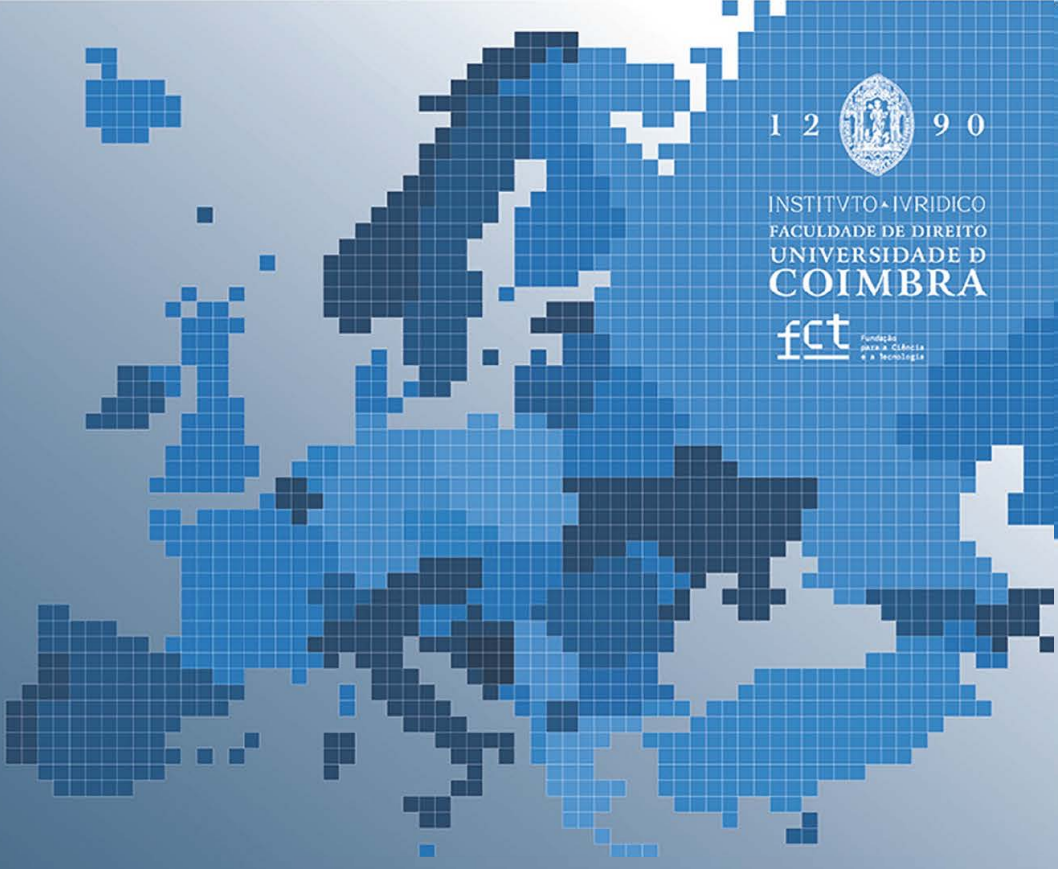

European Security, Borders, Crime and EU Law

Pedro Caeiro *(ed.)*

Didier Bigo
Elspeth Guild
Valsamis Mitsilegas
Ana Margarida Simões Gaudêncio
Dulce Lopes

TITLE
European Security, Borders, Crime and EU Law

EDITOR
Pedro Caeiro

EDITION
Instituto Jurídico
Faculdade de Direito da Universidade de Coimbra
geral@ij.uc.pt • www.uc.pt/fduc/ij
Colégio da Trindade • 3000-018 Coimbra

GRAPHIC DESIGN
Pedro Bandeira

COVER
Dalldesign

e-ISBN: 978-989-9075-88-7

DOI: https://doi.org/10.47907/EuropeanSecurityBordersCrimeandEULaw/Livro

August 2025

The present publication is part of the activities of IJ/UCILeR (Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra/University of Coimbra Institute for Legal Research), within the context of the strategic project UID 04643 – Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra (funded by FCT – Fundação para a Ciência e a Tecnologia).

Pedro Caeiro
Editor

European Security, Borders, Crime and EU Law

Authors
Ana Margarida Simões Gaudêncio
Didier Bigo
Dulce Lopes
Elspeth Guild
Pedro Caeiro
Valsamis Mitsilegas

INSTITVTO IVRIDICO
FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

Contents

Note from the editor

Borders: imaginary lines with very real consequences – legal, social, existential.

Crossing them entails risks, both for the resident population and for the foreigner. In Portuguese, *risco* denotes both risk and a line drawn on a surface, as, for instance, a dividing mark traced on the ground. Hence the expression *pisar o risco* (to step on the line), meaning imminent transgression (the crossing) that exposes the agent to risk. This linguistic peculiarity (I know of no other language in which this semantic overlap exists) is a vivid reminder that the border is more than a geopolitical device – it is also a calculation of exposure. Where a line is drawn, something is at stake – for the entitled and the *non-ayant droit* alike. The border becomes, for all parties, a symbolic locus of security (i.e., the successful management of risk), which, paradoxically, may drive them to adopt diametrically opposite behaviour: if need be, foreigners might be prepared to intrude illegally, whereas territorials might push them back illegally.

Borders are thus sites of power, vulnerability, crime and uncertainty. Over the last decade, the challenges they pose have grown more complex – empirically and normatively – prompting the Instituto Jurídico/UCILeR to host a seminar on the subject on 18 June 2024. We were privileged to welcome a distinguished group of scholars and practitioners, joined by invited guests and stakeholders, to explore topics such as: the outsourcing of border governance, public/private guilds, technocratic guilds (D. Bigo); the murky process of offshoring EU border anxiety to third countries (E. Guild); the several avenues used for criminalising migrants (V. Mitsilegas); the right to migrate as a human right (A. Gaudêncio) and the tensions between EU and (non-harmonised) domestic policies on integration (D. Lopes).

This e-book gathers the thoughtful papers presented at the seminar, followed by a brief epilogue of my own. I am deeply grateful to the authors for their engagement and generosity, and to the Coordination Board of the Instituto Jurídico for their unwavering support from the outset.

