The interoperability controversy or how to fail successfully: lessons from Europe

Didier Bigo*

Sociology/Sciences Po Paris,
27 Rue Saint Guillaume, 75007 Paris, France
Email: didier.bigo.conflits@gmail.com
*Corresponding author

Lina Ewert

Berlin Social Science Centre (WZB),
Reichpietschufer 50, 10785 Berlin, Germany
Email: lina.ewert@wzb.eu

Elif Mendos Kuşkonmaz

School of Law,
University of Portsmouth,
Richmond Building, Portland Street,
PO1 3DE, Portsmouth, UK
Email: e.m.kuskonmaz@qmul.ac.uk

Abstract: This article aims to discuss the interoperability controversy in the EU that followed the 2015 Paris attacks. Supported by visual methods, it analyses the historical developments of the databases that aim at facilitating migration and crime control in the area of Justice and Home Affairs (JHA). In so doing, it seeks to trace the paradox on freedom, technology, and surveillance since the Schengen area was established in the '90s, whereby the discourse on the freedom of movement (both as the rights of citizens and migrants crossing borders) has been reframed by the security reasoning using technological solutions. It critiques the technical framework within which the interoperability plans have been framed.

Keywords: interoperability; freedom of movement; borders; (in)security; surveillance; Schengen; integrated data management; ECRIS-TCN; PNR; eu-LISA; Europe.

Reference to this paper should be made as follows: Bigo, D., Ewert, L. and Kuşkonmaz, E.M. (2020) 'The interoperability controversy or how to fail successfully: lessons from Europe', *Int. J. Migration and Border Studies*, Vol. 6, Nos. 1/2, pp.93–114.

Biographical notes: Didier Bigo is a Professor of International Political Sociology at Sciences Po Paris, and researcher at CERI where he leads the GUARDINT project: https://www.sciencespo.fr/ceri/fr/content/oversight-and-intelligence-networks-who-guards-guardians-guardint-anr-ora. He is also a Professor in the Department of War Studies at King's College London, as well as the Director of the Centre d'etudes sur les Conflits, la Liberté, la Sécurité (CCLS)-Paris.

Lina Ewert is a Research Fellow in the research group 'Politics of Digitalization' at the Berlin Social Science Center (WZB). She is part of the research project 'Oversight and intelligence networks: Who guards the guardians?' (GUARDINT), taking a closer look at the potential for democratic control of digital transnational surveillance by intelligence agencies. A sociologist by training, her research interest lies with social inequalities, migration, power, and digital humanitarianism. Her PhD project focuses on data-driven migration governance and public-private-partnerships with a specific focus on emerging technologies, (biometric) digital identity ecosystems, surveillance and accountability.

Elif Mendos Kuşkonmaz received her PhD from Queen Mary University of London and is a Lecturer in Law at University of Portsmouth. Since 2012, she has been registered as a Lawyer at Istanbul Bar Association. Her PhD research explored the compatibility of transfers of passenger information for fighting terrorism with privacy and data protection rights. She worked as a research intern at the BIICL in the winter of 2014 and she volunteered at the NGO Privacy International in the autumn of 2015. She also was a visiting researcher at the Georgetown University Law Center, Washington DC, from April 2018 to June 2018.

1 Introduction

The year 2015 was marked by two kinds of events that have furnished EU officials a fit occasion to foster a renewed debate around security, migration and the interoperability of databases in the EU's area of Justice and Home Affairs (JHA): the terrorist attacks in France in January as well as in November 2015 and the so called long summer of migration when a number of migrants from predominantly war-torn countries sought refuge in the EU (Chandler and Jones, 2019). As scholars have shown, EU immigration has already been discursively linked to internal security and crime during the negotiations for the Schengen Agreement when compensatory measures for the abolition of borders where framed as a necessity for freedom of movement [Van Munster, (2009), p.21f]. What has then been proposed and implemented is a technologically induced solution in the form of three, initially separate databases.

The first database is the Schengen Information System (SIS). Operational for almost three decades, SIS is a networked system that includes information in the form of alerts on people and objects sought for law enforcement purposes as well as information on third country-nationals to be refused admission to the Schengen area for a variety of reasons. In hindsight, the establishment of SIS alerted the securitisation of border and immigration controls because it was put forward as a solution for the fragmentation between the creation of an area of free movement and its security (Bigo, 2002). It encompasses a dual purpose under the Schengen *acquis*: information exchange for immigration purpose on the one hand and criminal law purposes on the other (Arts 92–100).

The second database is the European Asylum Dactyloscopy Database (Eurodac), a centralised database that contains fingerprints of asylum seekers and migrants who have crossed borders or resided in an EU member state without valid documentation [Regulation (EU) No. 603/2013]. Operational since 2003 and originally set up to assist

with the determination of the member state responsible for examining an asylum claim, the scope and purpose of the database has gradually been widened to enable access by national law enforcement agencies and Europol for the purpose of preventing, detecting, investigating terrorism and serious crime (Art. 7, 20, 21; see also Aus, 2003; Roots, 2015). The third database is the Visa Information System (VIS), which has been operational since October 2011 and contains information about third-country nationals who seek entry into the Schengen area on a short-term visa [Regulation (EC) No. 767/2008]. Its objective is to implement the EU common visa policy, but Europol and law enforcement authorities can access it to detect, investigate, and investigate terrorist offences and other serious crimes (Arts 2–3). Ever since these databases were put on the map, scholars have addressed how they transformed the EU border and immigration control system, integrating it with security concerns over controlling criminal activities (Huymans, 2000; Brouwer, 2002; Baldaccini et al., 2007; Mitsilegas, 2015). Much also has been written about their implications on the fundamental rights of citizens and migrants (Brouwer, 2008; Vavoula, 2016).

Despite these critical voices, EU officials have pushed further in this direction by endorsing the vision of interoperability between JHA databases. The idea formally came to surface in 2005 with the European Commission's (2005a) first communication on interoperability where it called for an increased information sharing between and access by law enforcement agencies to all three existing databases. In view of the Commission, the operational management of these databases could be undertaken by a new agency, which would eventually be established as eu-LISA in 2011 [Regulation (EU) No. 1077/2011]. Taking the Paris terrorist attacks and increase in migratory movements towards the EU in 2015 as a starting point, the Commission introduced a new agenda on security in the same year. One point of action was enhancing information exchange among different actors (be it EU institutions, agencies, or national law enforcement authorities) and exploring new information sharing channels (European Commission, 2015). One year later, the Council of the European Union outlined a roadmap for interoperability and the European Commission setup a High-Level Expert Group (HLEG) on the issue (Council of the European Union, 2016; European Commission 2016a). These documents include a streamline of discussions on establishing yet another set of databases and reframing the existing ones. These new databases are; the European Travel Information Authorisation System (ETIAS), the EU equivalent of the US ESTA scheme which contains information on online forms that all citizens of Schengen visa exempt countries have to complete before they travel to the EU [Regulation (EU) No. 2018/1240]; Entry Exist System (EES), which contains the entry and exit records of all third country nationals to the Schengen area [Regulation (EU) No. 2017/2226]; and the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN), which contains the criminal records of third-country nationals and dual nationals [Regulation (EU) No. 2019/816].

The discussion on the interoperability of databases has evolved to indicate a shorthand for connecting existing and future EU databases and enhancing search capacities so that all authorised users (to be determined by national authorities) can carry out simple searches among the multiple databases at once. Thus, personal data which has been collected under a variety of different privacy regimes and subject to a host of contrasting privacy protections is rendered accessible in the name of an alleged efficiency in decision-making and police and criminal justice cooperation (European Commission,

2016b). This narrative employed by EU officials to justify interoperability mirrors the efficiency argument of the US 9/11 Committee that favoured technical interoperability and fusion centres to respond to terrorism (DHS, 2011).

