26

Interoperability: A political technology for the datafication of the field of EU internal security?

Didier Bigo

This paper is concerned with the changes occurring into what has been called the field of European Union (EU) internal security (Anderson,den Boer 1994; Bigo 1996; Sheptycki 1998). The notion of field is used to avoid that a vision of the multiple different practices of the actors who gather and compete to define security and insecurity, being reduced to a discussion on the progress or not of the institutions of the EU and an analysis of the success or failure of a spill over in matters of sovereignty. The existence of an EU internal security domain called Justice and Home affairs is not an autonomous domain that security studies can isolate as an object as such (Kees Gronendijk in this volume). The question of EU internal security is derivative from the practices of freedom of movement in the EU, of who is entitled to cross borders, to stay, to work to live with his family. This area, or better this social space is constructed as a field because many social actors who do policing, border controls, migration management, reception of refugees have been interested and pushed into strong disputes around the idea of an European internal security and have fought to privilege their reasoning and tools over the others, in order also to guarantee their funds and missions. The socio-genesis of the field of EU internal security is correlated with the transformations of practices of freedom for people to move and the ways this management of their travel has been correlated with the traditional tasks of coercion in case of crime and violence that police do, as well as the way they treat their citizen and the foreigners in these cases. The field is therefore a field of power, where different professionals engage transnationally on the best and worst practices that the other national traditions consider as legitimate options for coercing individuals in a specific state. Far from opposing homogeneous cultural entities of nations represented by their governments and their representative (commissioners, and permanent representation), a study of the last forty years shows that the alliance and the fights follow often about the way actors do their job, the similarity or not of their routines, their habitus and trajectories (Adler-Nissen 2012; Kauppi and Madsen 2013). To be a policeman, a gendarme, a border guard, whatever the country, is more important than the nationality, and frames how people act, beyond the diplomatic negotiation done in Brussels. This is what I have called transnational guilds (Bigo 2016). They are structured by the specific skills necessary to do a job, and the form of recognition about who is an expert on this domain, sometimes not in accordance with the formal hierarchies at work into institutions. As it has been explained many times such a research imposes combining different disciplines, which have all their own

narratives about the history of EU internal security (Bossong and Rhinard 2016). Many books have described what they call the emergence of the third pillar of the EU and the development of an area of freedom, security, and justice, where the key word is security and policing. These authors provide a detailed understanding of the juridification of sectors of national policing under the construction of the institutions of the EU and the tensions it has created. They are Europeanists political scientists and sometimes lawyers. They begin their books with the Maastricht Treaty and they look at the legal effects of the Europeanisation of policing in terms of criminal justice and border controls. This first line of thought is important by its detailed knowledge on policy making and its description of the personnel of the EU institutions as well as the impact of the norms of policing (Den Boer and Walker 1993, 2011, 2013; Mitsilegas, Monar and Rees 2003; Monar 2002, 2013; Wallace Hélène &Wallace William 2000) but this Europeanist narrative does not give the same picture than the one produced by the sociologist of policing and the criminologists. The latter insist more on the dynamics of the national polices, their models of policing, the dynamics that have constituted national polices from the eighteenth century and the Europeanisation from the nineteenth century giving to the field of policing a different historical scale (Anderson Malcolm, den Boer Monica 1994; Deflem, 2000; Liang, 1992). They insist on the longue durée of informal clubs of policemen, on the transatlantic links which have framed the field and which continue to be central nowadays to understand how policing in its management of violence (counter subversion, counter terrorism) is more and more connected with border controls and surveillance (Bigo 2014; Carrera and Mitsilegas 2017; Collantes and Celaldor 2012; Guild and Carrera 2013). The third approach which is necessary to have in mind to understand EU internal security is the social use of technologies by different actors, the correlations between technologies, surveillance, tracing of mobilities, identification of people, anticipation of behaviours. Based on sociology of technology, digital and surveillance studies as well as critical legal studies, this third line of thought connects researches on surveillance and human rights affected by transnational dynamics of control of mobility (and not only at borders). It includes a reflection on the objects by which security is produced and by an interest on the targets or unexpected victims, these competitions between actors produce (Brouwer 2008; Guild 2006; Mitsilegas 2008). The last image is more complex and diffracted than the other ones. Its advantage is sometimes to ask new questions about what seems pure technicalities: the passports, the visas, the databases, and the people who construct them and 'support' the non-specialists on technologies. This is also a way to understand some key transformations at stake in the general economy of the field of internal security today in its relation with the EU institutions and in the incremental use of digital technologies to regulate the circulation of people and the reframing of what is security in terms of preventive policing.