Caldas da Felgueira, 18 June 2025.

eu-LISA: The Emergence of a Digital Technology Guild and its Rise in the Field of EU Internal Security

(DOI: https://doi.org/10.47907/EuropeanSecurityBordersCrimeandEULaw/01)

Didier Bigo*

Abstract: This article seeks to explain the way in which security practices have changed over the last two decades, largely as a result of the emergence of specialists in the field of digital management of security tools, combined with arguments in favour of "preventive" security stemming from counter-terrorism policies. Even if the groups did not share the same beliefs and habitus, a centripetal dynamic of alliances was created, with a bandwagon of criminal investigation departments, border guards involved in intelligence gathering on drug routes and illegal migration patterns, as well as those involved in the administration of "preventive" criminal justice. From a marginal position in the field of security professionals, data managers, systems engineers and cyber security specialists have become a powerful group vying for control over the definition and implementation of security measures. The traditional view of liberal security as a trade-off for freedom of movement within the EU, or more specifically the Schengen area, has been challenged, despite its argument of a balance between freedom and security. This change in the dominant discourse has taken place in favour of an acceptance of a highly aggressive policy, in which the term "preventive" is often used to describe a practical organisation of a priori suspicion, tools of digital collection, biometric elements of populations of travellers, filtering of "groups of interest" through algorithmic research, and surveillance in the name of protection and order. This shift in the positions defended by different security professionals, based on different trades, has been shaped in Europe by factors that go beyond the borders of Europe and public policy. Private interests in the global development of digital technologies, US policies have played a key role, as well as internal conflicts within the EU's internal security professional groups.

Keywords: Digital Borders; eu-LISA; Surveillance; Preventive Security; Privacy; Criminal Justice; Freedom; Rule of law; Transnational Guilds; Foucault; Bourdieu

Introduction

This article begins by explaining the main concepts that allow us to speak of a security field as a theoretical tool for understanding what is at stake in Europe today, how this field has evolved and changed with the development of an insecurity continuum, and has extended to the so-called

* Professor; School of Law and Social Justice, University of Liverpool.

migration issues addressed by the Ministries of Interior and Justice. I used the notion of a "guild of digital technology" in security matters, which is existing beyond Europe and largely operated by private companies, to understand the logic at work in terms of communication and surveillance. I insist that digital technologies encourage a form of management based on suspicion, prediction and prevention for security and border controls and that it creates a bias against rule of law, privacy and data protection, seen as "silos", "slowness" and "inefficiency".

1. A "European" internal security field structuring the evolution of EU practices and institutions; an international sociology perspective

In the first section, I aim to synthesise the insights gleaned from the extensive research conducted by EU lawyers and Europeanists analysing internal security institutions. However, I will begin with the underpinning elements coming from a more sociological perspective. If one has to focus on the transformation of what can be called the domain of EU internal security, in which a process of juridification of police cooperation between EU Member States has slowly transformed informal networks or bilateral arrangements into multilateral agreements, many approaches are possible. The danger lies in looking at this large-scale phenomenon through a single disciplinary lens (law, history, political science or sociology of organisations) and through methodological nationalism. This is why a transdisciplinary perspective is required[1].

It is possible to pursue such a transdisciplinary perspective, because if differences of approaches and explanations occur, nevertheless convergences between disciplines exist as they all recognize that, in practice, a specific set of institutions and practices has been created, has a certain level of autonomy, and has resulted from the creation of a formal pillar organised around policing, criminal justice and freedom of movement, which was initially (and still is) called Justice and Home Affairs, although different

[1] For more details see T. Basaran *et al.*, *International Political Sociology: Transversal Lines*, London: Taylor and Francis, 2016; Didier Bigo, «Analysing Transnational Professionals of (In)security in Europe», in R. Adler-Nissen, ed., *Bourdieu in International Relations. Rethinking key concepts in IR*, Abingdon, Oxon / New York, NY: Routledge, 2013, 114-130; Didier Bigo, «Adjusting a Bourdieusian Approach to the Study of Transnational Fields. Transversal Practices and State (Trans)formations Related to Intelligence and Surveillance», in C. Schmidt-Wellenburg / S. Bernhard, *Charting Transnational Fields. Methodology for a Political Sociology of Knowledge*, Abingdon, Oxon / New York, NY: Routledge, 2020, 55-78.

variations of the name and boundaries have existed as explained and analysed by different authors[2].

This domain or "area" has expanded geographically and thematically with the development of an external dimension to internal affairs and the creation of many EU internal security agencies, Europol, Eurojust, CEPOL, Frontex and eu-LISA.

A substantial body of research on EU studies and EU legislation has detailed its origins, developments, peculiarities and problems. They have circumscribed its boundaries in terms of legal definitions and shown that issues of free movement, migration and asylum, privacy and data protection cannot be dealt with fairly if the focus is on security professionals from Justice and Interior ministries[3].

Historians and sociologists, inspired by the concept of "longue durée" articulated by Braudel and a socio-genetic approach based on the work of Pierre Bourdieu, have also emphasised the key role of both the permanent professionals of the institutions and juridification (the language of law) in the formation and maintenance of the European Union as such[4].

In general, they emphasise to a greater extent than the jurists that the internal security of Europe is constituted by a long history of policing networks with different styles and traditions, and by different views on the possibility of creating an area through a coalescence of national external borders that have been considered (or not) as internal borders of the EU Member States, which ultimately implies a difference between the EU borders and the Schengen borders.

Such a configuration is therefore the result of significant changes in the practices of the professionals concerned and the policies of their govern-

[2] See Malcolm Anderson / Monica Den Boer, *Policing across National Boundaries*. London: Pinter Publications, 1994; Didier Bigo, *Polices en réseaux: L'experience européenne*, Paris: Presses de la Fondation nationale des sciences politiques, 1996; James W. E. Shepticky, ed., *Issues in Transnational Policing*, London / New York: Routledge, 1998; Valsamis Mitsilegas / Jörg Monar / Wyn Rees, *The European Union and Internal Security: Guardian of the People?*, Basingstoke and New York: Palgrave Macmillan, 2003; Valsamis Mitsilegas, «The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data», *European Foreign Affairs Review* 8 (2003) 515-536.

[3] See Didier Bigo *et al.*, eds., *The Routledge Handbook of Critical European Studies*, Abingdon, Oxon / New York: Routledge, 2021, esp. the chapters by Kees Gronendijk, Elspeth Guild and Federica Infantino.

[4] See Antoine Vauchez, «The Power of a Weak Field: Law and Lawyers in the Government of the European Union (For a Renewed Research Agenda)», *International Political Sociology* 2/2 (2008) 128-44; Didier Georgakakis / Jay Rowell, *The Field of Eurocracy: Mapping EU Actors and Professionals*, Basingstoke and New York: Palgrave Macmillan, 2013.

ments, rather than the product of the institutionalisation of a European identity which has been accused of causing the problems.

These practices of policing, preventing, punishing, protecting, caring, which have been very diverse, remain highly differentiated, but they have nevertheless been polarised, almost monopolised by police professionals and interior ministries in the EU struggles around what can be called an "EU field of internal security professionals".

In this context, the assumption of "normality" that these issues of internal security in the EU are the domain of security, sovereignty and secrecy is misguided. Despite the persistence of this perspective and its increased prevalence over the past three decades, it is inadequate to explain the dynamics of this field and its turn towards the prevention of migratory "flows" that have become naturalised rather than politically debated.

