Chapter 12, in: Mary Bosworth and Lucia Zedner (Eds) "Privatising Border Control. Law at the Limits of the Sovereign State"?Oxford University Press, 2022.

The Digitalisation of Border Controls and their Corporate Actors

Didier Bigo, Sciences Po, Center for International Studies (CERI), CNRS, Paris, France

Abstract: The dematerialisation of physical borders via the digitisation of the process of control has changed the ways we understand international frontiers. Surveillance of the borders are now exercised at a distance, before individuals arrive. Even if most border guards insist that they have the ultimate (sovereign) right to decide who enters, the development of pre-check-in databases have de facto displaced the modalities of authentification and identification of travellers. This article depicts these changes, and shows how control is 'distributed' along the journeys of the passengers, and between many different actors, who are not all, by any means, public agents. The role of corporate actors are crucial.

Keywords: smart borders, surveillance, Schengen Information System (SIS), eu-LISA, Frontex, private providers, transnational guilds, intelligencification of control.

I Introduction

This chapter focuses on the dematerialisation of physical border controls through the digitalisation of border entry processes. It aims to contribute to critical studies of borders and surveillance by demonstrating that remote policing and identity control are not new. To understand their beginnings, it is necessary to go back at least to the early days of the Schengen Information System (SIS 1) , and analyse its transformation from a border control tool into a series of preventive policing tools for authentication, identification, automated detection of potential fraud, and the production of watch lists on a transnational scale.1 The chapter also highlights the role corporate actors specialising in data systems have played in designing and implementing the integration of data management into border security. I argue that these private actors are neither simply marginal players, nor pure technicians at the service of security professionals and national governments.

The vision of task delegation keeping sovereign decisions intact in public hands cannot hold in this field of digitalisation of security. On the contrary, corporate actors have been the driving force, since the 1990s, in building the data 'highways' that have emerged across the Global North, and especially inside the European Union (EU), for information exchange between security professionals. Working with their partners—who were familiar with computer systems, as well as being law-enforcement officers—computer (IT) systems corporate specialists planned some of the features that have changed the way border security is now conceptualised and delivered. These

1 Evelien Brouwer, 'Digital Borders and Real Rights: Effective Remedies for Third-country Nationals in the Schengen Information System' (Brill 2008)

groups of individuals had different backgrounds and statuses, but their trajectories converged towards a specific ambition: to reframe local border management into integrated data management (labelled 'IBM'). From this aim has emerged a field that is transversal to both the US and the EU, and which has its own characteristics, but whose transnational links are very strong in terms of infrastructures and social use of digital technologies of surveillance and control. This field of practice has given birth to dominant positions by actors that I call a 'transnational guild of data managers and IT systems engineers', which differs from traditional internal security bureaucracies, and involves corporate knowledge of digital surveillance management.2

In the first part, the chapter will, therefore, show that remote policing and border surveillance is an old practice, but that its implementation differs from before, as the digitalisation of controls delocalises the places of control, reinforces large-scale surveillance, and often privileges preventive logics over evidence-gathering or face-to-face border checks. In many scholarly articles which describe these evolutions of policing at a distance, the terminology of assemblage has gained ground to explain the complexity of the situation, the role of public–private partnerships in the process of de-assembling / re-assembling of the state,3 and the crucial importance of multi-positioned actors (whether individuals or agencies) who destabilise, by their habitus and trajectories, the traditional dualist categories of public and private,4 civil and military, and material and digital. In a more Marxist vein, some have also used the label of a border 'apparatus' to examine the role of a private industry that profits from the detention of foreigners, and from electronic walls and

2 Didier Bigo, 'Sociology of Transnational Guilds' (2016) 10 International Political Sociology 398 <http://ips.oxfordjournals.org/content/10/4/398> accessed 16 January 2017; Didier Bigo, 'Adjusting a Bourdieusian Approach to the Study of Transnational Fields' in Christian Schmidt-Wellenburg and Stefan Bernhard (eds), Charting Transnational Fields: Methodology for a Political Sociology of Knowledge (Routledge 2020); Christian Schmidt-Wellenburg and Stefan Bernhard (eds), Charting Transnational Fields: Methodology for a Political Sociology of Knowledge (Routledge 2020).

3 Rita Abrahamsen and Michael C Williams, 'Security beyond the State: Global Security Assemblages in International Politics' (2009) 3(1) International Political Sociology 1; EN Beck, 'The Invisible Digital Identity: Assemblages in Digital Networks' (2015) 35 Computers and Composition 125; Rita Abrahamsen and Anna Leander, Routledge Handbook of Private Security Studies (Routledge 2015).

4 Bosworth and Singler, in this volume.

biometric identifiers.5 Both science technologies and society (STS) and Marxist authors point to the importance of studying the specific trajectories of different social forces, and the places they inhabit, as well as their previous practices regarding coercion, violence, state secrecy, and forms of effective freedom (thought, opinion, and movement), in order to understand the processes of transformation induced by digitalisation of security beyond borders. Nevertheless, these two approaches can also lead one to see only the alliances, similarities, and continuities between the dominant actors, and to merge them under one general category (neo-liberal managers, surveillance capitalism, and racial capitalism), with the effect of deflating the responsibilities of those specifically in charge, instead of analysing their inner struggles around the different ways of organising security practices at borders.

Of course, from these different strands of research, important analyses concerning the impact of technologies on the daily routines of border guards exist for the North American, Australian, and EU cases,6 but they rarely touch on the organisation of digital technologies, as such (with the exception of Akkerman).7 Thus, while the proliferation of so-called smart borders has been critically studied,8 and while many evaluation reports have shown the

5 Claire Rodier, Xénophobie Business (La Découverte 2012); Gregory Feldman, The Migration Apparatus (Stanford University Press 2020).

6 Matthias Leese, 'Exploring the Security/Facilitation Nexus: Foucault at the "Smart" Border' (2016) 30(3) Global Society 412 <https://www.tandfonline.com/doi/full/10.1080/13600826.2016.117301 6> accessed 19 January 2019; Karine Côté-Boucher, 'Smart Borders?Customs, Risk Targeting, and Internal Politics in a Border Agency' in Stacey Hannem, Carrie Sanders, and Christopher Schenider (eds), Security and Risk Technologies in Criminal Justice: Critical Perspectives (Canadian Scholars Press Inc 2019) 225; Julien Jeandesboz, 'Justifying Control: EU Border Security and the Shifting Boundaries of Political Arrangement' in Raphael Bossong and Helena Carrapico (eds), EU Borders and Shifting Internal Security (Springer 2016).

7 Mark Akkerman, The Business of Building Walls (Transnational Institute 2019) <https://www.tni.org/files/publication-downloads/business_of_building_walls_-_full_report.pdf> accessed 28 November 2021.