We engage into the hypothesis that the professionals of security which were in charge for centuries (policemen; gendarmes, border guards, judges and the agencies of the EU into which they have congregated, Europol, Frontex, Eurojust) have now to take into account the emergence of a new guild with a different background of engineers, data analysts, experts on IT systems, that we can call a guild of 'digital technologies' which has emerged through the tendency of all the actors of the field of reducing security problems to a governmentality of unease which has thus to be solved by technical experts. This is illustrated by the creation of a specific EU agency, not very well-known to the public, but very central in terms of power politics, called EU-LISA an acronym for the full long title: European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

This article will question the EU-LISA mode of existence and its regime of justification as well as its relations with the politicians and the populations who are the objects of its attention. If, already numerous articles have been published recently and have given a better knowledge on

this agency, its design, its population, its purposes, and its relation to surveillance and fundamental rights, it is still rare that the interoperability between data bases allowing to compute data in different data bases by a single search, has been questioned on the validity of the reasons invoked to use more and more technologies at the borders, and on the engineer doxa of progress. Often privacy groups and lawyers who asked central questions on the consequences of interoperability still accepts as a departure point that instruments of interoperability are neutral and focus on their consequences. The formulations of the questions concern what these technologies bring really in terms of speed and efficiency, or in terms of predictive and preventive capacities, and are the advantages proportionate with the inconveniences that they create if they breach privacy of individuals and groups or generate structural discrimination and surveillance? (Glouftsios 2018; Illamosa Dausa 2015; Trauttmansdorff 2017).

We want here to supplement these questions by a more sociological, political, and international approach pointing on what kind of problems are posed by this framing of an international competition regarding high tech and digital circulation of information on 'internal security', and what is its historical construction and justification through the creation of institutions validating the common belief that relying on technologies to solve security problems is a 'matter of fact'. We want also to discuss the implications to put more and more, at the heart of the decisions on questions of collective security, the participation of non-traditional security specialists (data analysts, systems engineers, and even mathematicians experts on algorithms) even when themselves want to be 'modest' or minimally to be seen as such. This story implies to enter into the description of many instruments and data bases which look 'uninteresting', detached from the real and their political effects, even more than the visa stickers in passports that we have analysed years ago (Guild and Bigo 2005; Infantino in this volume). But it is important to repoliticise this apparent technicity and neutrality, as these instruments produce violence and segregation. They generate by their practices forms of ban-opticon at the same moment than they facilitate life for many other people (Bigo 2006). As a conclusion we will suggest that the field of security in Europe is modified by the formation of what we have called previously a transnational guild of 'digital technologies' whose existence began with the Schengen Information System in the mid-eighties, has developed in relation with border controls management, has been consecrated with the institutionalisation of EU-LISA and is now implementing a transition from integrated border management to integrated data management (IDM) which has many different implications (Basaran, Bigo, Guittet and Walker 2016)

EU-LISA: A purely technical agency or an important node in a network of power?

EU-LISA presents itself as a role of support for the implementation of the EU's Justice and Home affairs policies by managing large scale IT systems. Established in 2011 and operational only the first December 2012 the staff looks restraint with only 137 persons in 2019 which are in addition split in three sites, the headquarters in Tallin (Estonia), the operational site in Strasbourg, France, and a back-up site in Sankt Johann in Pongau, Austria. Nevertheless, the strong association of EU-LISA with private firms (their tenderers) boost strongly the number of people involved in the network of the agency and shows the specific public–private characteristic of the technologies at stake.

The agency has officially the task of managing the three databases which have been central in the EU to address the questions of Justice and Home Affairs: the Schengen Information System (SIS), Eurodac, and the Visa Information System (VIS) (see Guild, Infantino, and Jeandesboz in this volume).

The Schengen agreements implementation has introduced the idea of a SIS from 1988 and the design has been implemented with a central system in Strasbourg and national systems in each countries, avoiding a central data base containing all the data in a specific location. Political fear of centralisation via digitalisation have played in favour of such a solution. This system called retrospectively SIS1 has been replaced by another platform after the enlargement of the countries of Central and Eastern Europe under the name of SIS 1 for all which has continued the same logic but with speedy connections, and after a lot of fights by a platform called SIS2 which has changed the logic at work by including elaborated search functions and strategies of identification of suspects going beyond the control of documents at the borders (Niovi Vavoula 2017; Bigo 2020.