Historically, the concept of security in a liberal sense of limits to freedom has derived its legitimacy from the democratic rights and effective practices of freedom of movement, from the political economy of regions, from their definitions of social welfare and their openness to other cultures. Security, therefore, cannot be reduced to a dependent variable based on police decisions about who has the right to cross borders, to stay, to work, to live with their families, by each national state, or even by their common agreement on a particular ideological stance. Security is not what the state apparatus wants it to be. It must serve as a means of exercising freedom and rights, rather than as a means of limiting them. The so-called balance between security and democracy is flawed[5].

Despite numerous reiterations that the goal of security is to protect liberal democracies and the rights of individuals and their free societies, the establishment of a professional field in this "area", or rather in this transnational social space, is constructed as a field of power and struggle because, in practice, many social actors involved in policing, border control, migration management and refugee reception have been interested in and strongly challenged by the idea of European internal security as a complement to freedom of movement. These actors have fought for the primacy of their own arguments and tools over those of others, in order to guarantee their funding and their missions. Conversely, many others, who were and are de facto key actors, have been marginalised in the institutionalisation of decisions at EU level.

The field of security is therefore a field of power in which different professionals engage transnationally in the best and worst practices that

[5] Didier Bigo *et al.*, *Europe's 21st Century Challenge: Delivering Liberty*, Burlington: VT, Ashgate, 2010.

other national traditions consider legitimate options for coercing individuals in a given state. Those actors who have been marginalised or excluded from the field, either because they contested the view of security as a state of police, prioritising social order, or because they did not consider that some of their interests were at stake, have subsequently realised that they were unable to voice their claims any longer due to the institutional monopoly of home affairs in the EU definition of freedom, security and justice. This was particularly the case when policing and criminal justice included the management of illegal migration and, through this channel, the situation of foreign-born citizens, of asylum seekers, including the social conditions of their integration, and the social policies of large sections of the population dealt with by the bureaucracies of the welfare states, as a security issue[6].

Conversely, the main actors in the field of internal security, the police, but also the military police, some internal intelligence services, border guards, immigration and asylum services, private security companies, which increasingly were operating remotely via electronic data, failed to recognise the growing importance of many actors coming from computer sciences and data engineering in shaping the present of European security landscape. A series of networks of so-called groups of mathematicians, algocrats, data analysts, systems engineers, experts in IT systems met and collaborated with police and border guard managers who were trying to rationalise a neoliberal productivity in police and justice organisations via what has been called an algorithmic governmentality[7].

These individuals began to work together, creating a group whose competences came mainly from a technical background and via a dual public-private trajectory. This group, which I call the "guild of digital technologies", emerges with a strong sense of being different from traditional security actors. They profess to possess a more scientific knowledge and a less coercive approach via "preventive solutions" that digital

[6] See David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society*, Chicago: University of Chicago Press, 2001; Loïc Wacquant, «How Penal Common Sense Reaches Europeans: Notes on the Transatlantic Diffusion of the Neoliberal Doxa», *European Societies* 1/3 (1999), 319-352; Loïc Wacquant, *Punishing the Poor: The Neoliberal Politics of Social Insecurity*, Durham / London: Duke University Press, 2009.

[7] Antoinette Rouvroy / Thomas Berns, «Gouvernementalité algorithmique et perspectives d'émancipation», *Réseaux* 177/1 (2013) 163-196; John Danaher, «The Threat of Algocracy: Reality, resistance and accommodation», *Philosophy & Technology* 29/3 (2016) 245-268; Claudia Aradau / Tobias Blanke, «Politics of Forecasting: Security and the Time/Space of Governmentality in the Age of Big Data», *European Journal of Social Theory* 20/3 (2017) 373-391.

technologies could create[8]. It is only this latter movement or transformation of the EU security field that I want to discuss in this paper, but it was crucial to first insist on the continuous transformations of the boundaries and meanings of what is EU internal security, for whom and by whom.

Methodologically, this means that the paper has to question the arrival of this new group of people specialised in digital activities at the heart of security issues and their rise in terms of influence and power. It seems that, despite some heterogeneity in terms of trajectories, they all share a specific craft concerning the use of "data politics" in positions of power within the European (internal) security field, and are linked through strong chains of interdependence with the digital space of the global North and with a renewed defence industry that considers borders as critical points and tries to justify its own existence under the same triptych of suspicion, security, surveillance, leading to the prediction and prevention of catastrophic futures. The embeddedness of internal and external security is operationalised in part through the digitalisation of the various security "problems". The terminology of the guild is used to express the belief of all these actors in a scientific knowledge and predictive capacity. It is at the root of their solidarity with traditional security actors.

As the paper proceeds, it will become clear that the argument and the terminology are based on a Bourdieusian international political sociology, which uses the terminology of field, habitus, trajectories, but introduces notions of transnational guilds, transversal and entangled fields of power, centripetal and/or centrifugal dynamics. For the sake of clarity, the notion of field is understood, as in Bourdieu's work, simultaneously as a magnetic field that attracts actors to what is at stake in the field (here, the control of practices accepted as security practices rather than illegitimate violence), and as a field of struggle in which competition between institutions, professions and guilds organised along specific craft lines takes place. Thirdly, as a field of power that expresses sufficient autonomy to have its own forms of domination, even if it is subordinated to external rules coming from other fields – and always has a certain heteronomy[9].

[8] Didier Bigo, «The Socio-Genesis of a Guild of "Digital Technologies" Justifying Transnational Interoperable Databases in the Name of Security and Border Purposes: A Reframing of the Field of Security Professionals?», *International Journal of Migration and Border Studies* 6/1-2 (2020) 74-92.

[9] Didier Bigo, «Sociology of transnational guilds», *International Political Sociology* 10/4 (2016) 398-416; Didier Bigo, «The Socio-Genesis of a Guild of "Digital Technologies" Justifying Transnational Interoperable Databases in the Name of Security and Border Purposes: A Reframing of the Field of Security Professionals?», 74-92.

Taking into account the international dimension within a Bourdieusian reflection then leads us to modify the idea that the nation-state is an entity that possesses a meta-capital that allows the stabilisation of different types of capital to be exchanged. It allows us to insist on a transnational dynamic that runs through all these contemporary security issues, traversing states and markets. This transversal approach differs from classical transnationalism and, far from taking us away from the local and national practices of actors to focus on another level, the notion of multiple fields and habitus enacted in the same act obliges us, on the contrary, to anchor actions in specific practices and to script them in order to find the chains of diagonal interdependencies that link these issues at different scales.

