameworks of the SIS II, Prüm, API and PNR are not straightforward in clarifying the meaning of these terms. This lack of clarity constitutes a major loophole in the legislation that security agencies can potentially exploit in order to open up more and more data for re-use.

Therefore, in terms of data protection, providing an answer to the question of the death of data constitutes quite an urgent task for academic research, which requires to further dig into the "pandora box" of data. Such task goes beyond the scope of this research, yet it is a direction surely worth pursuing. One interesting observation is that every category of data that pertain to the infrastructures considered necessarily outlive the life of the person concerned by the collection. This observation is interrelated with the life of technologies. When we talk about the technical architecture of an information system we are not only referring to the material components that make up its functioning, such as cables, interfaces, screens etc. Rather we are talking about a digital space that exists beyond the physicality of the technology. As the database that stores the data continue to function, so does the data therein, either in an anonymised or depersonalised form. Accordingly, data have an existence of their own that leaves the individual aside. When a person dies, the data continue to live in the practices of the agents that use them. Once inserted in an information system, individual personal traits (e.g. DNA, fingerprints, etc.) can be used for instance to feed risk assessment or threat analysis, or again to assist law enforcement in the definition of patterns of suspicion. Accordingly, even what is not (i.e. depersonalised or anonymised data) informs "in bulk" what should or should not be (i.e. legitimate or suspect).

6.3. The "acts of power" in the lifecycle of data

Overall the result of these three acts of power is the structured possibility to act on the constitution of the space of security. Security is thus multiple and context-dependent on the political vision that informs the set-up of the information infrastructures for exchanging data, their regulatory frameworks, and lastly, their architecture and functional specifications. Yet

agency in itself should not be regarded as the "maker" of security. Whereas it is the possibility to act – *politically*, *materially* and *digitally* – as granted to a multiplicity of (human and non-human) agents, that "does", and hence produces the desired security output. This argument has a number of implications. The main one concerns the conceptualisation of power. Generally, power is represented as dark and obscure since it cannot be observed materially. However, as it is passed on, it is creative of the relations among the various actors, and hence, of the avenues for exchanging data. This entails that power is never local, but rather, it is located only for a limited time with a certain actor, that is, during the act of power. Additionally, the power to "(un-)make" data and in turn to form the fabric of actionable security knowledge is socio-technical since it circulates among an heterogenous set of actors. These are human and non-human agents in the form of regulations and directives (materiality); software developers, engineers, legislators and security authorities (human agents); and, databases, interfaces, cables etc. (technicality).

The second implication concerns how we think about the agency of these actors. Understanding agency as resulting from an act of translation of power implies not only that these agents have their own stake in the making of security, but also that they are capable to "empower" each other. Power is located in a range of documents, databases and in the hands of numerous human actors, but it is never always permanent and/or static. That is, it never resides only with one actor, rather it is first generated *through* the data, it circulates *with* it and it then enables "to act" on the governance of terrorism, mobility, etc. As one attempts to locate power in a certain document, technology or human actor, the danger is to lose the politics that happens in the longer-term. By considering, for example, only documents in the analysis of how security is first imagined and then produced, we would incur in an over-deterministic view of the role of the material. Similarly, the role of technologies in the production of data categories would be overemphasised if we look exclusively at their technical specifications. Whereas all these actors (human and non-human) contribute to structuring the field of security. Therefore, the role of power in the making of security occupies multiple spaces: the *political*, the *material*, and the *digital*. What gets decided through the digital is informed by previous design decisions made by engineers, policy makers, legislators etc. that work in a joint effort to embed the security vision into the architecture and regulatory frameworks of information systems.

Arguing that data can be reassembled and recomposed as many times as the data practices and the normative frameworks that regulate such practices allow for leads to question the circularity

of the lifecycle of data. The multiple (human and non-human) interventions transform the very ontology of data by directly or indirectly triggering different forms of re-use and hence multiple lifecycles. In order to account for these "acts of power" in the lifecycle of data, I propose to upgrade the notion to "disrupted" lifecycle. The term "disruption" points to an event, activity or process that causes disturbance and interferes with the normal arrangement and functioning of an entity – in this case the circulation of data. This conceptual revisitation offers a fresh grasp on the "making" of security through the "(un)making" data. Nevertheless, "disrupting" data does not concern interrupting their cyclical movement across the network. Rather it is about making data move in a certain direction as to enact certain uses. It has thus to do with the acts of power that I have outlined above. The trajectories that data follow are not contingent, neither are they inadvertent, rather they result from the translation of power from one actor to another. This argument is substantiated by the network visualisations of the SIS II, Prüm, API and PNR (Figures 6, 18, 19 and 20). Their graphical representations may not be faithful since they offer a "snapshot" of an (indefinite) moment in time. Yet what is remarkable is that the connections between the nodes are contingent upon the different acts of disruption in the data.

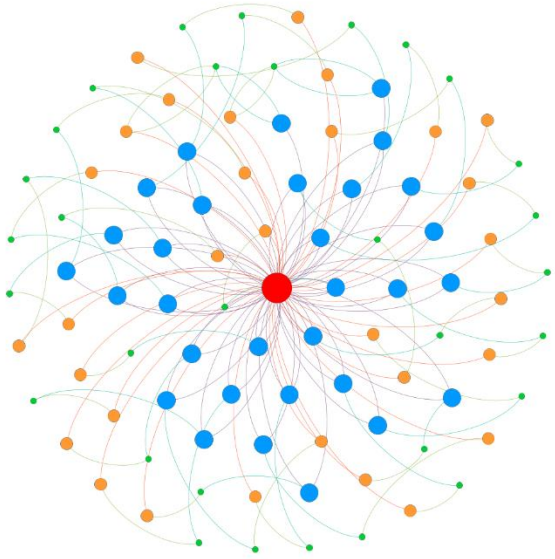

Figure 6. Graphical topology of the SIS II network.

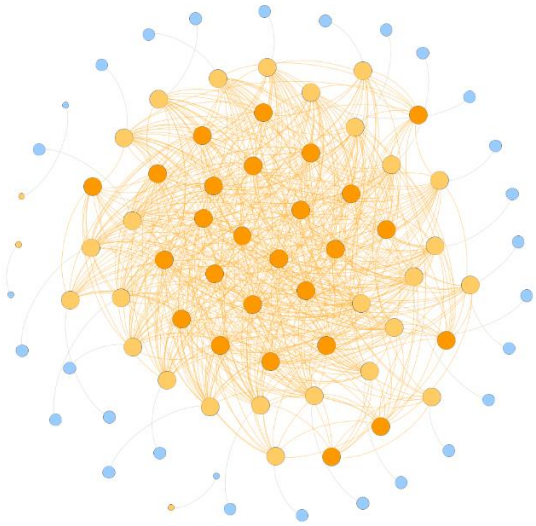

Figure 18. Graphical topology of the Prüm network.

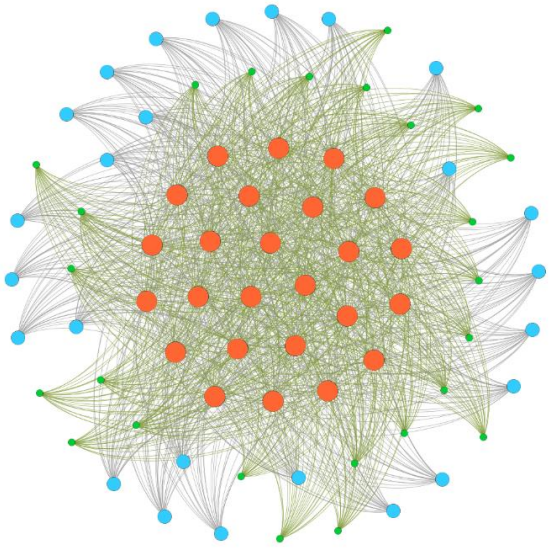

Figure 19. Graphical topology of the API network.