The Dublin agreements and the anxiety of some government that asylum seekers will ask in multiple places their asylum claims has generated also another database: the European Dactiloscopy renamed the European automated fingerprint identification system (AFIS) and more well known as EURODAC. Initially reserved to national authorities in charge of Asylum verifying that the asylum claim has been dealt effectively on one Member state only (to avoid asylum shopping) and that this state, often the first country of arrival, is responsible to send back the persons who have not left voluntarily the EU, has been also transformed when the law enforcement agencies and some of administrative agencies like the prefectures have been authorised to have specific access into the Eurodac database for their own purposes. It has been considered by many as a function creep transforming the nature of the data base purpose (Tsianos and Kuster 2016).

The development of the legislation on visa at the EU level has also added a third database called the VIS which contains all the information which third country nationals subject to a mandatory visa requirement must produce to obtain a visa. The number of people registered in this data base, which includes also the persons of the EU receiving at home the person asking the visa, has been criticized for its disproportionate collection of data and the link it has implemented with a counter-terrorist approach (Balzacq and Leonard 2013).

One can see therefore that politics is dense into the technicality of these data bases, and that technical choices are not only a question of support, their design frame possibilities and discard others (Glouftsios 2018). None of the data bases, initially conceived in relation to freedom of movement and compensatory measures has escaped from its use for preventive measures and search against terrorism and crime. Some critiques consider that these data, under anonymised formats are also used for profiling and risk analysis, generating suspicion by association and sometimes guiltiness by association. It was already the case in the mid-2000 after the reform of SIS2 and the access given to law enforcement to these three data-bases, but it has become even more obvious after 2015, when political declarations insisted to officialise these practices of data mining and insisted for new developments (see Manuel Valls).

Effectively, EU-LISA has also be put in charge more recently to develop new projects of large scale IT systems with different data bases: first, the EU Entry Exit System (EES),[1] second, the European Travel Information and Authorisation System (ETIAS),[2] and third, the European Criminal Records Information System for third-country nationals (ECRIS-TCN).[3]

So, in total there are therefore six EU-information systems which are concerned, and which relates to JHA-security only in part, while JHA want access to almost all of the data bases (see annex).

Nevertheless, here also, most comments done on interoperability takes for granted the presentation that these six systems are coherently necessary for JHA and therefore 'belong' to policing and border guards first and of course to EU-LISA, which is a way to deny the validity of the previous separation, or more exactly the compartmentalisation, distinguishing for good reasons, crime-terrorism and judicial request on one side, and border crossings, visas, travels on the other

side, as the EU has done for more than 20 years (from the Amsterdam Treaty and as a customary practice after Lisbon).

Against this idea of joining the dots between every types of data which, in a not too far future, may include in terms of scale exchange with the United States and Australia, as well as in terms of scope inclusion of data coming from both defense in the name of counter terrorism, and social welfare in the name of fight against radicalisation, the most striking feature of these current information and personal data systems is how heterogeneous they are. Not only do they contain very different types of data and have been established for different purposes, but the ways in which they operate and can be consulted are also entirely different. For example, Eurodac does not hold the names of people whose fingerprint data are held in the system. If a check reveals a fingerprint match, the checking authority must go to the authorities of the Member State that entered the fingerprints to find out the identity of the individual, and this is crucial for asylum seekers in order their names not to be passed through enlarge police cooperation. It is also prohibited that any data on EU citizens is included in this database. The ECRIS database, on the other hand is driven by the nationality of the convicted person and details of the conviction. Each database has thus a different trajectory in EU law and policy, and a different objective. (Guild 2019)

As long as they were not interoperable, and were allocated to different tasks and had different access for authorities designated expressly for their main activities, the problems existed about function creep, but they were limited. Now the implementation of the project of interoperability has changed deeply the global architecture and what a single search can bring as results. Even if the principle is still not the 'nice to know' for police and intelligence and is still driven by the 'need to know', obliging justification in order to have access, the possibility to have it on screen quickly, allow the different authorities to try to use these tools to the maximum of their possibilities, to relax their own self-discipline especially when what they want to find is just at a click of mouse but with a forbidden access. The tools of interoperability between the six data bases if they are finally implemented, will bring finally a huge amount of data and will unbundle the legal purpose limitations set up by the previous legislations in the name of avoiding silos in computation logic. The form of mentality and knowledge of security is therefore changed by this inclusion of data analysts approach.