However, there have been considerable reservations to the interoperability in the opinions of the Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS) and the expert reports asked by the EU Parliament (EDPS, 2018; FRA, 2018; Alegre et al., 2017). The critics have stressed a number of controversial aspects with regard to data protection and human rights. A key controversy is the possibility of cross-checking on one side and on the other the principle of purpose limitation in police search and the rights of privacy and data protection of internet users [EDPS, (2018), p.17]. Other controversies include the potential use of interoperable databases to extract profiles that then could provide a basis for anticipatory data analysis techniques to estimate the supposed risk that people crossing borders pose to the public security [see Alegre et al., (2017), pp.23–26]. Moreover, when the data stored are not accurate and reliable, its re-use could lead to inaccurate decisions.

The reservations raised by EU institutions and agencies have been accompanied by the recent case-law of the Court of Justice of the European Union (CJEU) that amplified concerns over the legality of the interoperability plans under EU law. Declaring a draft agreement signed between the EU and Canada on the transfer of passenger information incompatible with the EU fundamental rights standards, the CJEU made a number of observations on the protection of the right to privacy that may be relevant when questioning the extent which the interoperability plans are in line with the EU fundamental rights standards (Quintel, 2018). For instance, the CJEU's Opinion 1/15 put emphasis on the existence of fundamental rights safeguards and prior judicial authorisation requirements when automated processing is at stake (paras 168–174, 197, 202, see also Vedaschi, 2018). Also, the CJEU ruled in the same Opinion that once a person enters the territory, information about their travels can be retained during their stay and after they left the country insofar as there is objective evidence indicating a link with combating terrorism and serious transnational offences (paras 196–211). From a fundamental rights perspective, this means that searching interoperable databases for anything less than serious transnational offences (e.g., general objective of border management) and without identifying objective evidence on the contribution of the data retention for combating this type of offences would fall foul of the EU fundamental rights standards.

Both the institutional oppositions and legal developments indicate that nothing is settled. Thus, this article aims to discuss the interoperability controversy in the EU. It argues that the interoperability scheme is not purely a technical inquiry. Rather, it is a political one that relates to the framing of human mobility in the EU as a security issue with the aim of controlling crime through surveillance technologies. This article supports this position from two streams. First, it implements a data visualisation method in order to look at the historical developments of the databases in the JHA and the integration of general ideas on freedom, technology, and surveillance into those developments since the Schengen area was established. It thus seeks to support the argument that the discourse on the freedom of movement (both as the rights of citizens and migrants crossing borders) has been reframed by the security reasoning with technological solutions. Second, it analyses the key policy documents (e.g., European Agenda on Security and the 2017 report of the HLEG on information systems and their interoperability) that provided

the groundwork for the plans on the interoperability of databases, which embody the latest example of the systematic use of technological tools for crime prevention.

The article is structured as follows. Section 2 explains the methodology used in the visualisation. Section 3 investigates the debates around the establishment of databases from 1992 to early 2000s and discusses the extent which law enforcement provided the ground for the creation of the databases in this period. Section 4 then looks at the developments on the interoperability tools following the Paris attack of 2015 that are embodied in the forms of policy documents, such as the European Agenda on Security. Section 5 gives a bird's-eye-view of the current status of access by a number of authorities to the existing and planned databases for diverging purposes and the public authorities per member state who have access to the existing databases. Finally, in Section 6 is the conclusion.

2 Methodology for data visualisation

In order to answer the research question via visual methods, we have first chosen the Statewatch European Monitoring and Documentation Centre on JHA in the EU (SEMDOC) database (1976–2000) as well as the organisation's news database (1991–2018) as data sources. Because this research is interested in the contingencies and framings of technological solutions as well as the driving actors, it was vital to access documents that show the discussions within the Council's several working groups, committees and council meetings as well as communications between the council, the European Commission and the European Parliament. The above-mentioned databases were chosen as they offer unique access to otherwise not publicly accessible policy documents. As a next step, the authors have searched these two research databases with regard to the most relevant policy documents concerning the information systems of the Schengen agreements, e.g., SIS (in all its variations), VIS and Eurodac as well as documents regarding eu-LISA and the projects which have been presented for smart borders and identification (i.e., ETIAS, EES, and ECRIS-TCN). Due to the comparatively small number of documents on eu-LISA in the SEMDOC database, additional documents such as annual activity reports and conference reports were retrieved from the eu-LISA's website. We have thus gathered a total number of 950 documents dating from 1992 to 2018. In a next step, we have established a hierarchy of documents according to their relevance for the research interest. Priority has been given to documents discussing the establishment and modifications of different EU information systems and databases with regard to matters of policing, border, visa, and migration. These documents were ranked higher than provisional agendas due to their analytical value for the subsequent coding phase. A total of 373 documents were thus selected as most relevant. A preliminary coding system was established using an explorative data-driven coding approach in combination with a concept-driven dimension based on prior research focusing on the four guiding themes of policing and intelligence, borders and mobility, access of authorities to the databases as well as the juridical and technical procedures at work. As such, codes were generated based on the research interest as well as their discursive prevalence (see Table 1). After the coding-system had been consolidated, the most relevant documents were coded systematically. To create the timeline visualisations found in Figures 1 and 2, the coded documents were then grouped

under the four categories to show broader trends while the more granular codes were used as a basis for the network visualisations.

Table 1 Overview hypothesis with thematic categories and related codes

Category	*Codes*	*Hypothesis*
Policing	Foreign fighters Policing Terrorism Serious crime International organised crime	An increase in codes on foreign fighters, policing, terrorism, serious crime, and international organised crime may indicate the way in which judgements on the use of technology were represented as responses to the events occurring.
Border	Irregular migrants Irregular migration Smart borders Persons enjoying free movement External border Internal border Abolition of internal borders Free movement	This category encompasses thematic codes relating to the politics of borders and mobility of people. The co-occurrence of this category with the category of policing may depict the development of the discourse on immigration in relation to the surveillance of different forms of immigration.
Access	Access immigration and asylum authorities Access intelligence services Access eurojust Access europol Access law enforcement Access police Access prosecutor Access customs Access border guards Access judicial authorities Access visa authorities for security purposes Access intelligence and security services	An increase in codes on access may show the way in which the fluidity of data from one authority to the other has become the cornerstone of the JHA databases. A correlation between the category of access and of policing may further indicate the way in which the purposes of the JHA databases moved away from identifying people crossing borders to that of protection public security.
Procedure	Identification* Interoperability** Searchability Decentralised Silo	This category contains codes on the technical and juridical elements for access. The increase in these codes indicates the technological reconfigurations of databases to maintain the flow of data from one source (i.e., immigration authorities) to the other (i.e., law enforcement authorities), while circumventing the purpose limitation whereby the use of data for purposes other than the one for which they are collected is prohibited.

Notes: *this code consolidates granular codes in relation to identification, fingerprints, facial images, iris and biometrics.
**this tag granular codes in relation to interoperability, interconnectivity and linking.