2. A guild of digital technologies reshaping the notion of EU security

In short, the main actors in these chains of interdependencies are the bureaucracies of each state, the various supranational institutions, the mobilisation of sections of civil activists, but also the transnational guilds that are structured by the specific skills required to perform a task and by the form of recognition of who is an expert in that field, sometimes outside the formal hierarchies at work in institutions. These guilds do not constitute a profession but have a common set of skills or crafts that are considered to be specialised and often transcend national borders, although sometimes they are local, provincial, while having a global impact[10].

In the case we are discussing, for example, this field of digital actors in EU security is not bounded by a legal definition of the EU, even if belonging to the EU is an important asset for the legitimation and symbolic power of the main actors. The field exists on a transnational scale, with key actors often coming from other parts of the global North, especially the Silicon Valley of the US, and with many globalised private companies playing a role "at a distance" but with very strong supporters within.

This is why we characterise the field by the fact that its dominant actors are mainly transnational guilds of competing trades (with common skills, techniques, styles) that have an interest in justifying that they are doing security, protecting people and preventing harm in a new way: scientific prediction and prevention.

[10] Didier Bigo, «Sociology of transnational guilds»; David Cole / Federico Fabbrini, «Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders», *International Journal of Constitutional Law* 14/1 (2016) 220–237.

As we will see, the process at work is therefore not the result of EU norms and institutions, even if they contribute to it, but the result of a larger dynamic of *dispositifs* of practices that modify these norms and institutions through their existing local nodes.

The personnel of eu-LISA and its client environment that we are going to analyse are therefore, and this is one of our main hypotheses, the node of this specific guild of digital technologies for internal security matters. This guild may be operating in the US, Australia, or the EU and is fragmented internationally, but their forms of knowledge, their tools are often transversal to each area, and some private companies or schools of formation are truly international, creating forms of mutual knowledge and international carriers. Security matters are a small branch of activities compared to others for all these specialists of data management, and they are not the most well paid, but they have specificities which give them a high value on the fabric of security commodities related to data systems[11]. So, they are both becoming key insiders in the field of EU internal security while being strongly connected outside of it, because they have the opportunity to be in phase with the development of the so-called digital revolution and its general AI problem-solving capacities, along with other colleagues working (business, trade, big tech connect) on what appears to be the same problems but different applications. This transversality gives them access to many top politicians and not exclusively the ministries of justice and interior. The latter are not their "bosses" asking them to produce technologies, they are constrained by larger logics where using data systems and management at distance is a sign of the bureaucracies to be inside the trend towards greater and better decision-making power in terms of risk analysis. And this trend is itself a form of dromopolitics[12] in which those who don't adjust are "disqualified" as legitimate players in the field(s).

I explained a while ago how the necessity to have data bases for the police establishment was not so much driven by their efficiency than by the necessity to have one, in order to exchange with the others, and to be part in European negotiations concerning EU internal security development[13]. Now more than ten years after the apparition of data analysts and computer systems engineers, as a transnational field of computerised exchange of information, this guild is in a position to challenge what is security, by

[11] Lucia Zedner, «Article review about Against Prediction: Profiling, Policing, and Punishment in an Actuarial Age, by Bernard E. Harcourt», *New Criminal Law Review* 11/2 (2008) 359-362.

[12] Paul Virilio, *Vitesse et politique: Essai de dromologie*, Paris: Editions Galilée, 1977.

[13] Didier Bigo, *Polices en réseaux: L'experience européenne*.

whom and for whom, maybe not because of their own strength inside the security matters, but because of their strong alliances with multiple powerful actors beyond EU and public matters, as well as a feeling that they belong to a group which has a clear view about movement, data in what has been called the program of a global liquid world nicely organised to be "safe, regular and orderly", putting preventive surveillance at the core of its logic, instead of stop and search, systematic physical check and argument of absolute sovereignty[14].

To defend this argument, the next part of this paper will describe the rise of these "pretenders" for preventive digital security, challenging both criminal justice traditions and evidence-based logics based on local knowledge of individuals and groups in favour of statistical knowledge and big numbers coupled with machine learning algorithms. If they have effectively challenged the inheritors of the traditional field of security, represented by the police establishment, and even influenced justice professionals, their ascendancy is nevertheless not assured, as their promises of prevention oblige them to push "results" in the future and not in the present, creating growing frustrations about their own cost/effectiveness. A shift in the balance of power is therefore imminent.

In the next part, we will consider the real consequences of such a shift within the *rapport de force* between the powerful actors in relation to the marginal actors and the victims of these changes, victims who may be different from the designated targets. In order to avoid repetition and to provide a more detailed analysis of a subject that has been extensively researched, the next section will focus on only one of the most significant developments in the field of internal security, namely the creation of large-scale databases and the establishment of an EU agency, the European Agency for the Operational Management of Large-Scale IT Systems or eu-LISA, in which data managers, who arrive with their own views of what constitutes efficiency and security as a smooth and flat circulation of information, meet, confront and comply with the various police organisations that traditionally manage Justice and Home Affairs.

[14] Marie-Laure Basilien-Gainche, *État de droit et états d'exception : une conception de l'État*, Paris: Presses universitaires de France, 2013; Didier Bigo, «Sécurité maximum et prévention? La matrice du futur antérieur et ses grilles», in *Derrière les grilles: sortons du tout-évaluation*, Paris: Fayard, 2013; Elspeth Guild, «The EU's so-called Mediterranean Refugee Crisis: A Governmentality of Unease in a Teacup», in D. Bigo *et al.*, eds., *The Routledge Handbook of Critical European Studies*, Abingdon, Oxon: Routledge, 2020, 307-319; Valsamis Mitsilegas, «Contested sovereignty in Preventive Border Controls: civil society, the "hostile environment" and the rule of law», in M. Bosworth / L. Zedner, *Privatising Border Control: Law at the Limits of the Sovereign State*, Oxford: Oxford University Press, 2022, 36-56.

3. eu-LISA: the locus of a digital technology guild managing preventive security and border controls

It is important to remember that the existence of a group of actors specialised on computer science and data engineering skills is not new. They have already been influential in this field, for example in the design of the Schengen Information System, which was considered necessary in the 1980s in order to develop a common area of free movement. Born out of a series of networks and groups, mostly private or coming from national communication companies, they are part of a series of networking groups (called horizontal) that have been formed along the development of the Schengen agreements and the management of the SIS, as well as the link between the Dublin agreement and the registration of asylum seekers in Eurodac. The successive enlargements have given them an important role in border control, but they have been marginal in the struggles to define security and justice.

The development of the Schengen infrastructure has organised a monopsony in which different companies have offered technical solutions with an incentive to be "European" by organising, with the help of different EU research programmes, joint ventures of different national companies. This was seen as a good move in terms of competing with the US in this "market segment", and central for economic reasons.