8 Elspeth Guild and others, An Analysis of the Schengen Area in the Wake of Recent Developments (CEPS 2016) <https://www.ceps.eu/ceps-publications/analysis-schengen-area-wake-recent-developments/> accessed 28 November 2021; Médéric Martin-Mazé, 'Report: The Power Elite of Security Research in Europe: From Competitiveness and External Stability to Dataveillance and Societal Security' (2020) 6(1–2) International Journal of

limits of these technologies, the critique has focused more on the potential and actual social effects they imply concerning accountability, transparency, and human behaviour, than on the process itself, and the path dependency it may generate. Thus, while the consequences of these transformations are analysed in detail, the global, transnational landscape of the 'system of systems' of these interoperable technologies, and the number of participants in this electronic surveillance by dematerialised eyes, are still a map of archipelagos within uncharted waters, where only a few institutional islands emerge, but where the knowledge is still rudimentary concerning the 'oceanic' flows of private companies, industries, and the myriad of practitioners who work closely together to produce these systems of systems; to collect data, store and organise them for different profiles, and resell them for different purposes. All these activities impact on the practices and conceptualisations of border controls. Building on Mathiesen's 2000 research,9 which was one of the most detailed analyses of this early period of the process of 'globalisation of control', describing the Schengen Information System, I analyse, here, the delinkage between borders and controls, due to this digital globalisation, via a field approach, in the Bourdieusian sense. By doing so, this chapter hopes to repoliticise these developments concerning the emergence of a specific craft of security data management, whose effects are less a way of achieving technical interoperability and enabling the detection of terrorist or illegal migrant suspects, than a possibility for data analysts and systems engineers working for private firms to influence public decision-making power in respect of risk analysis, and to challenge traditional visions of sovereignty at the borders. This impact of a stratum of specialists in charge of transnational police data highways, who have de facto subordinated the specific traditional stakes of border controls to their own overall strategy of developing preventive tools for data analytics via artificial intelligence, has led to (partially) unintended consequences. The potential replacement of personnel at the borders with remote data analysis tends to dehumanise border controls, and to create a structural indifference on the fate of refugees, beyond current Frontex scandals of collusion with Libyan criminals wearing border guards' uniforms.

Migration and Border Studies 52; Médéric Martin-Mazé and Sarah Perret, 'Designs of Borders: Security, Critique, and the Machines' (2021) 6(3) European Journal of International Security 278 <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/designs-of-borders-security-critique-and-the-machines/8DB8A6640CA79355650EE731EE4F5455> accessed 14 July 2021.

9 Thomas Mathiesen, Siste Ord Er Ikke Sagt. Schengen Og Globaliseringen Av Kontroll (Pax Forlag 2000) 113.

Smart borders do not generate equal treatment and protection, but even more suspicion, surveillance, and exclusionary practices than human controls.

Until now, this guild of data managers and systems engineers has rarely been studied in detail, except through the specific prism of a 'European war on migration', in which a defence-surveillance industrial complex is building physical, maritime, and virtual 'walls' (TNI reports, Fortress Europe blogs). My own research is based on the results of the FP7 and Horizon 2020 grant-funded projects in which I have participated, enhanced by archival research, detailed findings of the European Commission reports, and my own participation in reporting for the European Parliament.10 From this background, I slightly disagree with the common framing in terms of a 'war machine', building 'electronic walls' blocking, stopping, and even killing people, as digitalisation of borders is based on the principle of 'letting people move', often presented as freedom of movement. But what have been called "smart borders" are different from the principle of 'free movement'. They often involve a form of movement under permanent surveillance, as

10 Methodological note: after the FP7 research programme SOURCE, an informal group of researchers have shared their different personal archives. Some were transcriptions of the early negotiations around Schengen, shedding light on some of the concerns raised at the time regarding 'compensatory measures', and the (un)desirable and technological solutions. They were completed with interviews and sessions of collective discussion, after the colloquium '30 Years of Schengen', in 2015, organised by King's College London and CEPS-Brussels. A paper by Christina Oelgemöller, Leonie Ansems de Vries, and Kees Groenendijkhas has already been published: 'The Crafting of a Paradox: Schengen inside and out' (2020) 6(1–2) International Journal of Migration and Border Studies 7. Didier Bigo, Emma McCluskey, Elspeth Guild, and Federica Infantino have also contributed to the group, especially on the last-mentioned topic. Inside this group, Didier Bigo, with the help of some professionals trainers of local trainers in police and border guard schools, carried out interviews with, and/or submitted questionnaires to, some of the first technicians of the companies involved at the beginning of Schengen. They asked for anonymity, including the names of their companies, as they were a very small group. In total, using the snowball effect strategy, we carried out more interviews (twenty-three in total) with their successors, and some who had entered into other groups (GoP, ESRAB, and ESRIFF). This paper is informed by these documents and interviews. See also the research of Martin Mazé and Sarah Perret : The Power Elite of Security Research in Europe (to be published 2023)

.

travellers forget that, by delivering their data in advance, they have allowed dataveillance by machines tracing their data doubles, and checking them like objects at the point of 'delivery'.

The lack of physical checks during travel, and the speed of this travel, do not constitute a form of freedom, but a convenient way of accepting surveillance. Thus, 'permitting mobility' works differently from stopping people, and from the image of walls. Most people crossing borders accept the situation, through the illusion that they are free because they are not stopped and checked as frequently as before. On the other hand, a small minority of travellers are under 'supplementary investigations', and blocked on the bases of poorly validated suspicions. This digitalisation of border security is, therefore, not identical to a military strategy of deterrence and combat; it is a 'ban-opticon', producing the othering of minorities, and the normalisation of majorities, that (in)security professionals implement.11 It is a strategy of predictive policing, based on detection of anomalies via algorithms, intelligence, and remote surveillance.12

This chapter focuses on the eu-LISA agency, which, officially, is small, and was only created to provide a long-term solution for the operational management of large-scale IT systems, but which is also a de facto nexus of power for all agents straddling the public and private sectors, and who design

11 Didier Bigo, 'Globalized-In-Security: The Field and the Ban-opticon' in Naoki Sakai and Jon Solomon (eds), Translation, Biopolitics, Colonial Difference (University of Hong Kong Press 2006); Didier Bigo, 'Globalized (In)Security: The Field and the Banopticon' in Didier Bigo and Anastassia Tsoukala (eds), Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11 (Routledge 2008); Marie-Laure Basilien-Gainche, 'Leave and Let Die: The EU Banopticon Approach to Migrants at Sea' in Violeta Moreno-Lax and Efthymios Papastavridis (eds), 'Boat Refugees' and Migrants at Sea: A Comprehensive Approach (Brill 2016).