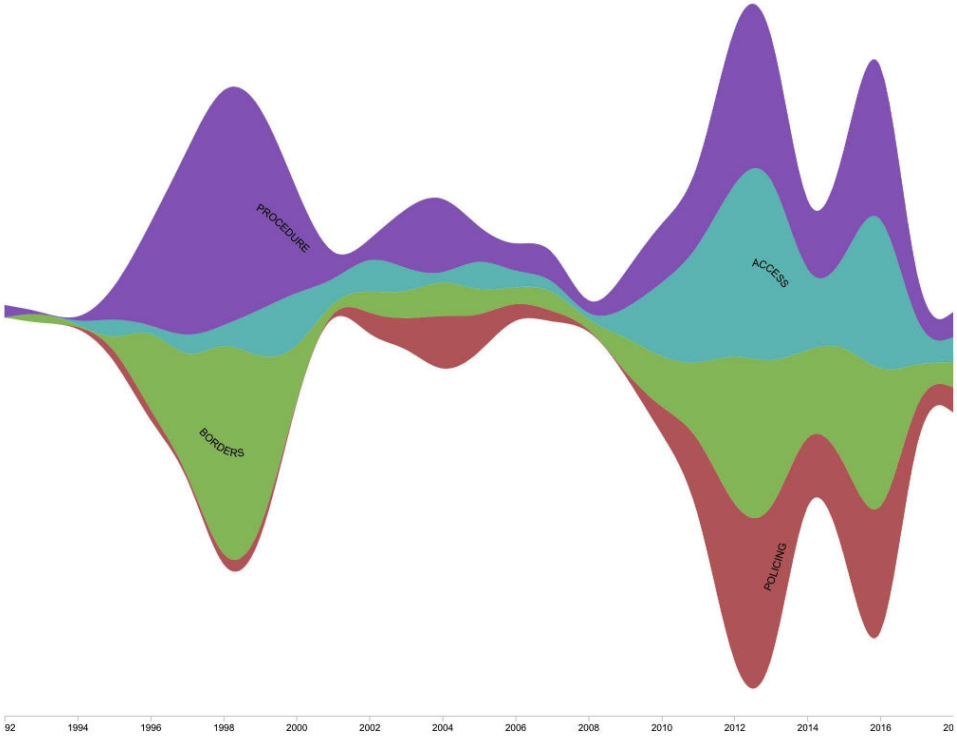
Table 2 Overview total number of (selected) documents by type of database from 1992 to 2018

	SIS (relevant/ total)	*VIS (relevant/ total)*	*Eurodac (relevant/ total)*	*EU-LISA (relevant/ total)*	*Total (relevant/ total)*
Statewatch	184/423	33/43	116/416	28/39	
EU-LISA website	--	--	--	12/29	
Total	184/423	33/43	116/416	40/68	373/950

Table 3 Overview number of documents by type of thematic category from 1992 to 2018

	Policing	*Borders*	*Access*	*Procedure*
Documents	79	134	102	162

Figure 1 Streamgraph showing the prevalence of thematic categories over time (1992–2018) (see online version for colours)



In relation to the investigation into the authorities' access to the JHA database (see Section 5), two sources of information were used to create the two visualisations (see Table 4 and Figure 3). Table 4 is from a study on the interoperability of JHA information systems (cf. Gutheil et al., 2018). Figure 3 is constructed via different EU information requests that have been made in order to know what was the exact list of authorities by country and the kind of access they were entitled to, especially to what extent the law enforcement agencies have access to other databases on migration, asylum, border and

visas, and conversely what migration or border authorities have access on law enforcement databases. These data were often published at the time of the creation of the database but were not updated. The responses to these information requests pointed us to a list of all the police stations entitled to access the databases without prior authorisation of their governments.

Figure 2 Streamgraph of mentioning of databases and information systems in document collection over time (1992–2018) (see online version for colours)

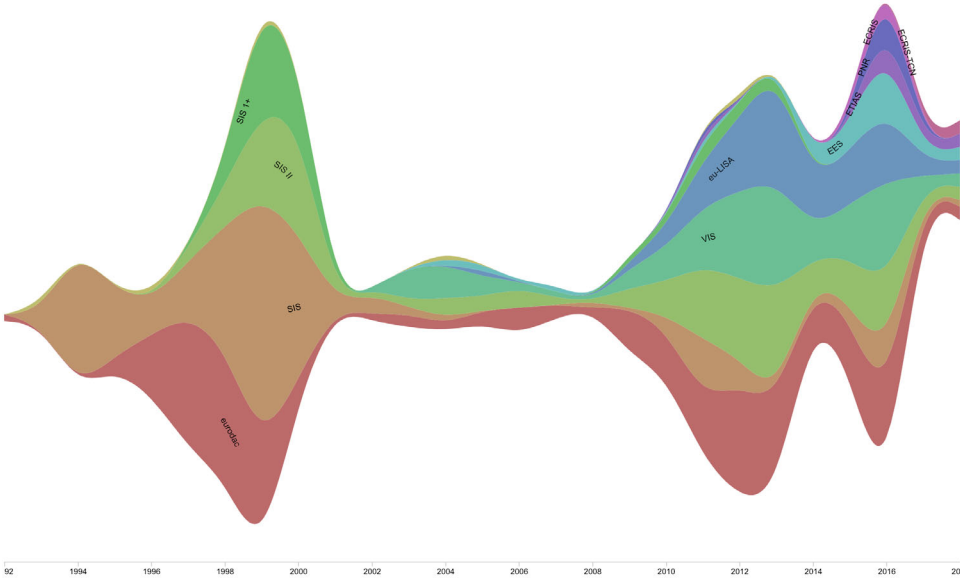
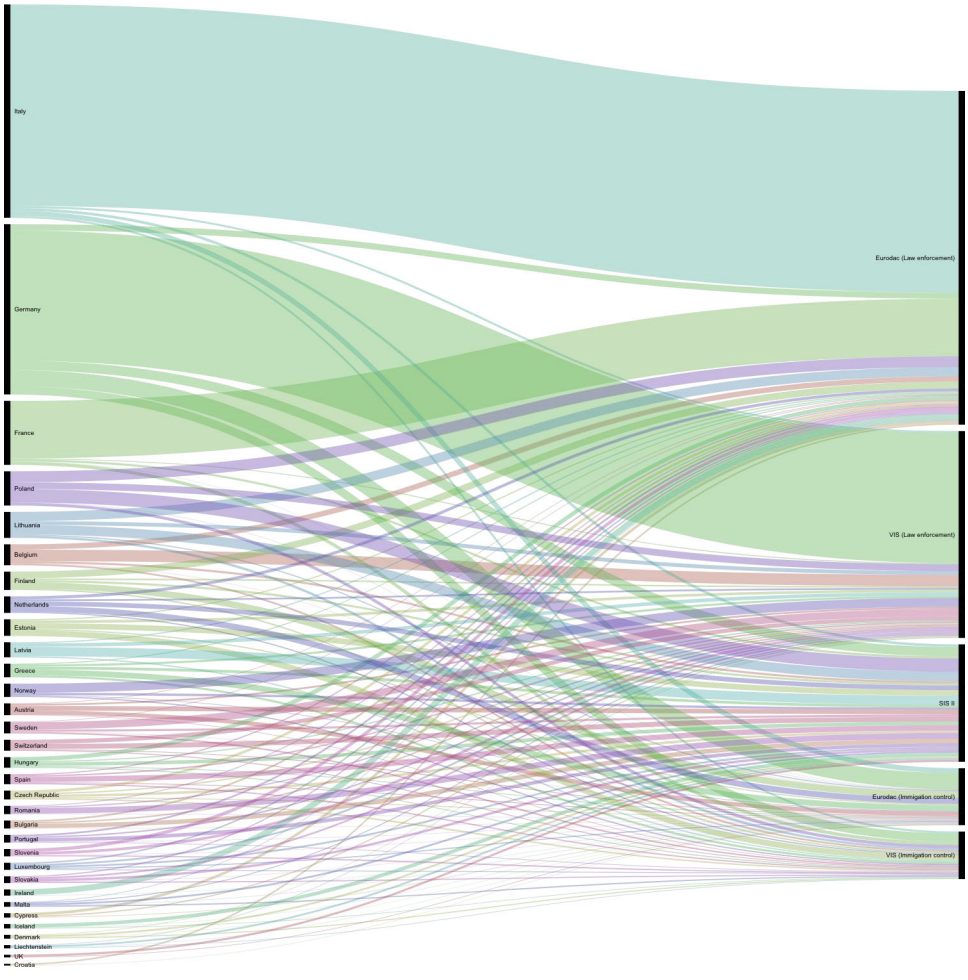