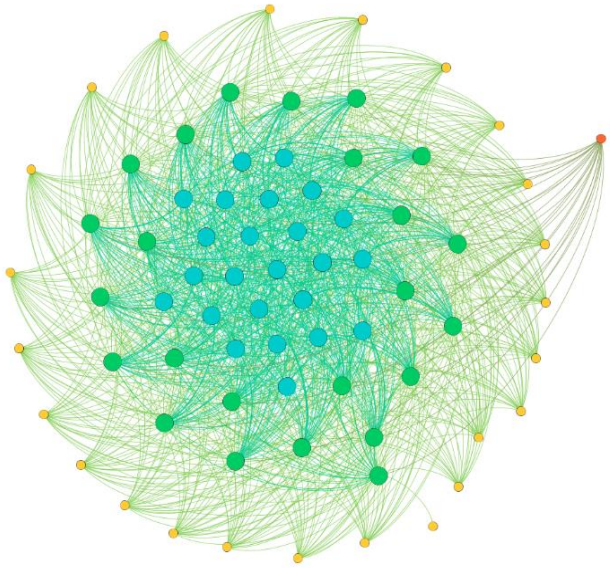

Figure 20. Graphical topology of the PNR network.

Figures 6, 18, 19 and 20 are well suited to represent the lack of order and systematicity in the lifecycle of data. Data are not only messy, but they are also never settled due to the multiple circumstances and purposes for which they can be exchanged. This is immediately visible in the number of trajectories reproduced. What prevails in all the visualisations are the relations between the actors (edges) above the assumed relevance of these actors themselves (nodes). This visual feature suggests that actors do not have the power to make data move across the network. Rather it is the movement of data from one actor to another that "empowers" them to act by creating an intricate network of contingent practices. Therefore, what is central to the composition of the network are the acts of power that occur by means of creating multiple cycles of uses. This observation illustrates the value of examining the relational distribution of a network through a graph. Even more crucially, it exemplifies that by reconstructing the data lifecycle both discursively and visually it is possible to understand how the circulation of data is functional to the enactment of a specific mode of "making" security. In other words, security is produced *through* the making and (un-)making of the categories of data that are collected, stored and exchanged through the various networks. Not only the SIS II, Prüm, API and PNR embody a specific security logic but also they are productive of it through the creation of multiple lifecycles.

Conclusions

Instead of focusing exclusively on databases, IT systems and algorithmic data analysis tools, the focal point of my research was on the data practices related to the gathering, processing and sharing of data and on the provisions that regulate such practices. I developed the empirical analysis by attending to the notion of "data lifecycle": how different forms of data are initially produced and how they are subsequently repurposed for policing purposes. Uncovering this methodologically, I examined the lifecycle of data as a network of practices through a research design based on the methods and tools of document analysis and visual network analysis. Given that the methodological and theoretical approaches favoured in IR in general, and critical security studies in particular, have often proved insufficient to peer into datafication technologies (see Hartong and Förschler 2019; Leese 2014; Matzner 2017), the tentative framework that I sought to advance through this research constitutes a valuable point of departure for the study of digitally-mediated security. The three overlapping dimensions – socio-political, legal and technical – that characterize it involved the conduct of specific analytical tasks that parsed out the analysis of institutional contexts, regulatory frameworks and technical arrangements, in the endeavour to reflect how different modes of "making" security are enacted through the "(un-)making" of different categories of data.

Even more importantly, coming to a visual representation of the data lifecycle suggests that an interesting aspect of the entanglement between security and technology is that they do not operate independently of each other, but rather they exist in a complex relationship to the physicality of data themselves. In this vein, rather than providing a mere account of the functioning and inner workings of AFSJ information systems and related data practices, I sought to question why and how the SIS II, the Prüm, the API and PNR have come to shape our knowledge of security. Addressing these questions invited to reflect on the heterogeneity of the practices and dynamics involved in the production of data for the governance of security issues. The research findings confirmed that this heterogeneity is co-constitutive of the data that are built-in different data infrastructures, of the technical arrangements of information systems and of the actors involved in their design, implementation and use. Thus, while personal data feature as *transversal* solutions to the management of security, I sought to open up a new avenue for inquiring, analysing and examining such *transversality* and its effects on social life. Such inquiry revealed that "securing *through* data" has become an inextricable

aspect of the EU AFSJ information infrastructures that has solidified their embodiment as technological solutions.

Accordingly, we have come to know about security through technology. At the same time, by problematizing how technological products intervene in security, we also strive to find space for human action within an increasing datafied society. Yet the question that emerges is: how is it that we came to engage with the tools and instruments for enacting security in order to make sense of it? Discourses about the entanglements between security and technology are not new. Before, technologies such as drones were conceptualised within the analysis of security dynamics in immaterial terms, as "tools" or "weapons" of war. They were bearing a meaning of power as power to do harm, and not power as agents. Accordingly, their capacity to act was constrained to the limits of those actors that deployed them as means for "doing" security rather than as ends in themselves. As Besters and Brom (2010: 455) note: 'today, information systems make the difference: being admitted to the European Union or not'. They have become increasingly mundane and well embedded in administrative processes of everyday life. However, depictions of information systems among the public are different from depictions of drones, rifles, tanks or other "hard" security tools. Yet individuals are compelled to conform to the norms and procedures at airports in order to be granted the possibility to travel. In Foucauldian terms, only the conformance to the norm legitimises their movement across borders (Matzner 2017; Murakami 2007). Instead of demonstrating "who they are" by claiming their identity, travellers have to demonstrate "who they are not" – that is, suspects, criminals or even terrorists. But for them it is just a matter of being subjected to administrative procedures that streamline their everyday actions.

In terms of depictions of security, what individuals see are barriers, automatic screening at gates, etc., understood as allowing movement across space and time. In other words, they see the "objects" of security without realizing that they are the "targets." The security logic built-into these systems is the logic of the everyday, of the routine, of what is required of us to be considered "good citizens." It is not the logic of the exceptional that is professed to develop them, or that is associated to images of drones. However, both drones and information systems can be conceived not only as technologies that "make" security, but also as "weaponized" technologies in themselves. This misperception of information infrastructures and of the incredible amount of personal data they circulate derives from the impairment of individuals to perceive them as "actants" in structuring the security field. This impairment, in turn, has

resulted in the primacy of technology over security, or rather of security over privacy and freedom. We, as social researchers, are actively contributing to this primacy by constantly emphasising and putting agency on the role of technological systems, and especially on datafication technologies, vis-à-vis the underlying dynamics, such as the "preventive" collection of data, that more directly impact on security governance. Therefore, the mundanity of these infrastructures has inevitably shielded from human eyes their projection as "policing" instruments or as instruments for ensuring "freedom from" *unknown* security threats. The question, indeed, the provocation to the reader is: if security governance is enacted *through* data, how can we "secure" our digital and physical selves *from* data?

Annexes

Annex I, II, III, Council of the European Union (2021b) Implementation of the provisions on information exchange of the "Prüm Decisions", Brussels, 11 October 2021, 5383/4/21 REV 4.

Annex I – DNA Operational Data Exchange

	DNA operational data exchange																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						X							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	
NO																													x

Annex II – Fingerprint Operational Data Exchange

	FP operational data exchange																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				x																									
DE					x																								
EE						x																							
EL							x																						
ES								X																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																												x	
NO																													x

Annex III – VRD Operational Data Exchange

	VRD operational data exchange																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	HR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK	NO
BE	x																												
BG		x																											
CZ			x																										
DK				X																									
DE					x																								
EE						x																							
EL							x																						
ES								x																					
FR									x																				
HR										x																			
IE											x																		
IT												x																	
CY													x																
LV														x															
LT															x														
LU																x													
HU																	x												
MT																		x											
NL																			x										
AT																				x									
PL																					x								
PT																						x							
RO																							x						
SI																								x					
SK																									x				
FI																										x			
SE																											x		
UK																													
NO																													

References

Abrahamsen, R., and Williams, M. C. (2010) *Security Beyond the State: Private Security in International Politics* (Cambridge University Press).