Politically, this emergence of non-traditional security actors can also be linked to the tendency in EU bureaucratic circles to avoid political struggles over security, freedom and justice by reducing security to a technical issue for professionals, and even by reducing sovereignty and security to the control of national borders. In this way, by introducing the idea that technology is the answer to security, the political professionals and the actors of the Council and the Commission of the European Union have both politicised security issues, ideologically, by gradually decoupling them from freedom, and depoliticised them, in order to avoid having to find non-consensual solutions themselves.

This has allowed the "problem" of border management to be delegated to "experts", to "professionals" in the various fields in question, with only one general instruction, which has been and still is to privilege all technical solutions in favour of "order" and "stability" over "fluidity" and change, especially when this change involves "costly adaptations" or "expropriation of authority by transfer to supranational institutions".

In a second phase, after 2004 and in response to the Madrid and London bombings, the idea of building a European homeland security changed the importance given to digital technologies, considering that they could

prevent terrorism through the construction of intelligent e-borders, with specific search engines analysing and anticipating the potential dangers or suspicious individuals travelling. The companies that applied were often involved in data management, but also in border security infrastructures. Their role was presented as a solution for modern policing and rapid border management, and they played a key role in the transformation from SIS1, which was an entry/exit tool, to SIS2, which in turn became a "search tool", almost from mid-2000 onwards. Europol and Frontex initially insisted that they wanted this modernisation before understanding the costs in terms of autonomy and recruitment. The focus on visa requirements, on imported conflicts through refugees, transformed trade and border technologies into security measures. This was the case with the use of Eurodac, the development of Passenger Name Records and the development of SIS II[15].

In addition to creating interoperable databases at the EU level (and beyond), their growth and influence as a group has been enhanced by their ability to offer alternatives in the internal battles over border control strategies. Against the idea of integrated border management, which was an attempt to reconcile police and border guards, they proposed an integrated data management with the use of interoperable databases to facilitate both counter-terrorism police searches and searches for illegal migrants.

This has been an important step showing their capacity to challenge the major players of the EU agencies of the internal security field, represented by Frontex and Europol. Even if they presented the project of Integrated Data Management (IDM) as a solution to complement Integrated Borders Management (IBM), in the different meetings with the Ministries of Justice and Interior of the EU, behind this formal consensus, it has been presented by the actors of eu-LISA themselves as a paradigm change, for a "soft" management of borders and smart solutions employing less people and costing less money by the systematic use of data bases to check travelers before they arrive at the borders with more efficiency than the current visa systems only, and by avoiding some biases led with discriminatory or even racist human border guards behaviours (Greece, Bulgaria, Hungary, Czeck Republic were evoked but other bigger Member States could not escape the implicit criticism of their own forces).

[15] Anneliese Baldaccini / Elspeth Guild / Helen Toner, eds., *Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy. Essays in European Law*, Oxford: Hart, 2007; Evelien Brouwer, *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*. Nijmegen: Wolf Legal Publishers, 2006; D. Broeders, «The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants», *International Sociology* 22/1 (2007) 71–92.

Far from a complementary approach, some actors saw that move as an internal critique of the ways the borders were managed operationally by Frontex and the national border guards. Stopping people at the borders and rendering these ones as electronic and physical walls more and more militarized, with people wounded or sent back to dangerous places, was, in the view of these high-tech managers, giving a bad image of the European Union in terms of high value standards on human rights – and this was in addition an argument "for" sales of new technologies, especially electronic privacy by design. The different actors of cyber security introduced the ideas of managing borders at distance via high tech solutions, avoiding the rise of militarization of border technologies, opposing the hard and soft dimensions.

A large part of the eu-LISA network of "friends" organized as a think tank mixing former eu-LISA members and big companies having a driving role on internet security succeeded to lobby efficiently the governments who did not want to look too repressive regarding arrival of migrants and flows of travelers visiting the country. For a while it looked like an alliance with some of the actors in favor of a delinking between crime and migration, including data protection agencies, but it will very quickly appears that this smooth management with smart data was not a chance for freedom of movement, but a form of less visible surveillance, based on the fact to avoid to stop people while using all possible technologies to identify (authentify) them via biometrics technologies allowing a communication at distance between the different locations of control, and "limiting the possible lies of the individuals about their origins and destinations". During another interview, a former member of eu-LISA said "we don't want violence at the borders, we want an iron fist in a velvet glove. Security can be smooth by regulating efficiently travels and people upstream, but it is still a channeling which needs to work better and harder. Nothing can block the movement and the data are there to achieve this point". This is this "vision" coming from the background of data experts that I want to dig out a little bit more. It is neither a cosmopolitan vision adept of global free movement, even if the language may think about it, and it is even less a vision open to effective privacy, but it not either a vision justifying violence at the borders and coercion, detention and send back of individuals in bad conditions. An original narrative emerges from the main arguments coming from the necessity of the fluidity of data and the control of population that is marked by the discussion around the notion of interoperability of data bases[16].

[16] Interoperability is not the same as the principle of availability (Willy Bruggeman *et al.*, «Principe de Disponibilité des Informations». Policy Recommendations, Paris: Centre d'études pour les conflits pour le Parlement européen, 2007).

4. Interoperability of data-bases and the building of data highways, a specific project for eu-LISA

In front of eu-LISA, Europol and Frontex, which already had uneasy relations and had both difficulties in positioning themselves vis-à-vis the national police and border guards, did not understand the effective role of their "technology providers". They continued to consider them only as "plumbers" useful, but not in command. Prisoners of their own internal struggles, they allowed this still lesser-known agency that the public and sometimes themselves did not really know, to become a powerful player[17].

Already in 2010, the objectives of eu-LISA professionals went far beyond border management through data management, and the network constituted around the agency was key to establishing the primacy of preventive policies, preventive justice, preventive surveillance through specific digital management tools.

The privacy groups and the European Data Protection Supervisor (EDPS) made successive reports on the rise of these technologies and their dangers, but they did not directly address the role of the agency in "designing and maintaining" them, so when the agency eu-LISA was officially created in 2011 and declared operational on 1 December 2012, most of the traditional security professionals and policy professionals in the EU Parliament or even the Council and the Commission were not really aware of what they were doing.

At the time, the agency's official mission was to manage the three databases that help the European Union meet its justice and home affairs needs: SIS, Eurodac and VIS. But after 2015 and the Paris attacks, the reluctance of the data protection and privacy group did not succeed in blocking the willingness of the French Interior Minister, Manuel Valls, to launch his own "war on terror" by pushing the agenda of counter-terrorism by other means, in particular electronic surveillance, and asking for the strong support of all other EU Member States. As a result of this impulse, and despite a weak capacity to show results, in 2018, i.e. with a sharp increase in funding, eu-LISA was given the task of developing three new large-scale IT systems with different databases – firstly, the European Entry and Exit System (EES), secondly, the European Travel Information and Authorisation System (ETIAS), thirdly, the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN), and even more recently, in 2023, the Agency took over the management of the cross-border justice tool

[17] The name eu-LISA is still obscure for most policemen and border guard and their understanding of the role is even more limited.

e-CODEX. The e-CODEX Regulation for the establishment of a computerised system of communication in cross-border civil and criminal proceedings serves as a reference standard for harmonising data collection.