Overcoming an organisation in silos: The argument in favour of interoperability

This critique of the value of purpose limitation did not come quickly and lightly as a revelation after the bombing of 2015. It has been the work of many years to criticise purpose limitation as a barrier to the effective work of research of potential suspects. Speaking in terms of 'silos' isolating data and then allowing people who were known by different bureaucracies but only partly, to have the chance to escape to the vigilance of the police preventive strategies, has been a political attack against legality via a technological argument. The first use of this metaphor of silos to speak of purpose limitation has been used by the intelligence services to complain about what went wrong with September 11, and the US 9/11/2001 Commission of Congress, has criticized them while buying the argument that they needed to have access to more data bases in order to 'prevent' future attacks (The US Commission Report of 9/11/2001, 2011). In their recommendations, they were the first to insist on relaxing the separation into different channels instituted by the Church Committee after the scandal of the CIA and FBI joining their efforts in manipulating the black civil right movement (Loch.K.Johnson 1986). It was like a reversal of jurisprudence. In 1975, the recommendations of the Church Committee have been to insist

on the contrary on purpose limitation as a key principle to avoid that agencies collaborate to bypass the limitations imposed by their mandates. Journalists have reported the juridical principle using the metaphor of stovepiping (an isolated vertical conduit) to justify these limits. This metaphor is rarely used nowadays or negatively only, like silo, despite its importance to show that security needs to have limits in its development if the services implementing it, does not want to become the sources of other forms of insecurity and violence against their own people. Interoperability has become synonymous of extended connectivity, more and better knowledge, against fragmented, isolated conduit, seen as cause of inefficiency. This use of metaphor was central to reverse public opinion in favour of helping the agencies to work together, despite dangers of infringement of their mandates. The most spectacular change was the initiative of admiral Pointdexter about the 'collect it all' logic that he tried to impose under the Total Information Awareness (TIA) system, that even the majority of the republican Congress considered as going too far (Whitaker 2006). TIA was changed from total to terrorist information awareness, but is obvious that most technicians continue to think in terms of total interoperability as the dream of instantaneous information. The EU plays a lot on its better value and norms than the United States of Georges Bush, nevertheless if, after 11 March 2004 in Madrid and 7 July 2005 in London, and despite the claims to have more integrated databases, the purpose limitations stayed in place, it was not the case later and the controversial propositions for interoperability were justified as a counter-terrorist instrument succeeded after the bombings of January and 13 November 2015 in Paris, March 2016 in Brussels and the long series of small scale attacks related to Daech actions in Europe until 2018. François Hollande and Manuel Valls were the first to be vocal in this domain and they succeeded to inspire other EU member states to push with them this question of the positivity of interoperability as the solution to 'join the dots' into the implementation in 2016 of the European Agenda on Security of April 2015 (Schiopu and Bobin 2015) (Bigo 2020 in Idil Attack).

The Commissioner for Security Union, Julian King who was in theory the last UK commissioner, has placed also a particular emphasis on 'overcoming the fragmentation that this organisation of data bases with purpose limitations' was in his view creating through the "interoperability" of existing and future EU databases. Following the commission report of the European agenda on security, he led the Task Force on Security Union and published in July 2017 a review of EU internal security. It described the EU architecture as: '(a) sub-optimal functionalities of existing information systems, (b) gaps in the EU's architecture of data management, (c) a complex landscape of differently governed information systems, and (d) a fragmented architecture of data management for border control and security'. Such a convergence of politicians from different countries pushes not only the Council, but the Commission to take this view, in order to show that the EU was not lenient on terrorism, but nevertheless, before hands, to appear more neutral, the EU Commission had commissioned a report to a so-called High-Level Expert Group on Information Systems whose details were limited in terms of professional status, as they were described only as providers and stake holders. The HLEG on IS was set up in 2016 and delivered in May 2017, a report doing a comprehensive assessment proposing with no surprise at all, a series of arguments on the need to develop interoperability between the different data bases and linking the success of that interoperability with the three future projects of EU-LISA still in discussion, writing into their report as if these projects were already accepted and functional (Carrera et al. 2017).

The result was in legislative terms that the 12 of December 2017, the Commission tabled two proposals for regulation establishing a framework for interoperability between EU information systems, one dealing with those covering police and judicial cooperation, migration, and asylum, and another on Schengen-related databases on visas and borders. They were almost completely

identical but it was a way to respect in appearance the difference of purposes in the eyes of the EU parliament and the European Data Protection Supervisor (EDPS), the Fundamental Rights Agency (FRA) who were disagreeing. Nevertheless the choice was not between technical options to choose, but to endorse a policy of IDM justifying the program of a full generation of instruments based on information systems and to push even further the very same logic of extension of the pool of data available towards a reasoning of total information awareness.