Acuto, M. and Curtis, S. (2014) 'Assemblage Thinking in International Relations', In Acuto, M. and Curtis, S. (eds.) *Reassembling International Theory: Assemblage Thinking and International Relations* (Basingstoke/New York: Palgrave Macmillan): 1–16.

Amankwaa, A. O. (2020) 'Trends in Forensic DNA Database: Transnational Exchange of DNA Data', *Forensic Sciences Research*, 5(1): 8-14.

Amoore, L. (2008) 'Governing by Identity', In Bennett, C.J. and Lyon, D. (eds) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective* (London: Routledge).

Amoore, L. (2013) *The Politics of Possibility: Risk and Uncertainty Beyond Probability* (Durham, NC: Duke University Press).

Amoore, L. (2014) 'Security and the Incalculable', *Security Dialogue*, 45(5): 423-439.

Amoore, L. and De Goede, M. (2005) 'Governance, Risk and Dataveillance in The War on Terror', *Crime, Law & Social Change*, 43: 149-173.

Amoore, L. and Raley, R. (2017) 'Securing with Algorithms: Knowledge, Decision, Sovereignty', *Security Dialogue*, 48(1): 3-10.

Aradau, C. and Blanke, T. (2015) 'The (Big) Data-Security Assemblage: Knowledge and Critique', *Big Data & Society*, 2(2): 1-12.

Aradau, C. and Blanke, T. (2017a) 'Politics of Prediction', *European Journal of Social Theory*, 20(3): 373-91.

Aradau, C. and Blanke, T. (2017b) 'Governing Others: Anomaly and the Algorithmic Subject of Security', *European Journal of International Security*, 3(1): 1-21.

Article 29 Data Protection Working Party and Working Party on Police and Justice (2007) Joint opinion on the proposal for a Council Framework Decision on the use of Passenger

Name Record (PNR) for law enforcement purposes, presented by the Commission on 6 November 2007, 02422/07/EN. Adopted on 5 December 2007 by the Article 29 Working Party and on 18 December 2007 by the Working Party on Police and Justice. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp145_en.pdf

Article 29 Working Party (2011) Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (WP181, adopted on 5 April 2011). Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf

Attride-Stirling, J. (2001) 'Thematic Networks: An Analytic Tool for Qualitative Research', *Qualitative Research*, 1(3): 385–405.

Austin, J. L. (2019) 'Towards an International Political Ergonomics', *European Journal of International Relations*, 25(4): 979–1006.

Austin, J. L., and Leander, A. (2021) 'Designing-With/In World Politics', *Political Anthropological Research on International Social Sciences (PARISS)*, 2(1): 83-154.

Aykut, S., Demortain, D., and Benbouzid, B. (2019) 'The Politics of Anticipatory Expertise: Plurality and Contestation of Futures Knowledge in Governance', *Science & Technology Studies: Special Issue*, 32(4): 2-12.

Balzacq, T., Bigo, D., Carrera, S., et al. (2006) 'Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats', *CEPS Working Document no. 234*, Brussels.

Balzacq, T. and Hadfield, A. (2012) 'Differentiation and Trust: Prüm and the Institutional Design of EU Internal Security', *Cooperation and Conflict*, 47(4): 539-561.

Barad, K. (2007) *Meeting the Universe Halfway. Quantum Physics and the Entanglement of Matter and Meaning* (Durham: Duke University Press).

Bellanova, R. (2008) 'The 'Prüm Process': The Way Forward for Police Cooperation and Data Exchange?', In Guild, E. and Geyer, F. (eds) *Security vs. Justice? Police and Judicial Cooperation in the European Union* (Aldershot: Ashgate): 203–221.

Bellanova, R. (2017) 'Digital, Politics, and Algorithms: Governing Digital Data Through the Lens of Data Protection', *European Journal of Social Theory*, 20(3): 329–347.

Bellanova, R. and Duez, D. (2012) 'A Different View on the "Making" of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage', *European Foreign Affairs Review*, 17(2/1): 109–124.

Bellanova, R. and Fuster, G. (2019) 'Composting and Computing: On Digital Security Compositions', *European Journal of International Security*, 4(3): 345–365.

Bellanova, R. and De Goede, M. (2020) 'The Algorithmic Regulation of Security: An Infrastructural Perspective', *Regulation & Governance*, 16(1): 102-118.

Bellanova, R. and Glouftsios, G. (2020) 'Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance', *Geopolitics*, 27(1): 160-184.

Beslay, L. and Galbally Herrero, J. (2015) 'Fingerprint Identification Technology for its Implementation in the Schengen Information System II (SIS-II)', *EUR 27473. Luxembourg (Luxembourg): Publications Office of the European Union* (JRC97779).

Besters, M. and Brom W. A., F. (2010) ''Greedy' Information Technology: The Digitalization of the European Migration Policy', *European Journal of Migration and Law*, (12): 455-470.

Bigo, D. (1996) *Polices en Réseaux: l'Expérience Européenne* (Presse de Sciences Po, Paris).

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): 209–25.

Bigo, D. and Carrera, S. (2004) 'From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU', *CEPS Commentary*.

Bigo, D., Carrera, S. and Guild, E. (2009) 'The Challenge Project: Final Policy Recommendations on the Changing Landscape of European Liberty and Security', *Challenge Research Paper No.16*.

Bigo, D., Isin, E., and Ruppert, E. (2019) *Data Politics: Worlds, Subjects, Rights* (London: Routledge).

Bonditti, P., Neal, A., Opitz, S., and Zebrowski, C. (2014) 'Genealogy' in Aradau, C., Huysmans, J., Neal, A., and Voelkner, N. (eds.), *Critical Security Methods: New Frameworks for Analysis* (New York: Routledge): 159-188.

Bonelli, L. and Ragazzi, F. (2014) 'Low-tech Security: Files, Notes, and Memos as Technologies of Anticipation', *Security Dialogue*, 45(5): 476–493.

Broeders, D. and Dijstelbloem, H. (2016) 'The Datafication of Mobility and Migration Management: the Mediating State and its Consequences', In Van der Ploeg, I. and Pridmore, J. (eds.) *Digitizing Identities: Doing Identity in a Networked World* (London: Routledge): 242-260.

Bueger, C. and Gadinger, F. (2018) *International Practice Theory* (2nd Edition, Palgrave Macmillan).

Bunyan, T. (2010) 'Just Over the Horizon – the Surveillance Society and the State in the EU', *Race and Class*, 51(3): 1–12.

Butler, J. M. (2006) 'Genetics and Genomics of Core STR Loci Used in Human Identity Testing', *Journal of Forensic Science*, 51(2): 253–265.

Campbell, Z. and Jones, C. (2020) 'Leaked Reports Show EU Police are Planning a Pan-European Network of Facial Recognition Databases', *The Intercept*, 21 February 2020 (online source). Available at: https://theintercept.com/2020/02/21/eu-facial-recognition-database/

Cavelty, M. D. and Leese, M. (2018) 'Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity', *European Review of International Studies,* 5(3): 49-69.

Commission of the European Communities (2001) Communication to the Council and the European parliament on the Development of the Schengen Information System II, 18 December 2001, COM(2011) 720 final.

Commission of the European Communities (2003) Commission Staff Working Paper on the Development of the Second Generation Schengen Information System (SIS II), 2002 Progress Report, Brussels, 18 February 2003, SEC (2003) 206 final.

Commission of the European Communities (2005) Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, Brussels, 12 October 2005.

Contini, F. (2009) 'ICT, Assemblages and Institutional Contexts: Understanding Multiple Development Paths, in *ICT and Innovation in the Public Sector: European Studies in the Making of E-government*, (eds.) Contini, F. and Lanzara, G. F. (Basingstoke: Palgrave Macmillan): 244-271.

Costa, S. (2020) 'Travelling to Prüm – Euphoria and Dysphoria Regarding the Use of DNA Data Between and Beyond Borders', *Crime, Law & Social Change*, 73: 551-573.

Côté-Boucher, K. (2020) *Border Frictions: Gender, Generation and Technology on the Frontline* (Routledge).