Table 4 Authorities' access to different databases and the three projects (ETIAS, EES, ECRIS-TCN) (see online version for colours)

Entity	SIS II	Eurodac	ECRIS-TCN	VIS	ETIAS	EES
Europol	Yes	Yes: Preventing, detecting and investigating terrorist and criminal offences	Yes: Access to ECRIS-TCN, but not ECRIS in its current format	Yes: Preventing, detecting and investigating terrorist and criminal offences	Yes: Preventing, detecting and investigating terrorist and criminal offences	Yes: Preventing, detecting and investigating terrorist and criminal offences
National law enforcement authorities	Yes	Yes: To check against latent fingerprints	No	Yes: Preventing, detecting and investigating terrorist and criminal offences	Yes: Preventing, detecting and investigating terrorist and criminal offences	Yes: Preventing, detecting and investigating terrorist and criminal offences
Visa authorities	Yes	Yes	Yes: May apply to criminal records authorities for access	Yes	Yes: In the event of rejection after automated application process	Yes
National border control authorities	Yes	Yes	No	Yes	Yes: Only for verification purposes	Yes
Immigration authorities	Yes	Yes	Yes: May apply to criminal records authorities for access	Yes	No	Yes
Asylum authorities	Yes	Yes	Yes: May apply to criminal records authorities for access	Yes	No	No
Eurojust	Yes	No	Yes: Access to ECRIS-TCN, but not ECRIS in its current format	No	No	No
Judicial authorities	Yes	No	Yes: Apply for access to criminal records data of an individual undergoing criminal proceedings	No	No	No

Figure 3 Alluvial diagram on the number of institutions per country that have access to databases by purpose (see online version for colours)



3 Prevalence of law enforcement purposes in databases from 1992 to 2000s

Figure 1 shows the occurrence of four thematic categories of policing, borders, access and procedures between 1992 and 2018 (see Table 1). As seen in this figure, there was a significant change in the trend towards policing and access over the 27-year period. Between 1992 and 2001, the codes grouped under the categories of access and policing[1] were mentioned the least in the selected documents, while the codes grouped under border and procedure[2] were mentioned the most. The prevalence of these last two categories is crucial because it supports the argument that the digitalisation of borders at the time was formed upon the idea of free movement, the abolition of borders and the need for identification in the context of the Schengen Agreement and compensatory measures. In the case of Eurodac, for instance, unique biometric identification of asylum

applicants (and immigrants entering irregularly or overstay their visa at a later stage) was the sole purpose of the database and debated extensively in the late 1990s [Peers and Rogers, (2006), pp.263–268]. Along the same line, despite the dual purpose of the SIS (immigration purpose on the one hand and the law enforcement purpose on the other), which was the only formally established database at the time under the Schengen *acquis*, the significantly low rank of policing indicates that the former purpose took priority over the latter [Peers, (2006), pp.201–221].

Between 2002 and 2008, access and policing showed the most drastic change compared to the earlier period, with policing reaching a first peak in 2005, in correlation with a small peak of discussions on procedures. This suggests that the cross-border information exchange by way of linking databases has been framed in relation to the search for solutions against terrorism and serious crime. This reframing of databases became possible with the window of opportunity that the 9/11 attacks as well as the 2004 Madrid and 2005 London attacks created in coupling the idea of border management with security. Evidence of this window of opportunity can be traced in establishing the VIS, which advanced the idea of granting access to law enforcement authorities and Europol from its very beginning (Council of the European Union, 2005a; European Commission, 2005b). This time period also witnessed discussions on developing the SIS II, which is the current technological platform of the original SIS, that hinged on expanding the grounds for access to the system (i.e., general purpose of the SIS II) as well as the authorities with access powers.[3] More importantly, SIS 1+, which was the first stage of integrating the SIS to the SIS II, already granted access to Europol and Eurojust, but was conceived in the traditional border controls functions: comparison of the documents of identity with the persons crossing the borders.[4] The SIS II, however, integrated the idea of 'searchability' and the collection of data for the purpose of constructing profiles [Vavoula, (2016), p.108]. These findings explain the increase in the discussions on access and policing depicted in the visualisation, supporting the argument that the purpose of protecting public security had started to become the predominant force behind the digitalisation of borders. Another related line of discussion in relation to the JHA databases concerned the inclusion of biometric identifiers in the SIS II [Regulation (EC) No. 1987/2006, Art 22] as well as in the VIS [Regulation (EC) No. 767/2008, Art 5(1)(b)–(c)]. In addition, it was in 2005 that Hague Programme called for effective information sharing and the European Commission first proposed to render databases and information systems interoperable. Both discussion threads explain the slight increase relating to procedures during this period (Council of the European Union, 2005b; European Commission, 2005b).

4 The impact of the Paris attack of 2015: the 'resurrection' of interoperability as a global solution against all threats

For most state agencies in the field, knowledge is valuable and only shared where necessary and on a reciprocal basis. Arguably, joined-up databases would weaken the knowledge exclusivity of each agency and hence the value of their knowledge. But the objections about the limited value of interoperability, which were developed by the opponents of automated processing since 2006, when compared to the collaboration through the principle of availability[5], were swept away (De Hert and Gutwirth, 2006).

The driving force towards the EU politics of joining the dots was the 9/11 attacks and more so the 2004 Madrid and the 2005 London attacks. The existing databases in the area of JHA (SIS, VIS, and Eurodac), have increasingly been discussed in conjunction with one another since the European Commission (2005a) issued its first communication on interoperability in 2005, calling for the increased information sharing and access by law enforcement agencies to all three databases. In addition, the Commission mentioned the establishment of an agency for the operational management of these databases that would eventually be established as eu-LISA in 2011, whose impact is shown in Figure 2 with a peak in the debates around the JHA databases in 2012. Since 2014, the Agency has been one of the driving forces on the smart border initiative, organising a conference on the topic and conducting several pilot studies (eu-LISA, 2014, 2015a, 2015b, 2015c). The conjuncture of events at the time also created a fertile ground to speed up the interoperability projects. As seen in Figure 1, the debates around policing, access, and procedure increased in 2016 shortly after the summer of migration in 2015 as well as the terrorist attacks in Paris and Brussels. Also, the parallel trend between the categories of policing and access after 2015 supports the argument that the JHA databases have been reconfigured to connect public authorities with different purposes (be it law enforcement or border control) for security purposes. The figure, thus, clearly shows that the discourse on borders and mobility was intertwined with the discourses on policing and access by various authorities while technical means for identification and interoperability have been discussed throughout the years in varying intensity.

While the tendency of discursively linking border controls and their absence with security risks was already present before the Paris attacks (Bigo, 2005), it became explicit and dominant afterwards. The traces of this transformation can be found in the European Agenda on Security, which is discussed in the following subsection.