What was decided after all these negotiations has marginalised the EDPS and the FRA arguments as well as a part of the European Parliament discussing in the Libe Committee, but has convinced many other committees of the economic and strategic importance of the interoperability move. So, finally a series of five instruments of interoperability will be set up to link the three existing data bases (SIS2, VIS, Eurodac) with the three projects (EES, ETIAS, ECRIS-TCN) to come.

Interoperability: The slow rise of the data analysts and system engineers in the domain of internal security

Contrary to many traditional analysis of EU studies that read the interoperability program as a result of the terrorist attacks of 2015 and the willingness of the EU Commission to show that on these transborder matters between France and Belgium, they were useful and as tough as the national governments, we refuse the idea that they were the result of this crisis. The projects existed long before and if the attacks in Paris and Brussels were used as a political opportunity by a group of professionals to reinforce their positions, they were not an 'answer'.

Interestingly also, what was absent from the debate because nobody dare really to discuss it, was the boundaries of the EU data bases that the Commission wanted to render interoperable. If the goal was about efficiency regarding antiterrorism and to sew the divide between internal and external security, a completely different set of databases could have been mobilised including all the ones coming from defense as we will see in conclusion, but there, the debate was to settle in favour of EU-LISA the control of the integration of the different data bases and to keep it into the Justice and Home Affairs (JHA) area. This highlight the fact that, beyond the common rhetoric on interoperability as a counter terrorist necessity in front of an hybrid threat developed by the different actors in 2015, and especially the rhetoric of the European agenda on security, the effective merging of the institutions of security (defense and police) was not into this agenda in terms of decision making and practices. What was at stake was more a fight on the high end of policing between military intelligence services and their police counterparts, but the policemen, the border guards are very aware that letting military forces and intelligence enter into the interoperability debate would have been the equivalent of a colonisation of their domain. As in many other examples the great proposals of fusion of forces are not congruent with the sociology of competing guilds representing different professional and social universes (see Bigo 2014; Rhinard and Bossong in this volume).

The interoperability controversy and the struggles around it are therefore in my view a key moment of transformation of the field of 'security' by allowing a specific group of agents on the transnational scale, those who construct the data bases for their 'clients', that is, data analysts, civil engineer of integrated border management or IDM to become increasingly powerful. These actors are thus now able to compete with police, intelligence, immigration, border guard agencies on who decides and frames what is labelled security, insecurity and fate in Western societies through their key role on the exchange of information in policing matters. And interoperability tools are their flagship to change security into a commodity and a political technology of datafication.

Tools of interoperability: A technical approach or a politics by other means to bypass purpose limitation and to impose a digital reasoning?

These five tools were the following:

1 A **Single-Search Interface** or SSI called also the European search portal (ESP) whose task is to query several information systems simultaneously and to produce combined results on one single screen. This first tool seems innocuous given that the users have already the right to access to the different database and is technically light because it can be built on. The search can use different criteria using both biographical and biometric identity data coming from Central-SIS after modification of its organisation, Eurodac, VIS, and later on from the future EES, the proposed ETIAS and ECRIS-TCN systems, as well as the relevant data coming from Interpol systems and Europol files. This ESP is for the time being not connected directly to national databases. Existing national SSI solutions remain necessary for that purpose, nevertheless the suggestion is that in the future they will be replaced by a national uniform interface (NUI) in order to lead to a platform of integration of NUIs linked with the future EES.

2 A NUI will allow the effective interconnectivity of information systems where data registered in one system will automatically be consulted by another system. It will help the harmonisation of the search and index functions, even if no information will circulate (or be copied) from one database to another one; nevertheless the tool has a significant impact on all the existing databases, by relaxing the possibility of access to ancillary purposes.

3 **A shared Biometric Matching Service (sBMS)** is established in order to implement the search by integrating both fingerprints and facial images; the idea being that better consultation is not sufficient, because what is at stake is more cross-checking and identification. Here we jump from verification of identity beginning with the trust on the person's document to a systematic search of identification in order to establish suspects. This is why also, instead of upgrading the SIS, VIS, and Eurodac with a dedicated AFIS for each individual system, the sBMS will search across different EU information systems by generating and storing mathematical representations of the biometric data (SIS, Eurodac, VIS, the future EES, and the proposed ECRIS-TCN) in order to establish comparison and to detect anomalies.