Council of Europe (2018) Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications. Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET), March 2018. Available at: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

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

Council of the European Union (2003) Doc. Nr. 6387/03: Summary of discussions, 25 February 2003.

Council of the European Union (2004) *SIS II Functions/Open Issues*, Brussels, 30 November 2004, 12573/3/04.

Council of the European Union (2005) Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation ("Prüm Convention"), Brussels, 7 July 2005, 10900/05.

Council of the European Union (2011) Implementation of the Prüm Decisions – Lessons Learned, Brussels, 20 December 2011, 18676/11.

Council of the European Union (2016) Implementation of the Provisions on Information Exchange of the "Prüm Decisions", Brussels, 4 May 2016, 5017/3/16 REV 3.

Council of the European Union (2017) Implementation of the Provisions on Information Exchange of the "Prüm Decisions", Brussels, 22 May 2017, 5081/2/12 REV 2.

Council of the European Union (2018a) Draft Council Conclusions on strengthening the cooperation and the use of the Schengen Information System (SIS) to deal with persons involved in terrorism or terrorism-related activities, including foreign terrorist fighters – Adoption, Brussels, 18 May 2018, 8974/18.

Council of the European Union (2018b) Draft Council Conclusions on the implementation of the "Prüm Decisions" ten years after their adoption, Brussels, 5 July 2018, 10550/18 – Annex.

Council of the European Union (2018c) Council Conclusions on the implementation of the "Prüm Decisions" ten years after their adoption, Brussels, 18 July 2018, 11227/18.

Council of the European Union (2019a) Next generation Prüm (Prum.ng) – Reports from focus groups / Report on face recognition, Brussels, 30 October 2019, 13356/19.

Council of the European Union (2019b) Council conclusions on widening the scope of the use of passenger name record (PNR) data to forms of transport other than air traffic – Council conclusions, Brussels, 2 December 2019, 14746/19.

Council of the European Union (2021a) Proposal for the possible inclusion of national databases on firearms and their owners in the future Prüm framework, Brussels, 16 February 2021, 5787/21.

Council of the European Union (2021b) Implementation of the Provisions on Information Exchange of the "Prüm Decisions", Brussels, 11 October 2021, 5383/4/21 REV 4.

Court of Justice of the European Union (2017) Opinion 1/15 of 26 July 2017 on the draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. Press Release No. 84/17, Luxembourg, 26 July 2017.

Court of Justice of the European Union (2022) Judgment of the Court in Case C-817/19, *Ligue des droits humains*, Press Release No. 105/22, Luxembourg, 21 June 2022.

Crossley, N. (2015) 'Relational Sociology and Culture: A Preliminary Framework', *International Review of Sociology*, 25(1): 65–85.

Cukier, K. and Mayer-Schoenberger, V. (2013) 'The Rise of Big Data: How It's Changing the Way We Think About the World', *Foreign Affairs*, 92(3): 28-40.

Davidshofer, S.; Jeandesboz, J. and Ragazzi, F. (2017) 'Technology and Security Practices: Situating the Technological Imperative', In *International Political Sociology: Transversal Lines* (eds.) Basaran, T.; Bigo, D.; Guittet, E. P.; and Walker, R. B. J. (London; New York: Routledge): 205-227.

Decuypere, M. (2020) 'Visual Network Analysis: A Qualitative Method for Researching Sociomaterial Practice', *Qualitative Research*, 20(1): 73–90.

Decuypere, M. and Simons, M. (2016) 'Relational Thinking in Education: Topology, Sociomaterial Approaches and Figures', *Pedagogy, Culture & Society*, 24(3): 371–386.

De Goede, M. (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies* (NED-New Edition. University of Minnesota Press).

De Goede, M. (2018) 'The Chain of Security', *Review of International Studies*, 44(1): 24–42.

De Goede, M., Simon, S., and Hoijtink, M. (2014) 'Performing Preemption', *Security Dialogue*, 45(5): 411–422.

Deloitte (2015) on behalf of the European Commission, 'Study on the implementation of the European Information Exchange Model (EIXM) for strengthening law enforcement

cooperation', Final Report, 26 January 2015. Available at: https://www.statewatch.org/media/documents/news/2015/feb/eixm-study.pdf

Deloitte (2020) on behalf of the European Commission, 'Study on the feasibility of improving information exchange under the Prüm Decisions', Final Report, May 2020. Available at: https://www.statewatch.org/media/1385/eu-com-prum-expansion-study-final-report-5-20.pdf

Derrida, J. and Caputo, J. D. (1997) *Deconstruction in a Nutshell: A Conversation with Jacques Derrida* (New York: Fordham University Press).

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

Dijstelbloem, H., Van Reekum, R., and Schinkel, W. (2017) 'Surveillance at Sea: The Transactional Politics of Border Control in the Aegean', *Security Dialogue*, 48(3): 224–240.

Donohue, L. K. (2014) 'Bulk Metadata Collection: Statutory and Constitutional Considerations', *Harvard Journal of Law & Public Policy*, 37(3): 759-900.

Douglas, D. G. (2012) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (eds.) Bijker, W., Hughes, T., and Pinch, T., (The MIT Press).

Dyson, K. and Sepos, A. (2010) 'Differentiation as Design Principle and as Tool in the Political Management of European Integration', In Dyson, K. and Sepos, A. (eds) *Which Europe? The Politics of Differentiated Integration* (Basingstoke: Palgrave Macmillan): 3–23.

Ecofin Council (2002) Council Conclusions 10089/02 (Presse 181), Madrid, 20 June 2002, 2442nd Council Meeting.

Egbert, S. and Leese, M. (2020) *Criminal futures: Predictive Policing and Everyday Police Work* (Routledge).

eu-LISA (2019) SIS II 2018 Annual Statistics, Tallin: eu-LISA, March 2020.

eu-LISA (2020) SIS II 2019 Annual Statistics, Tallin: eu-LISA, March 2021.

eu-LISA (2022a) SIS II 2021 Annual Statistics, Tallin: eu-LISA, March 2022.

eu-LISA (2022b) Report on the technical functioning of Central SIS II 2019-2020, May 2022.

European Commission (2010) Overview of Information Management in the Area of Freedom, Security and Justice, Brussels, 20 July 2010, COM(2010) 385 final.

European Commission (2011a) Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 2 February 2011, COM(2011) 32 final.

European Commission (2011b) Staff Working Paper, Impact Assessment, Accompanying document to the Proposal for a European Parliament and Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 2 February 2011, SEC(2011) 132 final.

European Commission (2013) Schengen Information System (SIS II) Goes Live, Brussels, 9 April 2013 (online source). Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_13_309

European Commission (2016a) Communication from the Commission to the European Parliament and the Council on Stronger and Smarter Information Systems for Borders and Security, Brussels, 6 April 2016, COM(2016) 205 final.

European Commission (2016b) Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, Brussels, 21 December 2016, 2016/0407 (COD) COM(2016) 881 final.

European Commission (2016c) Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, Brussels, 21 December 2016, 2016/0409 (COD), COM(2016) 881 final.

European Commission (2016d) Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, Brussels, 21 December 2016, COM(2016) 882 final.

European Commission (2016e) Proposal for a 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, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, Brussels, 21 December 2016, COM(2016) 883 final.

European Commission (2018) Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17 April 2018, COM(2018) 225 final.

European Commission (2020a) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'A European Strategy for Data', Brussels, 19 February 2020, COM(2020) 66 final.

European Commission (2020b) Report to the European Parliament and the Council on the Review of Directive 2016/681 on the use of passenger name record (PNR) data for prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 24 July 2020, COM(2020) 305.

European Commission (2020c) Strengthening the automated data exchange under the Prüm framework, Combined Evaluation Roadmap/Inception Impact Assessment, Ref. Ares(2020) 4214748, 11 August 2020.

European Commission (2020d) Staff Working Document. Evaluation of the Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (API Directive), Brussels, 8 September 2020, SWD(2020) 174 final.