12 Claudia Aradau and Tobias Blanke, 'Governing Others: Anomaly and the Algorithmic Subject of Security' (2018) 3(1) European Journal of International Security 1 <https://www.cambridge.org/core/product/identifier/S20575637170001 41/type/journal_article> accessed 19 January 2019; Bonnie Sheehey, 'Algorithmic Paranoia: The Temporal Governmentality of Predictive Policing' (2019) 21 Ethics and Information Technology 49 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056888956&doi=10.1007%2fs10676-018-9489-x&partnerID=40&md5=3388d8a852deb1e7b72fc60910f3af7f> accessed 28 November 2021; Didier Bigo, 'Sécurité Maximale et Prévention? La Matrice du Futur Antérieur et Ses Grilles' in Barbara Cassin (ed), Derrière les grilles: sortir du tout évaluation (Mille et Une Nuits 2013).

the tools of the other agencies (Europol and Frontex), transforming, by their action, the way security is both framed and changed into a commodity.13 It is this security commodity that the companies working for the eu-LISA agency are integrating, like many other 'objects', into the so-called data revolution of artificial intelligence.

II Sociogenesis of Policing at Distance: Sovereignty and Digitalisation

The interest in border controls and the control of foreigners by police officers, in addition to the forces in charge of passports and visas, is consubstantial with the beginning of national police forces in the nineteenth century,14 while the development of bureaucracies issuing travel documents is even older.15 The differentiation of the border guard profession from the military and police has, for some time, reinforced the idea of physical borders as symbols of entry into another state, often protected by a no man's land. The connection between sovereign narratives and border controls, in a nationalist context, has been crucial for politicians, despite the world's economic transformations, and the intensity and speed of the travel of goods, money, ideas, and people.

The terminology of sovereign borders, linked with right-wing narratives considering flows as a change to the identity of those living for a long time in a specific territory, is not the right depiction of reality; it is more a fantasy, or a mask allowing people to believe that, by erecting new walls and controls, the state can regain power alone, and afar from the international systems of states and the world economy.16 Recent outbreaks of ultra-patriotic (right-wing nationalist) narratives have reinforced this idea of a link between border and sovereignty, even if, as explained by Wendy Brown, the vision of protecting the country with electronic walls is more a sign of a 'waning' of sovereignty than a sign of reclaiming this sovereignty in the face of a global world.17 This waning is the central element which leads to two crucial evolutions. First, the development of a border theatre where the different

13 Lucia Zedner, Security: Key Ideas in Criminology (Routledge 2009). 14 Gérard Noiriel, Chapitre 1—L'identification des Personnes in Crettiez X and Piazza P (eds), Du Papier à la Biométrie: Identifier les Individus (Presses de Sciences Po 2006).

15 John C Torpey, The Invention of the Passport: Surveillance, Citizenship and the State (CUP 1999); Federica Infantino, 'The Politics of Management' in Federica Infantino (ed), Schengen Visa Implementation and Transnational Policymaking: Bordering Europe (Springer 2019).

16 Conor Gearty, On Fantasy Island: Britain, Europe, and Human Rights (OUP 2016).

17 Wendy Brown, Walled States, Waning Sovereignty (Zone Books/MIT Press 2010).

governments are happy to show that they brutalise unwelcome people at the borders, in a false hope of deterring them. Second, the development of digital forms of surveillance—less coercive, but more present, than traditional security—by tracing the data doubles of people, from their decision to travel, to their arrival. This evolution towards digital surveillance creates a chasm between an apparent depoliticisation of security as a technical issue, and a de facto political move in which bureaucrats and corporate actors decide about the effective travel measures and short-term migration rules: a sign of the ambiguous relationship between sovereignty, security, politics, and borders. Paradoxically, this technicisation of security gives state leaders and politicians more freedom to develop their own narratives on border policing, clearly disconnected from practice, by organising a political spectacle aimed at mobilising, within their political parties, the anxieties and uneasiness of an electorate in search of law and order, but without seeking to effectively regulate the long-term movement of foreigners. From the mid 1980s onwards, the strategy of transforming political choices concerning freedom, and its limits in democracies, into a technical debate on the best solutions for effective security, has led, in many countries, and at the institutional level of the EU, to the creation and multiplication of groups and subgroups of 'experts'. These European, and sometimes international, groups have collaborated transnationally to develop more knowledge exchange, more information sharing, and thus more electronic data, and the vision of a data 'container', accumulating as much electronic data as possible (including, but not limited to, personal data), allowing them to filter who travels.

Thus, politics has not disappeared. Rather, it has been displaced into bureaucratic networks and private corporate interests, the latest of which links border security to digital 'solutions'. The digital 'solutions' put in place have hardly ever been questioned, and, on the contrary, they have been extended beyond the area, and have also been developed nationally by the opponents to this Schengen area of freedom of movement, like the UK. The construction of a surveillance industry, under the label of civil security, has, therefore, developed silently, with little criticism. How was this possible? How have countries like Sweden, for example, been able to develop such an industry, while keeping the image of a peacebuilder? It is still difficult to answer these questions empirically. Nevertheless, some partial records of the discussions in the subgroup committees between 1985 and 1990 are now available, after thirty years of silence, and they are illuminating about the discussions and objectives of that time.18

A The Schengen Agreements and the SIS-SIRENE Innovations

18 A paper issued from the research described in n 10 has already been published: Oelgemöller, Ansems de Vries, and Groenendijk (n 10).

The Schengen Agreement (Schengen I) of 14 June 1985 regulated traffic between the Benelux countries, Germany, and France, while endorsing freedom of movement as a means of transforming the Common Market into an EU project. The principle of free movement of persons, for all inhabitants of those countries that were ready to move in this direction, was accepted. Nevertheless, negotiations continued after the signing of the 1985 text, to resolve what the German minister of the interior saw as a risk of the free circulation of criminals. Specific subgroups were set up to draft the agreement of 1990. The linking of crime/terrorism with the international mobility of (certain) persons, and the development of border control technologies, were thus concomitant with the opening-up introduced by this rather confidential document.19

Within the various subgroups that aimed to create a convention—eventually signed, as the Convention Implementing the Schengen Agreement (Schengen II), five years later, in June 1990—a key subcommittee was called the 'Horizontal Group', as it crossed all areas of terrorism, crime, and migration, analysing ways of collaboration, and introducing ideas of new technologies, beyond fax machines. At the beginning, it was only a small group of specialists from a few private companies linked to government authorities, and even a few police officers with knowledge of computer systems, who were involved in the development of a Schengen Information System, or 'SIS' (competing, at that time, with another project called EIS—European Information System).20 As some of these practitioners said in interviews, their different companies worked immediately on a solution refusing a central technology as it may have "helped" a federalist view of EU and they integrated politics deep into their technical designs. The German company Siemens teamed up with a Franco-Belgian-American company, Honeywell Bull, to form a consortium for the hardware of the SIS, while Steria (which would become later SopraSteria), a computer systems company of French origin, but widely distributed in Europe, developed specific software and data architecture. While the national defence industries were present in the competition to build the IT system, in the early 1990s they considered EU internal security to be too small a market. As a result, small start-ups challenged the traditional defence companies such as Thales or Finmeccanica (now Leonardo), and produced 'lighter' technologies adapted to police budgets; but this changed in the 2000s, as we shall see.