4.1 The European Agenda on Security after the Paris attacks: a longstanding incremental policy for interconnection between databases

On 28 April 2015, the European Commission (2015) published its communication setting out the European Agenda on Security. This was three months after the 14 January 2015 terrorist attacks in Paris on the offices of the satirical journal Charlie Hebdo. The EU security policy which followed that attack had the objective of ensuring that only people who live in the EU JHA without internal frontiers are protected. The agenda, thus, is the central tenet of the pressures to create interoperability of databases to manage human mobility for crime control purposes. If we look at the content of the European Agenda on Security, it sets out three priorities:

1 Developing a strong EU response to terrorism and foreign terrorist fighters. Already here the mixture of language of citizens and foreigners is pronounced. As regards the foreign terrorist fighters, the communication states "[E]uropean citizens continue to join terrorist groups in conflict zones, acquiring training and posing a potential threat to European internal security on their return" (ibid, p.12). This problematises the postulated hypothesis regarding the 'foreignness' of the perpetrators of attacks.

2 Fighting serious and organised cross-border crime. This engages the issue of movement of persons across borders as it includes trafficking in human beings as well as organised crime groups involved in the smuggling of migrants.

3 Fighting cybercrime. This is the borderless crime par excellence. While border crime is the consequence of the existence of a border, cybercrime is very frequently presented as crime in a field (cyber) without border controls which is the source of the danger.

To solve these three different objectives, the agenda proposes 'interoperability' as a way to guarantee the safety of populations within the EU. The document begins by outlining a transnational threat landscape and need to act jointly: "[i]n recent years new and complex threats have emerged highlighting the need for further synergies and closer cooperation at all levels. Many of today's security concerns originate from instability in the EU's immediate neighbourhood and changing forms of radicalisation, violence and terrorism. Threats are becoming more varied and more international, as well as increasingly cross-border and cross-sectoral in nature" (ibid, p.2). Promoting terrorism, organised and cybercrime as priorities for concerted efforts to ensure security within the EU, the authors of the agenda highlight the necessity for internal and external security experts to share information and express their hope for a technical solution to foster increased cooperation and trust among participating actors (ibid, p.4).

The agenda builds on the direct link between the fight against terrorism and the JHA databases already established in prior debates around the access of the law enforcement authorities. The authors of the agenda plead immediately for a better information sharing system, but also more profoundly for a vision of connecting all the possible dots that exist in the virtual world in order to detect which individuals may pose a danger. In this logic of totality of information for a maximum security that is inherited from a disconnection between security and freedom, any boundary limiting knowledge about suspicious activity becomes perceived as an insecurity as such. This leads to what one might call the 'intelligencification' of the social world where nothing can be genuinely innocent. Suspicion becomes the alpha and omega of awareness. A 'total records' policy emerges which does not account for operational/legal limits and institutional stakes. Once again, there is no sign of a grand strategy here, but rather the regression to the habitus, generated by a politics of unease for more than 20 years and the immediate reaction to blame the others abroad (the 'foreign' fighters) even if they are citizens coming from the inside (Bigo, 2002). The policy to further strengthen security at the external borders by reinforcing a "fuller use of the SIS together with Interpol's database on Stolen and Lost Travel Documents (SLTD)" [European Commission, (2015), p.5] is exemplary of this, as if this would have prevented the individuals from crossing borders between France and Belgium using their own regular passports to cross, or to prevent people who have not crossed any border to perpetrate their actions.

Thus, authorities have acknowledged that (foreign) citizenship no longer suffices as a proxy indicator for risk. Instead, a suspect is now marked by suspicious travel patterns and associations, as the following quote suggests: "[t]racking the movements of offenders is key to disrupting terrorist and criminal networks. It is now urgent that the co-legislators finalise their work on the establishment of an EU passenger name record (PNR) system for airline passengers that is fully compatible with the Charter of Fundamental Rights while providing a strong and effective tool at EU level" (ibid, p.7). However, the CJEU was more sceptical regarding the full compatibility of PNR systems with the fundamental right to privacy when examining the draft EU-Canada Agreement in its Opinion 1/15.[6] The CJEU's findings in Opinion 1/15 in relation to the use of PNR

data for counter-terrorism purposes brings out the question on the legality of the EU PNR scheme under EU law.

In addition, the text of the agenda disregards here any limits to security investigation and plays with the momentum of the emotion regarding the Paris attacks and subsequent acts in France and Belgium. In this context, the agenda treats the generalised link between terrorist attacks and mobility of many foreign-third country nationals almost as set in stone, despite the fact that most individuals were citizens of the countries in which they launched a clandestine attack. Once this initial move was made, a link was created between terrorism and mobility in the political imagination, more or less independently of the practices of the clandestine actions. This link aims at justifying that the struggles against terrorism and other forms of risk associated to mobility like illegal migration and trafficking of people. In order to give credentials to this bridge between security and mobility, the agenda suggests introducing so called 'common risk indicators' independent of the nature of the offence which should be elaborated by EU member states' authorities (i.e., mainly police and intelligence services) in order to support the work of national border authorities when conducting checks on persons.[7] The idea of interoperability of databases, each containing police, judicial, asylum or migration information (after the Eurodac debate) could be re-launched in order to allow police services to gain access to this information, albeit without accepting a principle of availability, whereby border authorities would reciprocally be granted the right to have access to police and justice databases.

While substantial efforts were made to transform the SIS II to accommodate this change of perspective [Regulation (EU) No. 610/2013], it never got beyond an alert for border guards that someone whose details they had run through the SIS II system at the external border was subject to an alert. However, border guards are not 'real' law enforcement agents. Their rights of arrest and investigation are generally limited. So, the alert system was not considered sufficient. Instead, the ECRIS, which makes available to authorised users' information about convictions of individuals in the EU by criminal justice authorities, was brought into play. The whole assumption of the ECRIS-TCN is that third country nationals are a greater security risk including in respect to terrorism than nationals of the member states. Embedded in the logic of ECRIS-TCN is the presumption that the privacy of foreigners is less protected as a human right than that of citizens. An interpretation that is contrary to the universality of the right to privacy yet common premise for surveillance practices by intelligence services (cf. OHCHR, 2014; Wetzling and Vieth, 2019). The system is limited to third country nationals convicted by a criminal court in a member state. However, this database will be open to a wider range of authorities than ECRIS, a matter that the EDPS raised in its rather critical assessment of the proposal (EDPS, 2017). In an audacious move that has been successful so far, the Commission proposed as an answer that ECRIS-TCN included all persons who are dual nationals who thereby become assimilated to third country nationals and the quality of their citizenship of an EU member state effectively undermined – quite a divisive proposal for all the people considering privacy and non-discrimination on basis of ethnicity as a fundamental right for any human being.

What we can see, therefore, is that a discursive linkage between migration by foreign citizens and terrorism still serves as a foundation of legitimacy while in practice the suspect population is gradually expanded to citizens with certain patterns of migratory

behaviour [Guild, (2009), pp.128–131]. This will certainly be one of the next fights: the destruction of the certainty of nationality and citizenship.