European Commission (2020e) Consultation Strategy for the initiative on strengthening the automated data exchange under the Prüm framework, October 2020. https://home-affairs.ec.europa.eu/system/files/2020-10/20200924_consultation_strategy_final.pdf

European Commission (2020f) Proposal for a Regulation of the European Parliament and of the Council on European Data Governance ("Data Governance Act"), Brussels, 25 November 2020, COM (2020) 767.

European Commission (2020g) Proposal for a Regulation of the European Parliament and of the Council amending 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 as regards the entry of alerts by Europol, Brussels, 9 December 2020, COM/2020/791 final.

European Commission (2021a) Report from the Commission to the European Parliament and the Council on the implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (the 'Prüm Decision'), Brussels, 7 December 2021, COM(2012) 732 final.

European Commission (2021b) Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council, Brussels, 8 December 2021, COM/2021/784 final.

European Commission (2022a) Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC, Strasbourg, 13 December 2022, COM/2022/729 final.

European Commission (2022b) Proposal for a Regulation of the European Parliament and of the Council on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious

crime, and amending Regulation (EU) 2019/818, Strasbourg, 13 December 2022, COM(2022) 731 final.

European Council (2011) European Council 23/24 June 2011 Conclusions, Brussels, 24 June 2011, EUCO 23/11, 14 concl. 4.

European Council (2015) Conclusions of 25 and 26 June 2015 (ST 22 2015 INIT), Brussels, 26 June 2015, EUCO 22/15.

European Data Protection Supervisor (EDPS) (2007) Opinion of the European Data Protection Supervisor (EDPS) on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 21 July 2007.

European Digital Rights (EDRi) (2020) Feedback to the Roadmap to strengthen the automated data exchange under the Prüm framework, 6 October 2020.

European Parliament (1999) Presidency Conclusions, Tampere European Council, 15 And 16 October 1999. Available at: https://www.europarl.europa.eu/summits/tam_en.htm

European Parliamentary Research Service (2018) Revision of the Schengen Information System for Law Enforcement. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599343/EPRS_BRI(2017)599343_EN.pdf

Faure-Atger, A. (2008) 'The Abolition of Internal Border Checks in an Enlarged Schengen Area', *CHALLENGE Research Paper No.8*, Centre for European Policy Studies.

Fenwick, T. and Edwards, R. (2010) *Actor-Network Theory in Education* (London: Routledge).

Forsyth, B. (2015) 'Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection', *Washington and Lee Law Review*, 72(3): 1307-1341.

Fruchterman, T. M. J. and Reingold, E. M. (1991) 'Graph Drawing by Force Directed Placement', *Software – Practice and Experience*, 21(11): 1129-1164.

Gabrys, J. (2019) 'Data Citizens. How to Reinvent Rights', in Bigo, D., Isin, E., Ruppert, E., *Data Politics: Worlds, Subjects, Rights* (London: Routledge): 248-266.

Gaisbauer, H. P. (2013) 'Evolving Patterns of Internal Security Cooperation: Lessons from the Schengen and Prüm Laboratories', *European Security*, 22(2): 185-201.

Glouftsios, G. (2018) 'Governing Circulation through Technology within EU Border Security Practice-Networks', *Mobilities*, 13(2): 185-99.

Glouftsios, G. (2019) 'Designing Digital Borders. The Visa Information System (VIS)', in Hoijtink, M. and Leese, M. (eds.) *Technology and Agency in International Relations* (London: Routledge).

Glouftsios, G. (2021) 'Governing Border Security Infrastructures: Maintaining Large-Scale Information Systems', *Security Dialogue*, 52(5): 452–470.

Glouftsios, G. and Scheel, S. (2021) 'An Inquiry into the Digitisation of Border and Migration Management: Performativity, Contestation and Heterogeneous Engineering', *Third World Quarterly*, 42(1): 123-140.

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

Gray, J., Gerlitz, C. and Bounegru, L. (2018) 'Data Infrastructure Literacy', *Big Data and Society*, 5(2): 1–13.

Guild, E., Carrera, S. and Eggenschwiler, A. (2009) 'Informing the Borders Debate', *CEPS Background Briefing* (Paris: CEPS).

Haggerty, K. D. and Ericson, R. V. (2000) 'The Surveillant Assemblage', *British Journal of Sociology*, 51(4): 605-22.

Hall, A. (2017) 'Decisions at the Data Border: Discretion, Discernment and Security', *Security Dialogue*, 48(6): 488–504.

Hansen, L. (2006) *Security as Practice: Discourse Analysis and the Bosnian War* (New York: Routledge).

Hanseth, O., and Lyytinen, K. (2010) 'Design Theory for Dynamic Complexity in Information Infrastructures: The Case of Building Internet', *Journal of Information Technology*, 25(1): 1–19.

Hartong, S. and Förschler, A. (2019), 'Opening the Black Box of Data-based School Monitoring: Data infrastructures, Flows and Practices in State Education Agencies', *Big Data & Society*, 6(1): 1-12.

Hayes, B. (2008) 'EU-SIS Schengen Information System Article 99 report: 33,541 people registered in SIS for surveillance and checks', *Statewatch Analysis*, 10(4): 1-5.

Hazou, E. (2022) 'Cyprus Approved Access to Schengen Information on People Entering the Country', May 3, 2022 (online source). https://cyprus-mail.com/2022/05/03/cyprus-approved-access-to-schengen-information-on-people-entering-the-country/

Hoijtink, M. and Leese, M. (2019) *Technology and Agency in International Relations*, (London: Routledge).

Hu, Y. (2005) 'Efficient and High Quality Force-Directed Graph Drawing', *Mathematica Journal*, 10(1): 37-71.

Innes, M. (2001) 'Control Creep', *Sociological Research Online*, 6(3): 13–18.

International Civil Aviation Organization (ICAO) (2010) Guidelines on Passenger Name Record (PNR) Data, Doc. 9944, First Edition, Montreal. Available at: https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf

ICAO (2013a) Proposal for an ICAO Traveller Identification Programme (ICAO TRIP) Strategy, Working Paper, A38-WP/11, Assembly – 38th session, 17 May 2013. Available at: https://www.icao.int/Meetings/a38/Documents/WP/wp011_en.pdf

ICAO (2015) Machine Readable Travel Documents, Doc 9303, 7th Edition, Montreal. Available at: https://www.icao.int/publications/pages/publication.aspx?docnum=9303

ICAO (2016) The Bigger Picture: Traveller Identification, ICAO TRIP Magazine, (11)1. Available at: https://www.icao.int/publications/journalsreports/2016/TRIP_Vol11_No1.pdf

ICAO (2017a) Adoption of Amendment 26 to Annex 9, ICAO State Letter No. EC 6/3-17/88, 14 July 2017. Available at: https://www.icao.int/Meetings/FALP/Documents/FALP10-2018/SL17.88.EN.pdf

ICAO (2017b) Annex 9 to the Convention on International Civil Aviation, Facilitation, Fifteenth Edition, Montreal, October 2017. Available at: https://www.icao.int/WACAF/Documents/Meetings/2018/FAL-IMPLEMENTATION/an09_cons.pdf

Jacomy, M., Venturini, T., Heymann, S. and Bastian, M. (2014) 'ForceAtlas2, A Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software', *PLoS ONE*, 9(6): e98679.

Jakubowska, E. and Naranjo, D. (2020) 'Ban Biometric Mass Surveillance. A Set of Fundamental Rights Demands for the European Commission and EU Member States', Brussels, 13 May 2020 (on behalf of European Digital Rights, EDRi). https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Janssen, M. and Kuk, G. (2016) 'The Challenges and Limits of Big Data Algorithms in Technocratic Governance', *Government Information Quarterly*, 33(3): 371-377.

Jasanoff, S. (ed.) (2004) *States of Knowledge: The Co-Production of Science and Social Order* (London/New York: Routledge).