The reason for emphasising these origins is that some of these early corporate players are still in the consulting business today, and are influential

19 Guild and others (n 8); Oelgemöller, Ansems de Vries, and Groenendijk (n 10).
20 Didier Bigo and others (eds), The Routledge Handbook of Critical European Studies (Routledge 2020).

beyond border management. This history is full of individual continuities, masked by changes of companies, and by mergers, or the acquisition, by large companies, of smaller ones (for example, the creation of the DIS of Thales through the acquisition of a small company, or the financial merging of Sopra and Steria, and so on). Some of these 'pioneers', as they call themselves, explained during interviews that they regularly met among themselves, and with their 'stakeholders', in specific subgroups, appreciating their diversity of nationalities but their technical homogeneity. They 'felt at home', and said they were 'surprisingly free' to work, because the stakeholders could not give them a clear vision of what they wanted, except for basic arguments about the danger of centralisation, if centralisation favoured the European Commission over the national ministries of interior. For thirty years, from the 1990s onwards, they have been in various colloquia, and groups of 'personalities', a terminology later validated by the European Commission for setting up the first series of calls on internal security, led by DG Research and DG Enterprise.21

As a result of these struggles over speed, capacity, price, and ease of use for end users, the first SIS consisted of a central technical node, C-SIS, based in Strasbourg, which did not contain any information, but had the capacity to connect the various national databases where data were stored. The complete architecture included, in addition to the local SIS and C-SIS, the so-called SIRENE mechanisms, which allowed the national magistrates delegated to the 'additional information required at national entry' ('airne' or 'sirene') to assist law enforcement agents in querying other national authorities, in order to identify suspects through requests for additional information. As Thomas Mathiesen and Statewatch revealed, the (then) confidential Sirene manual explained how to organise the operational links between the aliens databases and the police databases on criminals. Thus, even at its origins, the SIS-SIRENE was not only about border controls, but was created with the aim of raising additional suspicions of criminality, if persons were foreigners, migrants, or asylum seekers. While it was not an example of crimmigration as such, to the extent that the creation of criminal or administrative laws against foreigners was not involved, it was, nevertheless, a microprocess of (in)securitisation, transferring logics applied to tackle serious criminality to petty illegalities.22 This technological, digital system has helped to create a continuum of (in)security between anti-terrorist and anti-immigration

21 J Peter Burgess, Handbook of New Security Studies (Routledge 2010). 22 Mathiesen (n 9).

practices,23 generating discussions in critical security studies and immigration studies about its breadth and depth.24

In fact, the division into national markets did not work, and transnational companies played a key role in introducing innovations on the 'proactive' possibilities of digital applications. Corporate computer scientists, who were less mathematicians working on algorithms than systems engineers, became valuable, and many of them have, in the course of their careers, crossed the boundaries between the public and private sectors. Together, these IT system specialists with experience in security issues were mainly in control of the technical design, and understood each other, but the traditional police and border organisations were, nevertheless, adamant about certain objectives, notably the speed of the system, which they saw as the symbol of efficiency. Very soon, the question of the validity of the digital 'revolution' came to a halt, and the interconnection of computers appeared to be the only solution to unify the geographical space of the growing number of Schengen countries. All the experts stated that, without high-speed connections, the goal of control of people at the borders was not possible, across such a large area. On arrival at external borders, checks on passengers had to be compatible with the imperative of not slowing down the flows beyond about twenty seconds per person. Freedom of movement and control of persons were, thus, linked, and transformed into the speed at which controls occur.25

B Broadening of the Schengen Area, and Resistance to Reconfiguring the SIS Design into Predictive Policing Tools

Roughly finalised in 1988, at the Palma conference, the Schengen Convention of 1990 took two additional, crucial years of reflections on the nature of the Schengen Area, in relation to free movement and security issues, via the SIS. Events of 1989, including the end of the Cold War, and the collapse of the Soviet bloc, which resulted in the reunification of East Germany with the West, and the attachment of Central and Eastern European countries to NATO and the EU, further complicated matters, in terms of freedom of movement in the Schengen Area. Borders in Europe

23 Didier Bigo, 'Terrorisme, Drogue, Immigration: Les Nouvelles Figures de l'insecurite en Europe' (1995) 30(70) Revue Internationale d'Action Communautaire 43; Jef Huysmans, 'The European Union and the Securitisation of Migration' (2000) 38(5) Journal of Common Market Studies 751.

24 Mary Bosworth and Mhairi Guild, 'Governing through Migration Control: Security and Citizenship in Britain' (2008) 48(6) British Journal of Criminology 703.

25 Vicki Squire, The Contested Politics of Mobility: Borderzones and Irregularity (Routledge 2010).

were physically moving faster than EU politicians had envisaged.26 The logics of control were changed materially, in terms of infrastructure, beginning with Germany. Thinking of borders as more mobile and fluid, and less tied to their physical dimension, became an imperative that the digitisation of data made possible. What was still a marginal issue became an absolute priority, in the various meetings of the Schengen subgroups.

Remote control by digital means was no longer a potentiality; it became a common practice. The control was to be carried out upstream and downstream of the border, with the border being only the place of expression of the data gathered previously by the security forces (police and intelligence), and the place where state coercion applied more easily to foreigners (the citizen of other states), in the name of a shared territorial sovereignty around a 'space' of free movement. Telecommunication companies and national technology leaders on computer systems, have grouped themselves into associations lobbying for the police, and vice versa. The struggles between the Schengen countries and the European Commission came to an end, first with the adoption of the Schengen system by almost all member states, and later when the Schengen agreements became part of the third pillar of the EU.