4.2 Interoperability today: the justification for the launch of an integrated data management producing data suspects beyond the control of crime and migration

Following the Paris attacks and the adoption of the European Agenda on Security, the stage was then set for the next move that was simply called 'interoperability'. Being setup by the Commission in June 2016, the HLEG (High-Level Expert Group on Information Systems and Interoperability, 2017) on information systems and interoperability had its first meeting in the same month and it took less than a year to have its final report. The HLEG formally gathered high-level representatives of the commission, member states, associated members of the Schengen area, relevant EU agencies, the European Counter Terrorism Centre (ECTC), and the EDPS, as well as representatives of the European Parliament's Committee on Civil Liberties, JHA (LIBE) and of the general secretariat of the Council as observers. The declared objective of the HLEG was "to contribute to an overall strategic vision on how to make the management and use of data in full compliance with fundamental rights, and to identify solutions to implement improvements" (ibid, p.6). In their final report, they insist that "[t]his would provide a bridge between the technical expert level and the policy discussion at senior official level" (ibid). Even if the narratives of the HLEG and the Commission insist on the fact that they propose alternatives, it seems that the proposed technological solution is de facto the only solution in their mind. The above-mentioned report is a distinctively glaring example of priority inversions. The so-called 'experts' technical group on interoperability of eu-LISA has projected what needs to be a better collaboration and the technical tools to achieve this purpose. They make reference to an integrated data management (IDM) instead of an integrated border management (IBM)[8] when considering issues relating to EU's external border management, which we consider an example of managing 'identities' as a way to 'join the dots' for the securitisation of mobility discussed above. In other words, although the security-centric approach to borders that was embedded in the IBM strategy (Hayes and Vermeulen, 2012) continues, the 'personalised borders' comprising of identities of those who seek to cross EU external borders [Moreno-Lax, (2017), p.38] is more apparent under the IDM strategy. This position rests on the growing presumption that the information, especially biometric identifiers, contained in databases represent the 'real' identity of individuals and managing these 'real' identities means that states can manage human mobility for crime control purposes because the 'dots' are the identities contained or captured in EU databases (Lyon, 2008; Pallitto and Heyman, 2008; Whitley and Hosein, 2010). It is noteworthy that the process of interoperability is mostly internal to eu-LISA management, and is a justification for the next projects to be constructed, creating the impression that all the IT systems managed by the agency would otherwise be at peril. We therefore think it is important to detail more what the experts mean by such a move and how forms of exclusionary politics are less and less at the borders and more and more based on collection and interception of data for preventive and deterrence policies against many diverse flows of movements in the name of counter-terrorism, but practically used largely beyond this objective (Bigo, 2014).

The HLEG proposes to fill the general definition of interoperability with the restrictive one of 'tools'. The group suggests four of them, which are in some ways 'incremental' and are proposed in a certain order. For each tool, they suggest solutions but also signal some problems to be resolved. They consider four tools [i.e., single-search functionality, interconnectivity, shared biometric matching service (BMS), common identity repository (CIR)] to built-in the existing and future databases in order to allow for interoperability [High-Level Expert Group on Information Systems and Interoperability, (2017), p.27]. The FRA has helpfully set out a synthesis of what they are:

- First a European search portal (ESP) to allow competent authorities to search multiple IT systems simultaneously, using both biographical and biometric data.
- Second a shared BMS to enable the searching and comparing of biometric data (fingerprints and facial images) from several IT systems.
- Third a CIR containing biographical and biometric identity data of third-country nationals available in existing EU IT systems.
- Fourth a multiple-identity detector (MID) to check whether the biographical and/or biometric identity data contained in a search exists in other IT systems so as to enable the detection of multiple identities (FRA, 2018).

The most striking feature of these information and personal data systems is their heterogeneity – not only do they contain very different data and have been established for different purposes, but also the ways in which they operate and can be consulted are entirely different. For example, if the four tools are operated on the Eurodac database, this database does not yet hold the names of people whose fingerprint data are stored in the system.[9] If a check reveals a fingerprint match, the checking authority must go to the authorities of the member state that entered the fingerprints to find out the identity of the individual. It is prohibited that any data on EU citizens is included in this database. The ECRIS database, on the other hand, is driven by the nationality of the convicted person and details of the conviction. Each database has therefore a different trajectory in EU law and policy, and a different objective. These differences between the databases demonstrates that bridging them is not a technological necessity. It reveals a political strategy by eu-LISA that is the reminiscent of the US Homeland Security and its motto of Total Information Awareness with the focus on gathering information about individuals and implementing algorithmic decision making for the purpose of anticipating security threats (National Research Council Report, 2008). It is a question of building in the coming 20 years an interoperable common register that would be able to seek an individual through their biometric identifiers by identifying them through the traces they has left in the databases as a crime or terror suspect, but also as an illegal migrant or as a mere stranger travelling and passing through the territory, or as a person welcoming foreigners or even ultimately seeking to flee.

These proposals of the HLEG would take further form with a package of EU legislative proposals in 2017 to establish a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) (European Commission, 2017a, 2017b). They commence with the latest formulation of the inter-connection of border controls, movement of persons and terrorism. The first statement in the explanatory memorandum states "[i]n the past three years [2015–2017]

the EU has experienced an increase in irregular border crossings into the EU, and an evolving and ongoing threat to internal security as demonstrated by a series of terrorist attacks" [European Commission, (2017b), No. 46, p.1]. The logic of the integration of threats – irregular border crossing and terrorism – is thus at the centre of the justification for far reaching incursions regarding the human right to privacy.

In conclusion, the interoperability process post 2015 and the struggles around it are a key moment of transformation of the field of 'security' by allowing a specific group of agents on the transnational scale, those who construct the databases for their 'clients', i.e., data analysts, civil engineer of integrated border management or integrated data management to become increasingly powerful. These actors are thus now able to compete with police, intelligence, immigration, border guard agencies on who decides and frames what is labelled security, insecurity and fate in Western societies through their key role on the exchange of information in policing matters.

5 Current status of database access

While the plans on the interoperability of databases have clawed to the top of the European security policy, the current picture of the policies of member states in relation to the access to the existing (and proposed) databases are less then coherent. Superficially, if we were to categorise different authorities as in Table 4 according to their functions, we see that different authorities have access to certain aspects of databases for particular purposes. For example, the law enforcement authorities can gain access to almost all the databases under certain circumstances. This is even more the case for the border control, immigration, and visa authorities, who are certainly the key authorities for identification purposes and verification of profiled suspects when they cross the borders or present documents for travel. Asylum authorities are not concerned at the moment with the projects of ETIAS and EES. The judicial authorities have almost no access on the databases linked to travel.

The fragmented structure in relation to the access seen in Table 4 explains the HLEG's enthusiasm to suggest technical solutions to establish the framework of interoperability for the systems (see Subsection 4.2). However, as mentioned earlier, what is missing here is the implication of the interoperability for the fundamental rights because, as Table 4 shows, the authorities' access depends on their functions. Among other things, the interoperability projects pave the way for a function creep as interoperable databases may potentially allow the use of data for purposes other than it was originally collected for. Related to this issue is the fact that the availability of the data in one database is insufficient to support the interoperability argument. The databases relating to individuals who cross borders (e.g., VIS, Eurodac) originally collect the data in relation to visa and asylum purposes. Allowing the law enforcement authorities access to these databases came at a later stage and at the expense of the fundamental rights of migrants. The Eurodac Recast Regulation proposed by the European Commission in 2016 seeks to widen the scope of the data contained even more to also include facial images which may open up new avenues for surveillance via facial recognition technology (European Commission, 2016c). The interoperability thus cements the fundamental rights detrimental effect not least because it identifies those who want to cross borders as potential security threat unless the data tells otherwise and eradicates the presumption of innocence.

Moreover, as Figure 3 shows, there is a sense of disproportionate access between countries, and their diverse strategies and/or fears. As we can see in this figure, the extent of access depending on the strategy of the different ministries and from the structure of the government is different from one country to another one. Italy has maximised the transformation of access to Eurodac and allows all the local police to have access for law enforcement purposes with more than 600 points of access; a number which is no match for Spain or Portugal that have chosen on the contrary to have a very small number of points of access. France more or less follows Italy, while Germany has implemented access to Eurodac for law enforcement purposes. However, Germany has more access to Eurodac for migration purposes when compared to Italy's access to Eurodac for the same purpose. Germany is also using its access to the VIS extensively for law enforcement purposes. The difference of strategy between the different countries regarding the use of each database is striking. These uses are very heterogeneous. Here, a note of caution is necessary. Italy may have a large number of potential lists of access while it never uses them. Germany may have only a few lists of access, but it uses them intensively (cf. eu-LISA, 2018). What is relevant from the graph is the heterogeneity between member states at the level of official strategies to give to a large number (or not) of authorities' direct access albeit the effective use of said access may be similar.