However, the key project was not so much the development of the individual databases as such, but their interoperability, defined as "the ability of interconnected systems to share data and exchange information in order to provide relevant authorities with streamlined access to comprehensive information". A High-Level Group on Interoperability, made up of different nationalities but with almost the same backgrounds, i.e. police and border officials with backgrounds in data engineering or cybersecurity management, came up with a proposal for five "tools" to operationalise the idea.

The HLEG in 2017 therefore purported to fill the general definition with "tools" and proposed four of them, which were in a way "incremental" and put forward in a certain order, but the Commission proposed to get an additional tool on "fraud detection" to turn the system into a preventive system, responding to the will of the Council. The EU's JHA interoperability architecture consists of five components: For each of them, they suggested solutions but also signalled some problems to be solved. Their expectation in 2019 was to build it in three years, but in 2024 it is still under construction and proposed for 2026.

From 2017 to 2024, there were some changes in the details, but eu-LISA still considered that interoperability is based on four general principles to build the existing and future databases to enable interoperability between them[18].

To sum up, eu-LISA has therefore introduced various mechanisms for interoperability between the existing and future databases. Firstly, a single search interface to query several information systems simultaneously and produce combined results on a single screen. This first proposal seemed obvious (since users already had the right to access the various databases) and technically easy (since it could be built on the existing systems without major modifications). This step has now been operationalised through the creation of a National Uniform Interface (NUI), which is identical in all Member States as it is based on common technical specifications. As stated in the 2022 reports, "eu-LISA will not only develop this interface, but also coordinate the integration of the NUI by the Member States at their national level. In addition, eu-LISA will host the other external interface of the EES – the Web Service (WS) – which will provide services to third-country

[18] Didier Bigo, «The Socio-Genesis of a Guild of "Digital Technologies" Justifying Transnational Interoperable Databases in the Name of Security and Border Purposes: A Reframing of the Field of Security Professionals?», 74-92.

nationals wishing to verify their authorised length of stay. The WS will also act as a gateway for airlines to check whether or not third-country nationals holding a short stay visa, issued for one or two entries, have already used the number of entries allowed by the visa". The second recommendation was to achieve a real interconnectivity of information systems, where data registered in one system are automatically consulted by another; it was considered that the harmonisation of search and index functions may require a harmonisation of the systems, so that even if no information is circulated (or copied) between systems, the data structure will have a significant impact on all existing databases. The European Search Portal (ESP), a single search window for quick searches across all JHA systems managed by eu-LISA, is now operational and raises the question of differentiated access and the level of information provided by the quick search. The third "tool" was the establishment of a common biometric matching service to support different information systems for the cross-matching of biometric data across all JHA systems. It has allowed the various authorities to become autonomous from the individual's discourse on his or her own identity and to "trust each other", but to the detriment of an a priori presumption of innocence (which has turned into an a priori suspicion) with regard to each individual. The fourth tool was the creation of a common (or central) identity database (CIR) for the so-called correct identification of third-country nationals (biographical and biometric data), linking the different information in the database to reconstruct a profile aggregating data on a "data double", the person in the system. This CIR has already been the subject of much criticism in terms of effectiveness and privacy risks, but it is the fifth proposal that has been the most discussed, with a Multiple Identity Detector (MID) to detect multiple identities and combat identity fraud, as the errors of the administrations are turned in a way that it is the target (the victim) that is often considered at the origin of the "fraud", instead of recognising the poor quality of some aggregated data.

I will not repeat here the different critiques concerning the design of eu-LISA or the problems posed in terms of a reflexive approach to science and technology, as well as the risk these systems pose to privacy, discrimination and large-scale digital surveillance. These are important findings and they show that eu-LISA is not just a neutral technical agency[19]. It touches

[19] For a description and strong analysis of the data bases and their interoperability see Mariona Illamola Dausa, «eu-LISA, the New Model of Operational Management of the Various EU Databases», *Revista CIDOB d'afers Internacionals* 111 (2015) 105-126; Holger Pötzsch, «The Emergence of iBorder: Bordering Bodies, Networks and Machines», *Environment and Planning D: Society and Space* 33/1 (2015) 101-118, available at: <https://doi.org/10.1068/d14050p>; Paul Trauttmansdorff, «The Politics of Digital Borders», in C. Günay /

on the principles of the rule of law. However, some privacy groups and lawyers who have raised key questions about the privacy implications of interoperability are still assuming that interoperability tools are neutral and focusing on their impact on travellers and their different statuses and rights. This is a problem because these critiques are partly constrained by their disciplinary origins and a certain style based on litigation strategy before judges. If court rulings are important, they have not yet reached the issue of eu-LISA's activities, and this is partly because the critics do not understand the international dimensions of the political power struggles at stake in what is seen as a technical issue. Data is about politics[20].

Admittedly, regarding the ambition of these tasks, eu-LISA's staff appears to be very small compared to other EU security agencies, with only 137 people in 2019, additionally spread over three sites: the headquarters in Tallinn (Estonia), the operational site in Strasbourg (France) and the backup site in Sankt Johann in Panga (Austria). However, eu-LISA's strong association with private companies (its tenderers) has significantly increased the number of people involved in the Agency's network and demonstrates the specific public-private nature of the technologies involved.

This coordinating role, resulting from the so-called technical harmonisation of data collection between the various EU internal security agencies, is reinforced by the fact that eu-LISA has been given the chairmanship of the Justice and Home Affairs Agencies Network (JHAAN), which officially has the task of "connecting the EU agencies implementing EU policies in the area of freedom, security and justice". "Together, the JHA agencies

N. Witjes, eds., *Border Politics*, Springer, 2017, 107-126; Paul Trauttmansdorff / Ulrike Felt, «Between Infrastructural Experimentation and Collective Imagination: the Digital Transformation of the EU Border Regime», *Science, Technology & Human Values* 48/3 (2023) 635-662; Niovi Vavoula, *Immigration and Privacy in European Union law: the Case of Information Systems*, Leiden / Boston: Brill / Nijhoff, 2022; Georgios Glouftsios, *Engineering Digitised Borders: Designing and Managing the Visa Information System*, Singapore: Springer Nature, 2021; Matthias Leese, «Exploring the security/facilitation nexus: Foucault at the 'smart' border», *Global Society* 30/3 (2016) 412-429; R. Bellanova / H. Carrapico / D. Duez, «Digital Sovereignty and European Security Integration: an Introduction», *European Security* 31/3 (2022) 337-355. The critiques of these different data bases and the role of eu-LISA in terms of designing the different data bases first separately and then with the possibility to do interconnections and to enlarge the possibility of access to other data bases than initially accepted has been discussed by all these authors, and especially by Niovi Vavoula in multiple articles which are crucial to understand the structural problems this organization of interoperability create for privacy and more generally human rights. I agree with most of them, but I want to emphasize a different point concerning the change on the preventive security by the specificity of this digital vision of security and the alliance with some specialists of counter terrorism.