The enlargement of the EU with ten new member states from Central and Eastern Europe was less of a technical challenge for the SIS, as reported in the press, than a struggle of visions about the future role of digital technologies. Respondents recalled that the companies in charge of the Schengen infrastructure were in favour of developing search tools in the system, to give a practical dimension to the discourse on preventive crime and proactive policing. They insisted on the creation of a SIS 2, in particular with the European Commission's DG, which wanted to have more direct contacts with the United States, Canada, and Australia worldwide. Nevertheless, this reframing of the tools was too costly, and the Portuguese Presidency succeeded in destabilising the technical oligopoly of these large firms from Germany and France, but also from Spain, Italy, and even Israel. With the help of a Portuguese start-up that offered all the new (Eastern) member states a technology called 'SIS 1 for all', they won most of the market. The Portuguese company was adjusted to the same logic of limiting digitalisation to border authentication, but with fast connections. 'SIS 1 for all' was designed for border control, but not for police and suspect investigation. This reversal shows that the market was not completely in the hands of the initial actors and big companies. The major companies were

26 Gerrit Huybreghts, 'The Schengen Convention and the Schengen Acquis: 25 Years of Evolution' (2015) 16 ERA Forum 379.

upset by this 'unexpected' limit to their ambitions. But the situation changed after 2001, or more precisely, for the EU, after 2004.27

III The Changing Boundaries of the Digital Security Technology Domain and the Impact of Corporate Actors

As long as the number of internal security databases was limited, and they were managed directly by the structures of the EU Commission, the empowerment of the field was a concern for border security actors, but the impact was still marginal for other security professionals. Nevertheless, the logic of preventive policing, integrated with digitalisation tools, explains why promoters of global counterterrorism, after 2004, have facilitated the expansion of the field and its importance. The multiplication of the number of databases, the facilitation of access to them for various purposes, and the speed of connections, became key factors for the development of surveillance tools during the travel process. Corporate actors specialising in IT systems infrastructures met regularly with security professionals, until a certain 'craft' shared by different people emerged, and pushed them to try to institutionalise their relationships (see later). Specific grants, specific arenas, and specific agencies for IT systems have maintained this 'entre-soi' around the idea of interoperability of IT systems designed for internal security, even if they are now challenged by the attractiveness of their own field, which

27 Elif Kuskonmaz and Elspeth Guild, 'Rights-based Review of Border Surveillance' in Ramona Grimbergen, Aniel Pahladsingh, and Dean Spielmann (eds), The Charter and the Court of Justice of the European Union: Notable Cases from 2016–2018 (Wolf Legal Publishers 2019) <https://researchportal.port.ac.uk/portal/en/publications/rightsbased-review-of-border-surveillance(f4c64e48-db64-4788-8b15-353123d3ec86)/export.html> accessed 14 July 2021; Niovi Vavoula, European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications (Queen Mary School of Law Legal Studies Research Paper) (2017); Niovi Vavoula, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-country Nationals?' (2020) 26(1) European Public Law 131; <<<REFO:Other>>>Didier Bigo and others, 'Analytic Report: Visualisation on Societal Security Networks in Europe' <https://researchportal.port.ac.uk/portal/en/publications/analytic-report-visualisation-on-societal-security-networks-in-europe(a17e2c3a-1059-4225-9cbb-6a1570e2f721).html> accessed 7 February 2020; Didier Bigo, 'Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?' in Didier Bigo and others (eds), The Routledge Handbook of Critical European Studies (Routledge 2020).

attracts public and private defence actors, intelligence services, and/or cybersecurity specialists.

A The Proliferation of Police Data Highways: An Anti-terrorist Solution or an Institutionalisation of the IT Systems inside the Security Field?

Since the declaration of the war on terrorism, and the creation of a Department of Homeland Security, the US government has been pushing hard for transatlantic information sharing, especially on air travellers (API-PNR, visa programmes, entry/exit systems, travel authorisation, and no-fly lists). It is impossible to detail the transactions of this period, but many companies found that border security, which still had a small budget compared to defence, was, nevertheless, the most profitable of all time. Any bold idea was funded, and the development of the Internet, as well as the acceleration of broadband in submarine cables, gave data transfer the high speed needed for 'real time' action. The European Commission welcomed the 'pioneers' of the SIS, and from then on, EU money flowed in to develop this infrastructure, linking the so-called external borders with internal controls. After the Madrid bombing in 2004, the EU pushed EUMS companies to create specific joint ventures, in order to achieve economies of scale, and compete with the US 'civil security' industry. In a few years, SIS became SIS2, transforming the use of SIS; SIS was complemented by a VIS (Visa Information System), and became interconnected with other databases (see below). The creation of multiple databases, protected by the legal principle of purpose limitation, in terms of access, which was at the heart of the functioning of the area of freedom, security, and justice over the previous twenty years, has been reversed. Access to law enforcement authorities (police, border guards, criminal justice, and even administrative bodies (prefectures)) has been granted for almost all databases. This has radically changed practices and legal implications.28

In the mid 2000s, therefore, a series of 'internal' security databases in Europe proliferated, and their interoperability was planned. But it nevertheless took ten years, until 2015, to give them some semblance of a legal basis, while their links, and interoperability tools, were similarly slow to implement. Connecting heterogeneous databases on consumer preferences, entry checks, and travel authorisations, with specific categories of people wanting or needing to travel, in pursuit of the aim of turning this IT architecture into preventive policing tools, took time. The creation of these 'police data highways', by data analysts and systems engineers who specialised, over the years, simultaneously in border control and surveillance technologies, and in preventive and predictive tools based on the algorithmic claim to anticipate the future, has changed the dynamics of border control. The border controls

28 Vavoula, 'Interoperability of EU Information Systems' (n 27).

are now relying, increasingly, on digital information arriving before people reach the border, and they leave border guards with a narrow margin of autonomy. Thus, although most border guards still insist that they are based at the borders, and have the ultimate and sovereign right to decide who enters, and who is refused entry, the development of electronic visas, specific visitor programmes, and timely access to these data highways, have de facto moved the modalities of authentication, verification of documents, and pre-travel authorisations 'upstream'. 'Upstream' means that sending countries are obliged to collaborate with European police forces, and to prevent part of their own populations from leaving; that consulates have an important role in filtering access to travel; and, most importantly, that temporal, predictive, or at least 'on-time', decision-making, aggregating digital data from different databases, is carried out. Digitalisation allows for pre-transit, or in-transit, surveillance of a specific identified person, and for some potential offences, the unidentified individuals are also tested against (semi-automatic) risk profiles, based on categorical suspicion by association.

The interest in the avatar, or 'data double', of suspicious persons, and its ex ante identification, even before the control of persons, is becoming routine in airports, with Passenger Name Record (PNR), and new entry/exit systems. Of course, these territorial and digital logics have been combined, and this is why data management continues to use the territorial borders of the state as a place to extract (with a certain degree of discretion) data from people who want to travel; but their priority was, and is, to build algorithms on criteria of dangerousness, and to calculate scores on a scale of risk and suspicion, suggesting that individuals who have not yet done anything but resemble criminals are likely to be suspected a priori.

These changes were not made at random. They have been orchestrated by the 'new' eu-LISA agency, which has integrated, into its staff, the previous networks of corporate systems engineers, IT architecture designers, and public agents coming from proactive policing sectors.29 This is why this European agency looks like the 'camera obscura' lens of the entire landscape of internal and border security. Certainly, information is still very fragmented, and confidentiality—even secrecy—is very high. Nevertheless, more recently, some elements of its role have been studied by researchers.