6 Conclusions

This article aimed to trace the EU's plans on the interoperability of databases especially following the 2015 Paris attacks. It critiqued the technical framework within which the plans have been framed, rather than taking into account their implications for the fundamental rights of citizens and migrants. In this regard, it argued that this way of depoliticising the issues by promoting a technology-oriented discourse that is not unique for the discussions on the interoperability. Rather, it is entrenched in the paradox on freedom, technology, and surveillance that dates back to the introduction of the Schengen Agreement and the SIS as the first information system to be framed on the crossroads of freedom of movement and (in)security. To support this view, the article introduced visual companions to elaborate the development of JHA databases over the years. In so doing, it showed that the freedom of movement has been tainted by an ever-growing reliance on surveillance. The downgrading of the freedom of movement has been exacerbated by the security reasoning whose affect can be traced along the lines through intertwining of border control and law enforcement purposes and debates around the interconnection of databases with different purposes.

Post-2015, the example of the ongoing paradox has been embodied in the European Security Agenda and the HLEG's report on interoperability. Here, the interoperability of databases is used as a tacit way to intertwine the purposes of border controls, visa application managements, and law enforcement. While the discourse is presented as a technical solution, in reality it frames individuals crossing borders as de facto public security concerns, piercing through the presumption of innocence. The implications of interoperability for the fundamental rights (e.g., privacy, data protection, prohibition against discrimination, and right to asylum), or its alleged efficiency (e.g., the perpetrators of the 2015 attacks were mostly EU citizens) have been given little to no attention in the proposals, despite the critiques of the FRA, EDPS, and the experts reports

presented to the EU Parliament. Interoperability as the ultimate way for a greater security even disregards the great diversity of national policies regarding the access to databases and strategies among EU member states on border control and law enforcement. Instead, what rises to the surface is a political strategy shaped by IT specialists hinging on a massive information system at the expense of the rule of law, fundamental rights, and freedom.

Acknowledgements

The authors are grateful to Dr. Jonathan Gray for his essential contributions to the visualisations for Figures 1, 2, and 3, and to Dr. Niovi Vavoula for her valuable participation in the information requests that provided the essential preparatory work for Table 4 and Figure 3.

References

Alegre, S., Jeandesboz, J. and Vavoula, N. (2017) *European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection*, PE 583.148 [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583148/IPOL_STU(2017)583148_EN.pdf (accessed 24 July 2019).

Aus, J. (2003) *Supranational Governance in an 'Area of Freedom, Security and Justice' – Eurodac and the Politics of Biometric Control*, SEI Working Paper No. 72.

Baldaccini, A., Guild, E. and Toner, H. (2007) *Whose Freedom, Security and Justice?: EU Immigration and Asylum Law and Policy*, Hart Publishing, London.

Bigo, D. (2002) 'Security and immigration: towards a critique of the governmentality of unease', *Alternatives*, Vol. 27, No. 1, pp.63–92.

Bigo, D. (2005) 'Frontier controls in the European Union: who is in control?', in Bigo, D. and Guild, E. (Eds.): *Controlling Frontiers: Free Movement into and within Europe*, pp.50–99, Ashgate, Aldershot.

Bigo, D. (2014) 'The (in)securitization practices of the three universes of EU border control: military/navy – border guards/police – database analysts', *Security Dialogue*, Vol. 44, No. 3, pp.209–225.

Bigo, D. (2019) 'The emergence of a guild of 'digital technologies for security purposes'?: interoperability and its effect on freedom of movement, security technologies and human values', *Int. J. Migration and Border Studies*, in press.

Brouwer, E. (2002) 'Eurodac – its limitations and temptations', *European Journal of Migration and Law*, Vol. 4, No. 2, pp.231–247.

Brouwer, E. (2008) *Digital Border and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden-Boston.

Chandler, C.L. and Jones, C. (2019) 'EU pushes to link tracking databases', *Politico*, 15 April.

Council of the European Union (2005a) *Press Release 2645th Council Meeting Competitiveness (Internal Market, Industry and Research)*, 7 May, Doc. No. 6811/05.

Council of the European Union (2005b) *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, OJ C 53/1.

Council of the European Union (2006) *Integrated Border Management: Strategy Deliberations*, Doc. No. 13926/3/06 REV 3.

Council of the European Union (2016) *Roadmap to Enhance Information Exchange and Information Management Including Interoperability Solutions in the Justice and Home Affairs Area. Presidency of the Council of the European Union*, Doc. No. 9368/1/16 REV 1.

De Hert, P. and Gutwirth, S. (2006) *Interoperability of Police Databases Within the EU: An Accountable Political Choice?*, Tilburg University Legal Studies Working Paper No. 003/ 2006 [online] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=971855 (accessed 24 July 2019).

DHS (2011) *Implementing 9/11 Commission Recommendations* [online] https://www.dhs.gov/ xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf (accessed 24 July 2019).

European Data Protection Supervisor (EDPS) (2017) *EDPS Opinion on the Proposal for a Regulation on ECRIS-TCN*, Opinion 11/2017, 12 December [online] https://edps.europa.eu/ sites/edp/files/publication/2017_0542_draft_opinion_ecris_tcn_revab_en.pdf (accessed 24 July 2019).

European Data Protection Supervisor (EDPS) (2018) *Opinion 4/2018 on the Proposals for Two Regulations Establishing a Framework for Interoperability Between EU Large-scale Information Systems*, Opinion 4/2018, 16 April [online] https://edps.europa.eu/sites/ edp/files/publication/2018-04-16_interoperability_opinion_en.pdf (accessed 24 July 2019).

eu-LISA (2014) *1st eu-LISA International Conference – Smart Borders: A Faster and Safer Way to Europe*, Conference Report.

eu-LISA (2015a) *Testing the Borders of the Future – Smart Borders Pilot: The Results in Brief* [online] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_pilot_-_executive_summary_en.pdf (accessed 24 July 2019).

eu-LISA (2015b) *Smart Borders Pilot Project: Report on the Technical Conclusions of the Pilot*, Vol. 1 [online] https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf (accessed 24 July 2019).

eu-LISA (2015c) *Smart Borders Pilot Project: Technical Report Annexes*, Vol. 2 [online] https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical% 20Annexes.pdf (accessed 24 July 2019).

eu-LISA (2018) *Eurodac – 2017 Statistics*, February [online] https://www.eulisa.europa.eu/ Publications/Reports/Eurodac%20Statistics%202017.pdf (accessed 24 July 2019).

European Commission (2005a) 'Communication from the commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs', *COM*, 24 November, Vol. 597 Final.

European Commission (2005b) 'Proposal for a council decision concerning access for consultation of the visa information system (VIS) by the authorities of member states responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences', *COM*, 24 November, Vol. 600 Final.

European Commission (2015) 'Communication from the commission to the European Parliament, the council, the European Economic and Social Committee of the regions on European Agenda on Security', *COM*, 28 April, Vol. 185 Final.

European Commission (2016a) *High-Level Expert Group on Information Systems and Interoperability*, Scoping Paper, June.