Jeandesboz, J. (2010) 'Logiques et Pratiques de Contrôle et de Surveillance des frontières de l'Union européenne', In A. Scherrer, E. Guittet and D. Bigo (eds.) *Mobilités sous Surveillance: Perspectives Croisées UE-Canada* (Paris, Cultures et Conflits).

Jeandesboz, J. (2016) 'Smartening Border Security In The European Union: An Associational Inquiry', *Security Dialogue*, 47(4): 292-309.

Johnson, D., Ludwig, A., Younger, B. (2015) 'The Prüm Implementation, Evaluation and Strengthening (PIES) of forensic DNA data exchange', *Northumbria University Final Report* (Newcastle Upon Tyne: Northumbria University).

Jones, C. (2011) 'Implementing the "Principle of Availability": The European Criminal Records Information System, The European Police Records Index System, The Information Exchange Platform for Law Enforcement Authorities, *Statewatch Analysis*, 1 September 2011. https://www.statewatch.org/media/documents/analyses/no-145-ecris-epris-ixp.pdf

Jones, C. (2012) 'Complex, Technologically Fraught and Expensive: The Problematic Implementation of the Prüm Decision', *Statewatch Analysis*, 7 September 2012. https://www.statewatch.org/media/documents/analyses/no-197-prum-implementation.pdf

Kaufmann, M. (2019) 'Who Connects the Dots? Agents and Agency in Predictive Policing', In Hoijtink, M. and Leese, M. (eds.) *Technology and Agency in International Relations*, (London: Routledge): 141-163.

Kaufmann, M. (2020) 'Vocations, Visions and Vitalities of Data Analysis. An Introduction', *Information, Communication & Society*, 23(14): 1981-1995.

Kaufmann, M., Egbert, S. and Leese, M. (2019) 'Predictive Policing and the Politics of Patterns', *The British Journal of Criminology*, 59(3): 674–692.

Kaufmann, M., and Leese, M. (2021) 'Information In-Formation: Algorithmic Policing and the Life of Data', In Završnik, A., Badalič, V. (eds) Automating Crime Prevention, Surveillance, and Military Operations (Springer, Cham).

Kierkegaard, S. (2008) 'The Prüm Decision – An Uncontrolled Fishing Expedition in 'Big Brother' Europe', *Computer Law and Security Report*, 24(3): 243-252.

Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (London: SAGE).

Knox, H., Savage, M. and Harvey, P. (2006) 'Social Networks and the Study of Relations: Networks as Method, Metaphor and Form', *Economy and Society*, 35(1): 113–140.

Korff, D. (2015) Passenger Name Records, Data Mining and Data Protection: the Need for Strong Safeguards (Council of Europe), Strasbourg, 15 June 2015, T-PD(2015)11.

Korff, D. and Brown, I. (2011) 'Social media and human rights', in *Human rights and a Changing Media Landscape* (Council of Europe Publications): 175-207.

Lahneman, W. J. (2016) 'IC Data Mining in the Post-Snowden Era', *International Journal of Intelligence and Counter-Intelligence*, 29(4): 700-23.

Lanzara, G. F. (2009) 'Building Digital Institutions: ICT and the Rise of Assemblages in Government', in *ICT and Innovation in the Public Sector: European Studies in the Making of E-government*, (eds.) Contini, F. and Lanzara G.F. (Basingstoke: Palgrave Macmillan): 9-47.

Latour, B. (2005) *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press).

Latour, B., Jensen, P., Venturini, T., Grauwin, S. and Boulier, D. (2012) 'The Whole is Always Smaller Than its Parts' – A Digital Test of Gabriel Tardes' Monads, *British Journal of Sociology*, 63(4): 590–615.

Law, J. (1987) *Technology and Heterogeneous Engineering: The Case of Portuguese Expansion* (MIT Press).

Law, J. (1992) 'Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity', *Systems Practice*, (5): 379–393.

Law, J. (2008) 'Actor Network Theory and Material Semiotics', In *The New Blackwell Companion to Social Theory* (eds.) Turner, B. S.. Available at http://www.heterogeneities. net/publications/Law2007ANTandMaterialSemiotics.pdf

Layton, E. (1977) 'Conditions of Technological Development', In Spiegel-Rösing, I. and De Solla Price, D. (eds.) *Science, Technology and Society: A Cross-Disciplinary Perspective* (London and Beverly Hills: Sage): 197 – 222.

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. (2015) '"We Were Taken by Surprise": Body Scanners, Technology Adjustment, and the Eradication of Failure', *Critical Studies on Security*, 3(3): 269–282.

Leese, M. and Wittendorp, S. (2017) *Security/Mobility: Politics of Movement* (Manchester University Press).

Leese, M. and Hoijtink, M. (2019) 'How (Not) to Talk about Technology. International Relations and The Question of Agency', In Hoijtink, M. and Leese, M., (eds.) *Technology and Agency in International Relations* (London: Routledge): 1-23.

Lindskov J., K. and Monsees, L. (2019) 'Co-Production. The Study of Productive Processes at the Level of Materiality and Discourse', In Hoijtink, M. and Leese, M., (eds.) *Technology and Agency in International Relations*, (London: Routledge): 24-41.

Lobo-Guerrero, L. (2012) 'Archives', In Salter, M. B., and Mutlu, C. E. (eds.) *Research Methods in Critical Security Studies: An Introduction* (New York: Routledge): 121-124.

Logan, S. (2017) 'The Needle and the Damage Done: Of Haystacks and Anxious Panopticons', *Big Data & Society*, 4(2): 1-13.

Luif, P. (2007) 'The Treaty of Prüm: A Replay of Schengen?', In *European Union Studies Association, Tenth Biennial International Conference* (Montreal, Canada). http://aei.pitt.edu/id/eprint/7953

Lupton, D. (2015) 'Lively Data, Social Fitness and Biovalue: The Intersections of Health Self-Tracking and Social Media', *SSRN Electronic Journal*. http://doi.org/10.2139/ssrn.2666324

Lupton, D. (2016) 'Digital Companion Species and Eating Data: Implications for Theorising Digital Data-Human Assemblages, *Big Data & Society*, 3(1): 1–5.

Lyon, D. (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, (London: Routledge).

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique', *Big Data and Society*, 1(2): 1-13.

Lyon, D. (2016) 'Big Data Surveillance: Snowden, Everyday Practices and Digital Futures', In Basaran, T.; Bigo, D.; Guittet, E. P.; and Walker, R. B. J., (eds.) *International Political Sociology: Transversal Lines* (London; New York: Routledge): 254-271.

Machado, H. and Granja, R. (2018) 'Ethics in Transnational Forensic DNA Data Exchange in the EU: Constructing Boundaries and Managing Controversies', *Science as Culture*, 27(2): 242-264.

Machado, H. and Granja, R. (2019) 'Risks and Benefits of Transnational Exchange of Forensic DNA Data in the EU: The Views of Professionals Operating the Prüm System', *Journal of Forensic and Legal Medicine*, 68: 1-7.

Machado, H. and Granja, R. (2020) 'Forensic Genetics and Governance of Transnational Criminality', In *Forensic Genetics in the Governance of Crime* (Palgrave Pivot: Singapore).

Maguire, M., Rao, U. and Zurawski, N. (2018) *Body as Evidence: Security, Knowledge, and Power* (Durham: Duke University Press).

Martins, B. O. and Jumbert, M. G. (2020) 'EU Border Technologies and the Co-production of Security 'Problems' and 'Solutions'', *Journal of Ethnic and Migration Studies*, 48(6): 1430-1447.

Matos, S. (2019) 'Privacy and Data Protection in the Surveillance Society: The Case of the Prüm System', *Journal of Forensic and Legal Medicine*, 66: 155-161.

Matzner, T. (2016) 'Beyond Data As Representation: The Performativity Of Big Data In Surveillance', *Surveillance & Society*, 14(2): 197-210.

Matzner, T. (2017) 'Opening Black Boxes Is Not Enough – Data-based Surveillance In *Discipline and Punish* and Today', *Foucault Studies*, 23: 27-45.

McCartney, C., Wilson J., T. and Williams, R. (2011) 'Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability', *Eur J Crim Policy Res*, 17: 305–322.