B The Creation of eu-LISA, and the Role of Corporate Actors in the Making of a Specific Guild of Data Managers

Created in 2011, after a lapse of five or six years, and only operational on 1 December 2012, the eu-LISA agency presents its role as the implementation

29 Georgios Glouftsios, 'Governing Border Security Infrastructures: Maintaining Large-scale Information Systems' (2021) 52(5) Security Dialogue 452.

of EU justice and home affairs policies, through the management of large-scale IT systems. Eu-LISA is responsible for all the interconnections between the databases, and their future developments in terms of global interoperability, but it has no power over the day-to-day management given to the users, and is bound by the different legal agreements between the countries, as well as the ongoing debate on the distinctions between internal or civil security and defence.

Always downplaying their role, as mere 'digital plumbers', the staff of eu-LISA has shown restraint, with only 137 people in 2019, spread over three sites: the headquarters in Tallinn, Estonia; the operational site in Strasbourg, France; and a backup site in Sankt Johann im Pongau, Austria. Officially, they claim to support the technical infrastructure used by Europol and Frontex operations, but most of the few independent studies show their key role, and the agency's multi-positioning.30 This 'modesty' contrasts sharply with the self-promotion of the other agencies, be it Europol, Frontex, or Eurojust. It also explains why the public and journalists, and even 'experts', ignore them. On the other hand, according to the eu-LISA interviewees, they are not technicians at the service of the other agencies, but visionaries of a future in the making, through the implementation of global smart cities, in smart countries, via smart borders. Eu-LISA's first major operation was to establish the full implementation of SIS 2, on 9 April 2013, after more than five years of delays and complaints between the company Sopra Steria and eu-LISA, but de facto pushed by the Commission, and even more so by the European Parliament's LIBE Committee. Instead of highlighting the tremendous differences between SIS1 and SIS2, they present SIS2 only as a more modern system, offering additional functionalities that have come into use, and which concern objectives such as border control, national security, or law enforcement. Nevertheless, they stress that operational research, and the ability to process images, are essential for 'police work'.31 SIS2 has also been complemented by the Visa Information System (VIS), and access to Eurodac has been extended to all national police forces and Europol, in order to compare fingerprints taken in criminal investigations with those of asylum seekers and migrants in Eurodac. In the near future (end of 2022-2023), three new databases will be operational into the EU IT architecture. They are the European Travel and Authorisation System (ETIAS), the European Electronic System (EES), and the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN). Julien

30 Multi-positionality refers to actors who are in dominant positions in different fields, cf Didier Georgakakis, 'The Historical and Political Sociology of the European Union: A Uniquely French Methodological Approach?' (2009) 7(3) French Politics 437.

31 Akkerman (n 7).

Jeandesboz has described these databases and their implications for travellers in detail.32 The most important task was, nevertheless, to create the 'interchange' between these 'data highways'. This work, done in close association with the corporate companies they have worked with previously, and in particular the digital company Sopra Steria, has changed everyday practices at the borders and beyond. Krum Garkov, executive director of eu-LISA from the creation of the agency, declared recently, '[d]igital transformation is one of the building blocks of Next Generation EU and eu-LISA is the Agency delivering the necessary digital platforms, to justice and home affairs communities, that provide tangible benefits for EU citizens, enabling the practical implementation of one of their fundamental rights – freedom of movement' (26 November 2020). But can we agree with this statement? Are interoperable databases the implementation of freedom of movement, or an instrument of surveillance? Contrary to many traditional analyses of European studies that read the interoperability programme as being a result of the 2015 terrorist attacks, and the European Commission's desire to show that, on these cross-border issues between France and Belgium, they were useful, and as 'tough' as national governments, the author reject the idea that they were a result of this crisis of 2015, and that they are now the best tools of protection of our freedoms. As we have seen, the interoperability project existed long beforehand, and if the attacks in Paris and Brussels were used as a political opportunity by a group of professionals to strengthen their positions, they were not a 'fresh response to the bombings'. In a discussion that started in 2005, in the transatlantic arenas, and which crystallised in 2013, before being implemented in 2017, after four years of intense debate, the full discussion on interoperability and the construction of highway interchanges was, on the contrary, reduced to the IT tools already belonging to eu-LISA.

The five tools of the Commission proposal constituted a de facto induction course towards the goal of predictive analytics, and they were presented in a specific order, starting with a single search interface; then a uniform interface protocol; thirdly, a shared biometric system; fourthly, a common identity repository; and, finally, a multiple-identity detector, wanted by the Commission despite the initial reluctance of the high- level expert group to validate this last 'tool'.33 The argument of detecting fraudulent identification was envisaged to be applied against each passenger. This extension of targets

32 Julien Jeandesboz, 'Smartening Border Security in the European Union: An Associational Inquiry' (2016) 47(4) Security Dialogue 292. See also migration, security, surveillance in Europe Ryerson workshop 2019–under publication.

33 For more details, see Emma McCluskey, in special issue (2020) 6(1–2) International Journal of Migration and Border Studies.

was associated, beyond fraud, with the search for overstayers via the procedures of the European exit systems, and with the control of biometric identifiers, facial recognition, and internal EU PNR for the detection of suspected 'radicalised' EU citizens. Many non-governmental organisations, therefore, challenged the overall logic of connecting the dots at all costs, on everyone. In this ongoing struggle, the weight of corporate actors who wanted to develop a digital industry in a context of 'global war' was crucial, but it should also be read also as a competition between the EU and the US for the control of the cybersecurity market. While some key players remain, it would be wrong to see only continuities. Seniority in the field has given powerful positions to the winners of the first battles, who have been influential in the way in which so-called technical solutions have framed the imaginary of the conceivable use of databases for security reasons. These winners, such as Sopra Steria or GMV, benefited from continuous subsidies, specific calls for tenders that they managed to 'inspire', in which they had niche markets, and social recognition abroad. Nevertheless, their previous autonomy changed when the big operators of the defence industry, such as Leonardo or Thales, after 2004, and more clearly after 2015, decided to recolonise the civil security market on border infrastructures, and also on digital technologies. Thales, for example, has proposed new packages with a wide range of military and security equipment, including biometric identification systems. Border infrastructure has been the logical entry point, through the connection with military logistics (see Thales, for example), but they have also acquired specific companies to complete their 'offer' for digital border technologies tenders.