[20] Didier Bigo / Engin Isin / Evelyn Ruppert, *Data Politics: Worlds, Subjects, Rights*, London: Routledge, 2019.

contribute to the implementation of the EU's objectives in the fields of migration, asylum and external border management, the fight against organised crime, drug trafficking and terrorism, gender equality and respect for fundamental rights". It should be noted that the last two topics have been added very recently, perhaps after the series of scandals that hit the former director of Frontex, Leggeri, when he reported on the practices of the Greek border guards of refoulement and mistreatment of refugees arriving by boat in the Greek islands, and was forced to resign following the reports of OLAF, which acted as a watchdog, and the report of the European Parliament.

It seems that eu-LISA is no longer, if it ever was, a service provider for Frontex, but the agency in charge of the general strategy of integrating data management for border purposes; Frontex keeps the operational task and the intelligence on the ground but loses the leadership of the "border apparatus".

Organised around the idea of being a hub within the networks of EU agencies, eu-LISA has also organised its own management board, composed of representatives of the EU Member States and the European Commission, as well as the associated countries (Switzerland, Iceland, Norway and Liechtenstein) and the other agencies Eurojust, Europol, Frontex and EPPO (European Public Prosecutor).

It is not surprising that after the long ten-year "reign" of Krum Garkov, who was closely linked to the police and some private security companies, the agency's leadership has also taken a different direction, with the choice of women trained more in risk management and software for cybersecurity. The curriculum vitae of Agnes Diallo, who was briefly director of eu-LISA, shows that "she has led the development and management of numerous European reference IT systems, fully compliant with GDPR and cybersecurity requirements", developing the idea of risk compliance and, as she said in her letter of resignation to return to the IN Group, but as French CEO, "harnessing the power of transversality and togetherness" within eu-LISA[21]. According to eu-LISA's website,

> "the Agency will continue to develop the theme of digitalisation, which has been one of the key priorities of the previous EU presidencies. Taking into account the rapid digital development in the

[21] As French director of IN group she presents her new mission as to build the state-of-the-art identity solutions and secure digital services integrating electronic, optical and biometric technologies to the French government, putting biometrics recognition technologies at the core her vision of fluidity.

> JHA area and the Agency's role as a developer and integrator of pan-European systems, eu-LISA intends to organise a series of events on the use of new technologies and common challenges related to digitalisation in order to promote exchange and cooperation between JHA agencies. In particular, activities will focus on the potential use of cloud services and artificial intelligence (AI) in the JHA field, as well as on biometrics and standardisation. For example, the potential and challenges of using AI in the field of human resources will be explored as an issue relevant to all agencies. eu-LISA will also highlight the opportunities and changes that the Commission's proposal on the digitisation of travel documents and travel facilitation will bring to EU citizens. Finally, this priority will also address the innovation dimension of digitalisation. Together with the EU Innovation Hub for Internal Security, we will explore the possibilities of familiarising the network with the latest relevant results of the Hub's projects, as well as the creation of a common platform for a central knowledge repository and exchange".

She was replaced on 16/07/2024 by Marili Mannik as interim director. But it seems that the idea of being a "platform" is now well embedded in eu-LISA. Marili Mannik, from Estonia, was the former head of eu-LISA's board in July, and had previously worked as a director at PwC, to "bring her experience in public sector management consulting and digital transformation, as well as in the firm's internal management activities" to the development of eu-LISA, which now includes more AI algorithmic procedures and remote biometric recognition for surveillance purposes, renamed "proof identities" to justify this acceleration towards prediction and anticipation logics in addition to identity verification.

All these new systems, which eu-LISA will have to set up, are based on the idea of connecting the dots by ensuring the validity of heterogeneous data, creating large data pools with differentiated access and filtering them according to objectives, in order to detect suspicious behaviour, to monitor certain clusters of individuals and to develop predictive tools that allow for "preventive security". They are looking for a total awareness and a maximum extension on a global scale, even if they know that it could be only a step by step process.

The main tool (or concept) to achieve this great goal is the creation of an interoperable system that links the various existing databases with the new projects within Europe and, in the near future, with the various interoperable platforms of the same type that exist in the USA, Canada, Australia, New Zealand and, why not, South Africa. This notion of interoperability is therefore the keyword for bringing together technical, economic and political elements.

The digitisation of data is not just about fast knowledge and ease, it is a specific episteme that destroys fundamental principles: innocence, purpose limitation, privacy, in the name of the fight against "silos", lack of connections, the need for interoperability, instant communication between internal security agencies to timely and preventive policing through surveillance and predictive technologies.

5. The metaphors of "silos" and the alliance between the doxa of data security managers and counter-terrorism logics

Talking in terms of "silos", i.e. an organisation that isolates data for its own purpose, is seen by data managers as the worst possible outcome. Their career path pushes them to accept differentiated access, but as long as they don't compromise the constitution of large pools of data that need to be available to them to be cross-checked and verified (trusted). They can be anonymised, but the large number is essential as a priority to run algorithms with self-correcting mechanisms (so-called learning machine), because they can go beyond average statistics by discovering some specific clusters of behaviour located at the edges of the data pool (that often geometric visualisation helps to detect).

The accumulation of data, the retention of data for as long as possible, the refinement of algorithms explain that the mean of interoperability is so important that it becomes an end in itself. Anything that works against interoperability is a problem to be solved, to be eradicated. They call these "problems" of limiting the growth and retention of data by the terminology of "thinking and organising in silos". It is identified as the major problem of data management in most books on management theories applied to data. It should be noted that they call many things "working in silos", be it some process to collect information without enough ambition or speed, some operational technologies and degree of specialisation, some organisations that refuse to share data, some legal elements blocking fluidity in particular purpose limitation, and the use of gateway for access to large pool of data that they compare to toll in highways.

Here is one of the key problems in terms of professional habitus. What they call silos and inconvenience in their data world is called "purpose limitation" in the language of law and privacy, so a large set of rights and basis for freedom of movement are seen by data managers as "silos" to be eliminated!

This engineer mentality and training on data with a view to progress in knowledge is organised along this way, and it is very rare to have reflexivity

on this "prenotion" or "common sense" that big data is better than small packs of isolated data. The question provokes laughter.