McCulloch, J. and Pickering, S. (2009) 'Pre-Crime and Counter-Terrorism', *The British Journal of Criminology*, 49(5): 628-45.

Mitsilegas, V. (2007) 'Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance', in A. Baldaccini, E. Guild and H. Toner (eds.) *Whose freedom, Security and Justice? EU Immigration and Asylum Law and Policy* (Oxford: Hart Publishing).

Mol, A. (2002) *The Body Multiple: Ontology in Medical Practice* (Durham: Duke University Press).

Mol, A. (2008) 'I Eat an Apple. On Theorizing Subjectivities', *Subjectivity,* 22: 28–37.

Mol, A. (2010) 'Actor-Network Theory: Sensitive Terms and Enduring Tensions', *Kölner Zeitschrift für Soziologie und Sozialpsychologie,* 50(1): 253–69.

Monroy, M. (2018) 'Sharp Increase of Secret Alerts in the Schengen Information System', March 1 (online source). https://digit.site36.net/2018/03/01/sharp-increase-of-secret-alerts-in-the-schengen-information-system/

Murakami, D. W. (2007) 'Beyond The Panopticon? Foucault and Surveillance Studies', In Crampton, J. and Elden, S., (eds.) *Space, Knowledge and Power: Foucault and Geography*, (Aldershot: Ashgate): 245-63.

Mutlu, C. E. (2012) 'The Material Turn – Introduction', In Salter, M. B., and Mutlu, C. E. (eds.) *Research Methods in Critical Security Studies: An Introduction* (New York: Routledge).

Mutlu, C.E. and Salter, M. B. (2012) 'The Discursive Turn', In Salter, M. B., and Mutlu, C. E. (eds.) *Research Methods in Critical Security Studies: An Introduction* (New York: Routledge).

Nyman, J. (2016) 'Pragmatism, Practice and the Value of Security', In Nyman, J. and Burke, A. (eds) *Ethical Security Studies* (London and New York: Routledge): 131–144.

Offenhuber, D. (2010) 'Visual Anecdote', *Leonardo,* 43(4): 367–374.

Official Journal of the European Union (OJEU) (1995a) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 23 November 1995, L 281, pp. 31-50.

OJEU (1995b) Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), 27 November 1995, C 316, pp. 1-32.

OJEU (1998) Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, 23 January 1998, C 24, pp. 2-22.

OJEU (1999) Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen acquis for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the acquis, 10 July 1999, L 176, pp. 1-16.

OJEU (2000a) Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 22 September 2000, L 239, pp. 19–62.

OJEU (2000b) The Schengen Acquis – Decision of the Executive Committee of 7 October 1997 on the development of the SIS (SCH/Com-ex (97) 24), 22 September 2000, L 239, pp. 442-443.

OJEU (2004) Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data ("API Directive"), 6 August 2004, L 261, pp. 24-27.

OJEU (2005a) The Hague Programme: Strengthening Freedom, Security and Justice in the European Union, 3 March 2005, C 53, pp. 1–14.

OJEU (2005b) Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, 29 September 2005, L 253, pp. 22–24.

OJEU (2006a) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public

communications networks and amending Directive 2002/58/EC ("Data Retention Directive"), 13 April 2006, L 105, pp. 54-63.

OJEU (2006b) Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the second-generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, 28 December 2006, L 381, pp. 1-3.

OJEU (2006c) Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), 28 December 2006, L 381, pp. 4-23.

OJEU (2006d) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU ("Swedish Initiative"), 29 December 2006, L 386, pp. 89-100.

OJEU (2007a) Commission Decision 2007/171/EC of 16 March 2007 laying down the network requirements for the Schengen Information System II (3rd pillar), 20 March 2007, L 79, pp. 29-37.

OJEU (2007b) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), 7 August 2007, L 205, pp. 63–84.

OJEU (2007c) Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon on 13 December 2007, 17 December 2007, C 306, pp. 1-271.

OJEU (2008a) Commission Decision 2008/334/JHA of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II), 8 May 2008, L 123, pp. 39-75.

OJEU (2008b) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 6 August 2008, L 210, pp. 1–11.

OJEU (2008c) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 6 August 2008, L 210, pp. 12-72.

OJEU (2008d) Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals, 24 December 2008, L 348, pp. 98-107.

OJEU (2010a) Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure, 5 May 2010, L 112, pp. 31-37.

OJEU (2010b) Council Decision 2010/482/EU of 26 July 2010 on the conclusion of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/516/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Annex thereto, 9 September 2010, L 238, pp. 1-2.

OJEU (2011) Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice, 1 November 2011, L 286, pp. 1-17.

OJEU (2012) Treaty on the Functioning of the European Union, 26 October 2012, C 326, pp. 47–390.

OJEU (2013) Commission Implementing Decision 2013/115/EU of 26 February 2013 on the SIRENE Manual and other Implementing Measures for the Second Generation Schengen Information System (SIS II), 14 March 2013, L 71, pp. 1-36.

OJEU (2016a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation"), 4 May 2016, L 119, pp. 1-88.

OJEU (2016b) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 4 May 2016, L 119, pp. 89-131.

OJEU (2016c) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, ("PNR Directive"), 4 May 2016, L 119, pp. 132-149.

OJEU (2016d) Commission Decision of 17 June 2016 on Setting up The High-Level Expert Group on Information Systems and Interoperability, 15 July 2016, C 257, pp. 3–6.

OJEU (2016e) Commission Implementing Decision 2016/1345/EU of 4 August 2016 on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II), 6 August 2016, C 257, pp. 15–20.

OJEU (2016f) Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, 16 September 1016, L 251, pp. 1-76.

OJEU (2017) Commission Implementing Decision 2017/759 of 28 April 2017 on the common protocols and data formats to be used by air carriers when transferring PNR data to Passenger Information Units, 29 April 2017, L 113, pp. 48–51.

OJEU (2018a) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, 21 November 2018, L 295, pp. 99-137.

OJEU (2018b) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 28 November 2018, L 303, pp. 59-68.

OJEU (2018c) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, 7 December 2018, L 312, pp. 1-13.

OJEU (2018d) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, 7 December 2018, L 312, pp. 14-55.

OJEU (2018e) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, 7 December 2018, L 312, pp. 56-106.

OJEU (2020) Passenger Name Records (PNR). Updated list of Member States who have decided the application of the PNR Directive to intra-EU flights as referred to in Article 2 of Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 26 October 2020, C 358, p. 7.

OJEU (2021) List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31(8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System, 16 July 2021, C 287, pp. 1-181.

Oliveira M., B. and Gabrielsen J., M. (2022) 'EU Border Technologies and the Co-Production of Security 'Problems' and 'Solutions'', *Journal of Ethnic and Migration Studies*, 48(6): 1430-1447.

Organization for Security and Co-operation in Europe (OSCE) (2016) Decision No. 6/16 on Enhancing the Use of Advance Passenger Information, 9 December 2016, MC(23) Journal No. 2, Agenda item 7.

Packer, M. (2018) *The Science of Qualitative Research* (2nd ed.) (Cambridge: Cambridge University Press).

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', *CEPS Paper in Liberty and Security in Europe*, April 2011. https://www.ceps.eu/wp-content/uploads/2011/04/SIS_II_paper_liberty_security_formatted1.pdf

Passoth, J. H. and Rowland, N. J. (2010) 'Actor-Network State: Integrating Actor-Network Theory and State Theory', *International Sociology*, 25(6): 818–841.

Payne, L. (2017) 'Visualization in Analysis: Developing ANT Analysis Diagrams (AADs)', *Qualitative Research*, 17(1): 118–133.

Pickering, S. and Weber, L. (2006) 'Borders, Mobility and Technologies of Control', In: Pickering, S. and Weber, L. (eds) *Borders, Mobility and Technologies of Control* (Springer: Dordrecht).

Prainsack, B. and Toom, V. (2010) 'The Prüm Regime. Situated Dis/empowerment in Transnational DNA Profile Exchange', *British Journal of Criminology*, 50(6): 1117–1135.