In all these transactions, the current European Organisation for Security (EOS), which is now one of the most powerful lobbying organisations, and has its origins in the SIS, organises the convergence of military and digital technologies under the name of cybersecurity. In conjunction with the Frontex and LEA networks, some colloquia have been de facto informal negotiations between the military and the civil security firms, and have been the vehicle for these mergers of interests. According to Akkerman, and to give just one example, 'in 2019, Thales acquired Gemalto, a large (biometric) identity security company, for €4.8 million, integrated as its Digital Identity and Security (DIS) division. In 2017, Gemalto had purchased 3M's identity management business, which included Cogent Systems (acquired by 3M in 2010) for $850 million. Between 2000 and 2017, Cogent and 3M were returning partners in a consortium led by Sopra Steria for several large European contracts for the development and maintenance of EURODAC, VIS and SIS II. Gemalto, formerly Cogent, also provides the fingerprint identification technology for the EURODAC database.'34

34 Akkerman (n 7) 37.

Recently, most of the major EU contracts for digital security have been awarded to just two companies: Sopra Steria for data highways, and GMV for Eurosur. It is far from an open competition, and it seems that the logic follows more of a 'mercantilist approach' in a 'strategic area' than that of a free market. Nevertheless, the field of digital surveillance technologies, which was almost ignored, has become more visible, due to the scandals involving its end users: Europol, but also, and especially, Frontex. Their actions have created a backlash against the role of digital surveillance.35

IV Conclusion: Security Techno-solutionism—how to Fail Successfully

Intellectually, the distinctions between digital and physical, private and public, and data-embedded knowledge and privacy, which were the last boundaries, had to be dissolved, in order to achieve a form of totalisation of security through its integration in a large-scale project linking military and civilian components, and national and European space. Security is no longer a goal to be achieved, but a condition of life in modernity. Technologies invented by private companies in the civil protection and security sector, designed to combat clandestine organised violence, are being tested for use to combat crime, incivilities, illegal aliens, or even deviant non-violent behaviour. The interoperability of data related to crowd detection and composite facial recognition, behavioural anxiety detectors, operate in certain locations (often airports), and work in a systematic way to do this kind of investigation while not spending too much time in human investigation. Or, at least, it is the dream of this programme that, if it is impossible to obtain intimate knowledge of all travellers protected by privacy regulations, they nevertheless have to detect weak signals of dangerousness remotely, by associations based on suspicions only.

The guild of data managers and IT systems engineers have, therefore, transformed what security does, and what it means. As we have seen, they do not agree with traditional security professionals, and in particular, with border guards. They have different appreciations of the means of achieving security, and they sometimes also prioritise the most important dangers differently. They are more pretenders than heirs, in the general field of security professionals, but they have the advantage that their vision is attractive to politicians, and the highest levels of management in public administrations. This gives them a strong influence, today, on all issues

35 Claudia Aradau, 'Experimentality, Surplus Data and the Politics of Debilitation in Borderzones' (2020) 0 Geopolitics 1 <https://doi.org/10.1080/14650045.2020.1853103> accessed 14 July 2021; Martina Tazzioli, 'What Is Left of Migrants' Spaces? Transversal Alliances and the Temporality of Solidarity' (2020) 1(1) Political Anthropological Research on International Social Sciences (PARISS) 137.

where digital technologies are involved in tackling terrorism, crime, migration, and fraud.

Nevertheless, it is important for scholars to ask what legitimacy the data managers have to decide, in advance, on these IT infrastructures of security, and then to present them as necessities. Their narrative often recognises that these technologies can fail, but they consider that they just need to be improved, not discontinued. And to convince their opponents, they often insist that the cost of investment is so great that the only solution is to continue to develop and correct the technologies,36 a narrative of techno-solutionism already used to justify smart cities initiatives. Their practices of digital security, and building data highways, have not created smart ways of travel with more protection and more freedom of movement; they have used border controls to their own aims, capturing more data for the global surveillance of travellers, and the people who are receiving foreigners as guest too often (VIS, ETIAS, and PNR). They have accentuated the 'ban-opticon' logic described earlier. The digital technologies they use refine their targets through more complex profiling, but they also extend the observation of the social network via a suspicion of criminality by association, and they manage to do so without major protest, as long as they do not affect the majority of people, and are presented to them as a benign protection of their way of life, or the means to achieve a bright utopian future of smart borders and cities regulated by future programmes integrating artificial intelligence.37

References

Abrahamsen R and Leander A, Routledge Handbook of Private Security Studies (Routledge 2015)

— — and Williams MC, 'Security beyond the State: Global Security Assemblages in International Politics' (2009) 3 International Political Sociology 1

Akkerman M, The Business of Building Walls (Transnational Institute 2019) <https://www.tni.org/files/publication-downloads/business_of_building_walls_-_full_report.pdf>

36 Paul Watzlawick, Ultra-solutions: How to Fail Most Successfully (WW Norton & Co 1988); Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (US Public Affairs 2013).

37 <<<REFO:WBLN>>>Marco Marsili and José Borges, 'The European Union Artificial Intelligence Strategy' (Zenodo, 28 June 2021) <https://zenodo.org/record/4972574#.YaPFDC2l10s> accessed 28 November 2021.; See also the new Horizon Europe security research programme: <https://ec.europa.eu/programmes/horizon2020/en/area/security> accessed 16 December 2021.

Aradau C, 'Experimentality, Surplus Data and the Politics of Debilitation in Borderzones' (2020) 0 Geopolitics 1 <https://doi.org/10.1080/14650045.2020.1853103>

Claudia Aradau and Tobias Blanke, 'Governing Others: Anomaly and the Algorithmic Subject of Security' (2018) 3(1) European Journal of International Security

Basilien-Gainche M-L, 'Leave and Let Die: The EU Banopticon Approach to Migrants at Sea' in Moreno-Lax V and Papastavridis E (eds), 'Boat Refugees' and Migrants at Sea: A Comprehensive Approach (Brill 2016)

Bigo D, 'Terrorisme, Drogue, Immigration: Les Nouvelles Figures de l'insecurite en Europe (Terrorism, Drugs and Immigration: The New Faces of Insecurity in Europe)' (1995) 70 Revue Internationale d'Action Communautaire 43

— —, 'Globalized-In-Security: The Field and the Ban-opticon' in Sakai N and Solomon J (eds), Translation, Biopolitics, Colonial Difference (University of Hong Kong Press 2006)

— —, 'Globalized (In)Security: The Field and the Banopticon' in Bigo D and Tsoukala A (eds), Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11 (Routledge 2008)

— —, 'Sécurité Maximale et Prévention? La Matrice du Futur Antérieur et Ses Grilles' in Cassin B (ed), Derrière les grilles: sortir du tout évaluation (Mille et Une Nuits 2013)

— —, 'Sociology of Transnational Guilds' (2016) 10 International Political Sociology 398 <http://ips.oxfordjournals.org/content/10/4/398>