European Commission (2016b) 'Communication from the commission to the European Parliament and the council, stronger and smarter information systems for borders and security', *COM*, 6 April, Vol. 205 Final.

European Commission (2016c) 'Proposal for a regulation on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by member states' law enforcement authorities and Europol for law enforcement purposes (recast)', *COM*, 4 May, Vol. 272 Final.

European Commission (2017a) 'Proposal for a regulation of the European Parliament and of the council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)', *COM*, 12 December, Vol. 794 Final.

European Commission (2017b) 'Proposal for a regulation of the European Parliament and of the council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No. 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226', *COM*, 12 December, Vol. 793 Final.

Fundamental Rights Agency (FRA) (2018) *Interoperability and Human Rights Implications: Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion – 1/2018 [Interoperability], 19 April [online] http://fra.europa.eu/en/opinion/2018/interoperability (accessed 29 January 2019).

Guild, E. (2009) *Security and Migration in the 21st Century*, Polity Press, Cambridge.

Gutheil, M., Liger, Q., Eager, J., Oviosu, Y. and Bogdanovic, D. (2018) *Interoperability of Justice and Home Affairs Systems* [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf (accessed 24 July 2019).

Hayes, B. and Vermeulen, M. (2012) *Borderline: The EU's New Border Surveillance Initiatives*, Heinrich Böll Foundation [online] https://www.statewatch.org/news/2012/jun/borderline.pdf (accessed 24 July 2019).

High-Level Expert Group on Information Systems and Interoperability (2017) *Final Report* [online] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1 (accessed 24 July 2019).

Huymans, J. (2000) 'The European Union and the securitization of migration', *Journal of Common Market Studies*, Vol. 28, No. 5, pp.751–777.

Lyon, D. (2008) 'Biometrics, identification and surveillance', *Bioethics*, Vol. 22, No. 9, pp.499–508.

Mitsilegas, V. (2015) *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law*, Springer, London.

Moreno-Lax, V. (2017) *Accessing Asylum in Europe: Extraterritorial Border Controls and Refugee Rights under EU Law*, Oxford University Press, Oxford.

National Research Council Report (2008) *Protecting Individual Privacy in the Struggle Against Privacy*, National Academies Press, Washington, DC.

OHCHR (2014) *Report of the Office of the United Nations High Commissioner for Human Rights The Right to Privacy in the Digital Age*, *27th Sess.*, UN Doc. A/HRC/27/37.

Pallitto, R. and Heyman, J. (2008) 'Theorizing cross-border mobility: surveillance, security and identity', *Surveillance & Society*, Vol. 5, No. 3, pp.315–333.

Peers, S. (2006) *EU Justice and Home Affairs Law*, Oxford University Press, Oxford.

Peers, S. and Rogers, N. (2006) *EU Immigration and Asylum Law*, Martinus Nijhoff Publishers, Leiden-Boston.

Quintel, T. (2018) *Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention*, University of Luxembourg Law Working Paper No. 002-2018 [online] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3132506 (accessed 24 July 2019).

Roots, L. (2015) 'The new EURODAC regulation: fingerprints as a source of informal discrimination', *Baltic Journal of European Studies*, Vol. 5, No. 2, pp.108–129.

Van Munster, R. (2009) *Securitizing Immigration – The Politics of Risk in the EU*, Palgrave-Macmillan, London.

Vavoula, N. (2016) *Immigration and Privacy in the Law of the EU: the Case of Databases*, PhD. QMUL.

Vedaschi, A. (2018) 'The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15', *European Constitutional Law Review*, Vol. 14, No. 2, pp.410–429.

Wetzling, T. and Vieth, K. (2019) 'Upping the ante on bulk surveillance – an international compendium of godd legal safeguards and oversight innovations', *Heinrich Böll Stiftung Publication Series on Democracy*, Vol. 50.

Whitley, E.A. and Hosein, G. (2010) 'Global identity policies and technology – do we understand the question?', *Global Policy*, Vol. 1, No. 2, pp.209–215.

EU legislation

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), OJ L 381/4.

Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-Stay Visas (VIS Regulation), OJ L 218/60.

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, OJ L 286/1.

Regulation (EU) No. 610/2013 of the European Parliament and of the Council of 26 June 2013 Amending Regulation (EC) No. 562/2006 of the European Parliament and of the Council Establishing a Community Code on the Rules Governing the Movement of Persons Across Borders (Schengen Borders Code), the Convention Implementing the Schengen Agreement, Council Regulations (EC) No. 1683/95 and (EC) No. 539/2001 and Regulations (EC) No. 767/2008 and (EC) No. 810/2009 of the European Parliament and of the Council, OJ L 182/1

Regulation (EU) No. 2017/2226 of the European Parliament and of the Council of 30 November 2017 Establishing an Entry/Exit System (EES) to Register Entry and Exit Data and Refusal of Entry Data of Third-Country Nationals Crossing the External Borders of the Member States and Determining the Conditions for Access to the EES for Law Enforcement Purposes, and Amending the Convention Implementing the Schengen Agreement and Regulations (EC) No. 767/2008 and (EU) No. 1077/2011, OJ L 327/20.

Regulation (EU) No. 2018/1240 of the European Parliament and of the Council of 12 September 2018 Establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No. 1077/2011, (EU) No. 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ L 236/1.

Regulation (EU) No. 2019/816 of the European Parliament and of the Council of 17 April 2019 Establishing a Centralised System for the Identification of Member States Holding Conviction Information on Third-Country Nationals and Stateless Persons (ECRIS-TCN) to Supplement the European Criminal Records Information System and Amending Regulation (EU) 2018/1726, OJ L 135/1.

The Schengen Acquis – 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, [2000] OJ L 239.

EU cases

Opinion 1/15 *(Passenger Name Record Data) (European Union/Canada)*, ECLI:EU:C:2016:656.

Notes

1 The category of access is composed of codes relating to the granting of access to various authorities, the category of policing entails codes relating to terrorism, serious or organised crime (see Section 2).

2 While the category of borders is constituted of codes relating to free movement, borders and illegal immigration, the category of procedure encompasses codes relating to identification and interoperability (see Section 2).

3 *Regulation (EC) No. 1987/2006*, Art 1(2) "(t)he purpose of SIS II shall be [...] to ensure a high level of security within the area of freedom, security and justice of the European Union" [see also ibid, Art 28 "(u)sers may only access data which they require for the performance of their tasks"].

4 See Bigo's (2019) article in this special issue.

5 The principle whereby information held by a competent authority in one member state for law enforcement purpose must be made available to an equivalent authority in another member state.

6 PNR is an umbrella term to refer to the information that comprises a wide array of data about passengers' travel history, originally collected by private companies such as air carriers, travel agencies, or reservations systems for commercial purposes. This information was used to track down people for whom there is a search warrant and especially to identify people who may be risk to the public security through algorithmic decision-making process despite the fact that no criminal suspicion has fallen upon them.

7 The so-called Fichiers S (for surveillance) in France, even if these data are not based on law enforcement logic, but on an intelligence logic including parameters for the surveillance of friends of friends, as well as elements of 'reputation' collected locally and not verified.

8 The IBM refers to an ensemble of policies, legislations, institutions, and actors in relation to constitutionalisation and institutionalisation of EU external borders. It comprises the objectives of border controls through conducting surveillance including risk analysis and crime intelligence, detection and investigations of cross-border crimes, cooperation and coordination among agencies in this field, and four tier access control model that indicate cooperation with third countries for EU border and immigration management (Council of the European Union, 2006).

9 The Eurodac Recast Regulation proposed by the European Commission (2016c) seeks to widen the scope of the data contained to also include biographical data.