Prainsack, B., and Toom, V. (2013) 'Performing the Union: The Prüm Decision and the European Dream', *Studies in the History and Philosophy of Science*, 44(1): 71–79.

Rose, N. (2001) 'The Politics of Life Itself', *Theory, Culture and Society*, 18(6): 1-30.

Roth, S., and Luczak-Roesch, M. (2018) 'Deconstructing the Data Life-cycle in Digital Humanitarianism, *Information, Communication & Society*, 23(14): 2014-2029.

Rouvroy, A. (2013) 'The End(s) of Critique: Data-behaviourism vs. Due-process', In Hildebrandt, M. and De Vries, K. (eds.) *Due Process and the Computational Turn. The Philosophy of Law Meets the Philosophy of Technology* (New York: Routledge): 143-68.

Rouvroy, A. and Berns, T. (2013) 'Gouvernementalite´ Algorithmique et Perspectives d'e´mancipation': Le disparate omme condition d'individuation par la relation? Re´seaux, 1(177): 163–196.

Ruppert, E., Law, J., and Savage, M. (2013) 'Reassembling Social Science Methods: The Challenge of Digital Devices', *Theory, Culture and Society*, 30(4): 22–46.

Ruppert, E. and Scheel, S. (2019) 'The Politics of Method: Taming the New, Making Data Official', *International Political Sociology*, 13(3): 233–252.

Sallavaci, O. (2018) 'Strengthening Cross-Border Law Enforcement Cooperation in the EU: the Prüm Network of Data Exchange', *Eur J Crim Policy Res*, 24: 219-235.

Santos, F. (2016) 'Overview of the Implementation of the Prüm Decisions', *Exchange*, November 2016. https://estudogeral.uc.pt/bitstream/10316/41091/1/Overview%20of%20the%20implementation%20of%20the%20Prüm%20Decisions.pdf

Santos, F. (2017) 'The Transnational Exchange of DNA Data: Global Standards and Local Practices', In K. Jakobs and K. Blind (eds.) *Proceedings of the 22nd EURAS Annual Standardisation Conference. Digitalisation: Challenge and Opportunity for Standardisation*, 305–322.

Santos, F. and Machado, H. (2017) 'Patterns of Exchange of Forensic DNA Data in the European Union through the Prüm system', *Science and Justice*, 57(4): 307-313.

Savage, M. (2013) 'The 'Social Life of Methods': A Critical Introduction', *Theory, Culture and Society*, 30(4): 3–21.

Scheel, S., Ruppert, E. and Ustek-Spilda, F. (2019) 'Enacting Migration Through Data Practices', *Environment and Planning D: Society and Space*, 37(4): 579–588.

Schengen Visa News (2021) Ireland Officially Joins the Schengen Information System – SIS II, March 16, 2021 (online source). https://www.schengenvisainfo.com/news/ireland-officially-joins-the-schengen-information-system-sis-ii/

Segel, E. and Heer, J. (2010) 'Narrative Visualization: Telling Stories with Data', *IEEE Transactions on Visualization and Computer Graphics*, 16(6): 1139–1148.

Singler, S. (2021) 'Biometric Statehood, Transnational Solutionism and Security Devices: The Performative Dimensions of the IOM's MIDAS', *Theoretical Criminology*, 25(3): 454-473.

Statewatch (2007) Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System, Report nr. 07-02, Brussels, 18 December 2007. Available at: http://www.statewatch.org/news/2008/feb/JSA-art-99.pdf

Statewatch (2012) Statewatch News Online: Three-Quarters of a Million "Illegal Aliens" Now Banned from Schengen Area, 28 March 2012 (online source). http://www.statewatch.org/news/2005/apr/08SISart96.htm

Toom, V. (2018) 'Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision', *LIBE Committee Study*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

Toom, V., Granja, R. and Ludwig, A. (2019) 'The Prüm Decisions as an Aspirational regime: Reviewing a Decade of Cross-Border Exchange and Comparison of Forensic DNA Data', *Forensic Science International: Genetics*, 41: 50-57.

Topfer, E. (2011) '"Network with Errors": Europe's Emerging Web of DNA Databases', *Statewatch Journal*, 21(1): 1-5. Available at http://www.statewatch.org/analyses/no-134-dna-databases.pdf

United Nations Office on Drugs and Crime (UNODC) (2018) Airport Communication Project (AIRCOP) Real Time Operational Communication Between International Airports to Fight Transnational Organized Crime, Including Drug Trafficking, and Terrorism, Egypt, November 2018. Available at:

https://www.icao.int/MID/Documents/2018/Interregional%20AVSEC%20and%20FAL%20Seminar/PPT%209%20%20AIRCOP-Dina.pdf

United Nations Security Council (UNSC) (2014) Resolution 2178 on Threats to International Peace and Security Caused by Terrorist Acts. Adopted by the Security Council at its 7272nd Meeting on 24 September 2014, S/RES/2178.

UNSC (2016) Resolution 2309 on Threats to international Peace and Security Caused by Terrorist Acts: Aviation security. Adopted by the Security Council at its 7775th Meeting on 22 September 2016, S/RES/2309.

UNSC (2017) Resolution 2396 on Threats to International Peace and Security Caused by Terrorist Acts – Foreign Terrorist Fighters. Adopted by the Security Council at its 8148th Meeting on 21 December 2017, S/RES/2396.

UNSC (2019) Resolution 2482 on Threats to International Peace and Security Caused by International Terrorism and Organised Crime. Adopted by the Security Council at its 8582nd Meeting on 19 July 2019, S/RES/2482.

Van den Eynden, V. (2014) 'The Research Data Life Cycle', In Corti, L., Van den Eynden, L. Bishop, L. and Woollard, M. (eds.) *Managing and Sharing Research Data*, (London: Sage): 17-23.

Van Dijck, J. (2014) 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology, *Surveillance and Society*, 12(2): 197-208.

Velicogna, M. (2014) 'The Making of Pan-European Infrastructure: From the Schengen Information System to the European Arrest Warrant', In: Contini, F., Lanzara, G. (eds) *The Circulation of Agency in E-Justice* (Law, Governance and Technology Series, vol. 13): 185-215.

Venturini, T., Jacomy, M. and Pereira, D. (2015) *Visual Network Analysis* (online source). Available at: www.tommasoventurini.it/wp/wp-content/uploads/2014/08/Venturini-Jacomy_Visual-Network-Analysis_WorkingPaper.pdf

Venturini, T., Jacomy, M., and Jensen, P. (2021) 'What Do We See When We Look at Networks: Visual Network Analysis, Relational Ambiguity, and Force-directed Layouts, *Big Data and Society*, 8(1): 1-16.

WCO/IATA/ICAO (2013a) Principles, Functional and Business Requirements PNRGOV, Version 13.1, October 2013. https://www.icao.int/Security/FAL/Documents/2-PNRGOV-Principles_13-1version_FIRST.pdf

WCO/IATA/ICAO (2013b) Appendix IIA to the Advance Passenger Information Guidelines, Passenger List Message (PAXLST) Implementation Guide, Version 3.0, October 2013. Available at: https://www.icao.int/Security/FAL/Documents/3.API%20Guidelines%202013%20Appendix%20II%20A%20-%20PAXLST%20Message%20Implementation%20Guide_English_Only%20updated.pdf

WCO/IATA/ICAO (2014) Guidelines on Advance Passenger Information. Available at: https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf

Wendt, A. (1987) 'The Agent-Structure Problem in International Relations Theory, *International Organization*, 41(3): 335–370.

Wienroth, M. (2018) 'Socio-Technical Disagreements as Ethical Fora: Parabon NanoLab's Forensic DNA Snapshot™ Service at the Intersection of Discourses around Robust Science, Technology Validation, and Commerce', *BioSocieties*, 15: 28-45.

Yeung, K. (2018) 'Algorithmic Regulation: A Critical Interrogation', *Regulation and Governance*, 12(3): 505-523.