— —, 'Adjusting a Bourdieusian Approach to the Study of Transnational Fields' in Schmidt-Wellenburg C and Bernhard S (eds), Charting Transnational Fields: Methodology for a Political Sociology of Knowledge (Routledge 2020)

— —, 'Interoperability: A Political Technology for the Datafication of the Field of EU Internal Security?' in Bigo D, Diez T, Fanoulis E, Rosamond B, and Stivachtis YA (eds), The Routledge Handbook of Critical European Studies (Routledge 2020)

— —, Diez T, Fanoulis E, Rosamond B, and Stivachtis YA (eds), The Routledge Handbook of Critical European Studies (Routledge 2020)

Bosworth M and Guild M, 'Governing through Migration Control: Security and Citizenship in Britain' (2008) 48(6) British Journal of Criminology 703 <https://academic.oup.com/bjc/article-lookup/doi/10.1093/bjc/azn059>

Brouwer E, 'Digital Borders and Real Rights: Effective Remedies for Third-country Nationals in the Schengen Information System' (Brill 2008)

Brown W, Walled States, Waning Sovereignty (Zone Books/MIT Press 2010)

Burgess JP, Handbook of New Security Studies (Routledge 2010)
Côté-Boucher K, 'Smart Borders? Customs, Risk Targeting, and Internal Politics in a Border Agency' in Hannem S, Sanders C, and Schenider C (eds), Security and Risk Technologies in Criminal Justice: Critical Perspectives (Canadian Scholars Press Inc 2019)
Feldman G, The Migration Apparatus (Stanford University Press 2020)
Gearty C, On Fantasy Island: Britain, Europe, and Human Rights (OUP 2016)
Georgakakis D, 'The Historical and Political Sociology of the European Union: A Uniquely French Methodological Approach?' (2009) 7(3) French Politics 437
Glouftsios G, 'Governing Border Security Infrastructures: Maintaining Large-scale Information Systems' (2021) 52(5) Security Dialogue 452 <https://journals.sagepub.com/doi/10.1177/0967010620957230>
Guild E and others, An Analysis of the Schengen Area in the Wake of Recent Developments (CEPS 2016) <https://www.ceps.eu/ceps-publications/analysis-schengen-area-wake-recent-developments/>
Huybreghts G, 'The Schengen Convention and the Schengen Acquis: 25 Years of Evolution' (2015) 16 ERA Forum 379
Huysmans J, 'The European Union and the Securitisation of Migration' (2000) 38 Journal of Common Market Studies 751 <http://onlinelibrary.wiley.com/doi/10.1111/1468-5965.00263/abstract>
Infantino F, 'The Politics of Management' in Infantino F (ed), Schengen Visa Implementation and Transnational Policymaking: Bordering Europe (Springer 2019) <https://doi.org/10.1007/978-3-030-10647-8_5>
Jeandesboz, J, 'Justifying Control: EU Border Security and the Shifting Boundaries of Political Arrangement' in Bossong R and Carrapico H (eds), EU Borders and Shifting Internal Security (Springer 2016)
— —, 'Smartening Border Security in the European Union: An Associational Inquiry' (2016) 47 Security Dialogue 292
Kuskonmaz E and Guild E, 'Rights-based Review of Border Surveillance' in Grimbergen R, Pahladsingh A, and Spielmann D (eds), The Charter and the Court of Justice of the European Union: Notable Cases from 2016–2018 (Wolf Legal Publishers 2019) <https://researchportal.port.ac.uk/portal/en/publications/rightsbased-review-of-border-surveillance(f4c64e48-db64-4788-8b15-353123d3ec86)/export.html>
Leese M, 'Exploring the Security/Facilitation Nexus: Foucault at the "Smart" Border' (2016) 30 Global Society 412 <https://www.tandfonline.com/doi/full/10.1080/13600826.2016.1173016>

Marsili M and Borges J, 'The European Union Artificial Intelligence Strategy' (Zenodo, 28 June 2021) <https://zenodo.org/record/4972574#.YaPFDC2l10s>
Martin-Mazé M, 'Report: The Power Elite of Security Research in Europe: From Competitiveness and External Stability to Dataveillance and Societal Security' (2020) 6 (1–2) International Journal of Migration and Border Studies 52
— — and Perret S, 'Designs of Borders: Security, Critique, and the Machines' (2021) 6 European Journal of International Security 278 <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/designs-of-borders-security-critique-and-the-machines/8DB8A6640CA79355650EE731EE4F5455>
Mathiesen T, Siste Ord Er Ikke Sagt. Schengen Og Globaliseringen Av Kontroll (Pax Forlag 2000) (translated into English in Statewatch)
Morozov E, To Save Everything, Click Here: The Folly of Technological Solutionism (US Public Affairs 2013)
Noiriel G, 'Chapitre 1—L'identification des Personnes' in Crettiez X and Piazza P (eds), Du Papier à la Biométrie: Identifier les Individus (Presses de Sciences Po 2006) <https://www.cairn.info/du-papier-a-la-biometrie-identifier-les-individus--9782724609891-page-29.htm>
Oelgemöller C, Ansems de Vries L, and Groenendijk K, 'The Crafting of a Paradox: Schengen inside and out' (2020) 6 International Journal of Migration and Border Studies 7
Rodier C, Xénophobie Business (La Découverte 2012)
Schmidt-Wellenburg C and Bernhard S (eds), Charting Transnational Fields: Methodology for a Political Sociology of Knowledge (Routledge 2020)
Sheehey B, 'Algorithmic Paranoia: The Temporal Governmentality of Predictive Policing' (2019) 21 Ethics and Information Technology 49 <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85056888956&doi=10.1007%2fs10676-018-9489-x&partnerID=40&md5=3388d8a852deb1e7b72fc60910f3af7f>
Squire V, The Contested Politics of Mobility: Borderzones and Irregularity (Routledge 2010)
Tazzioli M, 'What is Left of Migrants' Spaces? Transversal Alliances and the Temporality of Solidarity' (2020) 1(1) Political Anthropological Research on International Social Sciences (PARISS) 137 <https://brill.com/view/journals/pari/1/1/article-p137_137.xml>
Torpey JC, The Invention of the Passport: Surveillance, Citizenship and the State (CUP 1999)
Vavoula N, European Travel Information and Authorisation System (ETIAS): A Flanking Measure of the EU's Visa Policy with Far Reaching Privacy Implications (Queen Mary School of Law Legal Studies Research Paper) (2017)

— —, 'Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-country Nationals?' (2020) 26 European Public Law 131 <https://www.kluwerlawonline.com/abstract.php?area=Journals&id=EURO2020008>

Watzlawick P, Ultra-solutions: How to Fail Most Successfully (WW Norton & Co 1988)

Zedner L, Security: Key Ideas in Criminology (Routledge 2009) <http://lib.myilibrary.com/?id=208467>