They respond with the term "old silo thinking", which for them is the exact opposite of a smooth communication that authenticates data, reduces errors and creates trust between partners. They associate "specific" access and "specialised" work as a mistake or as a strategy of secrecy linked to a lack of competence. They want a "flat" world of security management, where everything can be mobilised in time to solve any problem…

They are not alone in thinking this way. In the world of security, it was the people from their ranks and the counter-terrorism analysts (especially from DARPA and NSA) who strongly influenced the report of the US 9/11/2001 Congressional Commission.

If we want to understand the current doxa in favour of interoperability, data management at the borders, artificial intelligence for preventive policing (and justice), we need to go back to the root of the problem of the paradoxical alliance between data managers and anti-terrorist policing, secrecy and control in relation to EU policing and border management, which favours the free movement of people and sees security as the limit of freedom in an enlarged zone.

This report of the 2001 Congressional Commission was key in identifying, by analogy, the use of this metaphor of silos to speak of purpose limitations in setting up the databases, strongly criticising the lack of exchange between the different US services of police, local, national, federal and the rivalries of the different intelligence services, which, in their view, were reluctant to share all their information and therefore responsible for what went wrong on 11 September.

All the measures put in place by the Church Commission to avoid the "dangerous mix" of data, missions and functions that led to the major scandals of the mid-1970s became, on the contrary, the causes of the 11 September attacks. This semantic change allows the services to benefit from more data, less control over their purpose and a strong hierarchisation between those who are obliged to hand over all their own data without having the chance to look at those of their partners and those who have the possibility to have access to almost all the data they want. The US Department of Homeland Security has been built with this major objective in mind, "interweaving" the web of data coming from the intelligence services, the police and the border guards, while maintaining specific organisations to avoid the "Latin American" model of a unified security force.

To reinforce the argument of interoperability as a fight against "silos", it has also been said, with much authority but little evidence, that this way of managing data will make it possible to prevent terror and crime by

anticipating the actions of enemies or the behaviour of petty criminals through the predictive techniques coming from the mass of data and the algorithmic capacities of what is now called artificial intelligence, but at the time was called total information awareness.

We know that the European Union has for a long time been divided between some services and countries that wanted to organise a strong "European" internal security with some federal powers, and those that strongly resisted this idea in the name of national sovereignty that would be endangered by the sharing of data. The story of eu-LISA's progress and limitations in terms of tasks and powers is the result of these major political battles. They are the underlying elements that explain most of the description of the developments described above. The false opposition between those who create AI and those who regulate it (reduced to the US versus the EU) is much more a mask that obscures the strong chains of interdependence in favour of the AI technological revolution in all sectors, including security, by major entrepreneurs and by civil servants, lawyers and judges on both sides of the Atlantic who want to maintain the primacy of law and criminal justice over technologies, even in a preventive context.

The second element limiting the argument for data interoperability in the global North (US, Canada, Australia, New Zealand… and Europe) was that, in the mid-2000s, privacy and data protection regulators in Europe were better organised than in the US and they managed to put forward the idea of a necessary regulation for privacy if the project of data interoperability was accepted. They insisted on "function and mission creep", preserving the idea of purpose limitation as a key element for a democratic state. Around 2005, many debates forced the construction of EU databases for internal security purposes to be organised around the idea of surveillance authorities and the preservation of human rights and freedom of circulation through "purpose limitations" for each service, meaning limited access to the pool of data. However, in order to achieve this purpose, they often accepted the general principle of operability, while demanding limits where privacy was concerned; a line of thinking that they often continue today.

For a while there was a kind of equilibrium, and in a way the birth of eu-LISA was the product of that period. But the will to go as far as possible in the interoperable management of data was reintroduced in Europe after the bombing in France in 2015, and the multiplication of access to different databases for the purpose of terrorism and crime (even if not serious) became accepted. In the case of the EU, with the moral panic about migration and disinhibited right-wing racist and differentialist discourses, the interoperability tools were even pushed beyond the criminal justice and criminal police to the point of linking all data, considering asylum seekers and third

country nationals as criminals, and the idea of controlling both entry and exit of all travellers in Europe was put forward as a goal for these EU internal security databases (in contrast to the US, which de facto abandoned exit control).

The radical right in various EU countries has succeeded in presenting this extension of border controls to every traveller as a necessity, and this has been welcomed by many police authorities who have some access to these data borders. Interestingly, some of these right-wing parties (in power or in opposition) have silenced their pretence of national sovereignty in order to put forward police cooperation, while others reject any intensification of police cooperation, and even more so of intelligence services and border guards, which are seen as the ramparts of the territory.

6. Conclusion

The common interest between the police authorities, who claim to be united against crime (and migration), the border guards, who want data analysts to join them, and the radical right is still to be analysed, as it is a very complex, mixed and fragile platform, but they share what is at the heart of this transformation of EU internal security, its reformulation along the categories of suspicion and surveillance through data politics and preventive logics, and the abandonment of the economic liberal paradigm of the free movement of capital and people.

In short, the push for interoperability and rapid time management, mobilising all data to prevent future events, has been a political attack on legality through a technological argument.

It has had many consequences and created many forms of (un)voluntary victims of this logic. I have called this political economy of surveillance a ban-opticon rather than a pan-opticon because this (un)voluntary process of victimisation is a ban-opticon in which travellers, even if they are not targeted, become victims of a process of a priori suspicion and entering under surveillance is not seen as coercive surveillance. So we end up with a paradoxical situation in which people under suspicion see this as beneficial to their future security.

These elements are subject to what might be called an epistemic transmutation, in which the ideas of individual freedom and popular democracy are countered by policies of fear, suspicion and prevention aimed at shaping the primacy of societal security and the preservation of the existing order in the face of any transformation that the elites deem alarming. The old “qualities” ascribed to concepts such as prevention,

protection and freedom are then replaced by other meanings that undermine and subvert them. Predictive, preventive security is not linked to the welfare state as a means of limiting disorder and pacifying social conflicts, but on the contrary to an intensification of suspicion and anticipation of behaviour that seeks to prevent crime and anticipate action on the basis of risk profiles and statistical categories that are themselves constructed around selected persons of interest, but not the totality of the population.

In conclusion, this orientation towards intelligence-led policing, anticipation of future criminal activity, pre-emptive and pro-active work by border guards, police, intelligence services via the work of the node that represents eu-LISA is therefore the development of this ban-opticon that targets visible minorities in order to reassure anxious majorities that they are not the target of surveillance, even if they are. It helps a certain vision of the radical right to emerge as a common sense of security, and yet it is the product of forces that criticise it, like most of the guild of data managers and security professionals. This convergence remains to be discussed.