4 **A Common Repository of alphanumeric Identity data renamed Central Identity Repository (CIR).** As explained by the initial report of the HLEG the shared BMS alone needs to be complemented by a common repository of alphanumeric data in order to aggregate to the biometrics attributes (fingerprints and facial images) the common biographical attributes (names, surnames, place and date of birth, sex, nationalities, travel documents) that are contained into the other data bases. For each set of data, the CIR will include a reference to the information systems to which the data belongs to from the various existing systems (Eurodac, VIS, the future EES, and the proposed ETIAS, and ECRIS-TCN systems) in order to construct a common identity repository facilitating law enforcement searches using data-presence flags and enabling the detection and prevention of identity fraud.

Even if the Commission and later EU-LISA recognised partly that the constitution of this repository, however, will require dealing with complicated questions of deduplication and disambiguation, they consider that it is possible and will improve the data quality by detecting discrepancies and in theory will limit investigation other than identification by distinguishing identification requests from other requests.

Clearly, for them, the CIR is the tool which justifies the cost of interoperability improvement. The Commission proposals share also this view and after discussions to clarify the option the terminology of central will replace the one of common identity repository, but this has opened a discussion if in fact the CIR was not already a new data base.[4] This was even more discussed when the Commission did not hesitated to insist in its final proposal for a new tool connected with the sBMS and performing a search for fraudulous identities check in addition to the storage of the CIR that the High-level Expert Group on Information Systems and Interoperability (HLEG) had implicitly discarded. Different reports have converged on the idea that the CIR coupled with a Multiple-Identity Detector (MID) is creating de facto a new set of data without a proper legal base, even if it seems that the technical process concerning the exploitation of results differs from the creation of new data. In any case the purpose to combat fraud cannot be interoperable for all data-bases and applicable to Eurodac and refugees, but this question has for the moment not be resolved and may come back again when the first implementation will begin and is followed by a court case.[5]

5 **MID:** The last tool was added by the Commission in order to provide a search for multiple identities associated to the same biometrics, becoming a 'fraud' detector. This would check whether queried identity data exists in more than one system and allow a mechanism for investigating and verifying the linked identity data (data held in the CIR as well as SIS). The MID would store links providing information when one or more definite or possible match(es) is(are) detected and/or when a fraud identity is used. It would check whether queried or input data exists in more than one of the systems to detect multiple identities (e.g. same biometric data linked to different biographical data or same/similar biographical data linked to different biometric data). The MID would show the biographical identity records that have a link in the different systems.

Practically these links will be labelled in four categories: white, yellow, green, and red: a white link meaning that the different biographical identities belong to the same person; a yellow link meaning that there are potential differing biographical identities on the same person; a green link confirming that different persons happen to share the same biographical identity; or a red link meaning that there are suspicions that different biographical identities are unlawfully used by the same person.

To finish the picture the interoperability proposals came alongside another one aimed at strengthening the mandate of the EU-LISA Agency, which was formally adopted on 14 November 2018.

This long description of the tools may be tedious to read for some, but it is necessary to understand that what is at stake is an incremental logic where the language, knowledge of technology imposes itself in security matters, not as a solution, but as a way of reasoning reframing what counts as security and danger. We are far from the idea of a technical support at work. EU-LISA becomes a central node of power, delegitimising the legal argument of purpose limitation and favourising speed in politics, as well as narratives of prevention and prediction, which have been used to justify already some dispositions of a state of emergency against terrorism and a generalisation of suspicion around circulation of money, of persons and of ideas via algorithms connected to 'big data' which have to have a certain degree of consistency. The search of a fraud regarding anyone claim to its own identity via check of biometrics identifiers result in the negation of language and dialogue with the person and the focus on the body as locus of truth versus the language as permanently suspected to lie. It also eliminates the dialogue with the person and privileges only the communication of transnational bureaucracy of controls between them,

objectifying even more the person as an object. Still important in the interaction with border guards in the integrated border management, it seems that the IDM pushes even further the logic of distantiation by negating the presence of the individual in favour of its data-double. If it is the case what interoperability means in a paradigm change linked with the mode of reasoning of a guild of professionals of digital technologies, who have not specific values in terms of security, but who have codes in mind for a data politics.

Integrated data management: A debordering of national space controls of border and a rebordering of transnational cyberspace bureaucracies led by EU-LISA?

IDM is supposed to have complemented Integrated Borders Management (IBM), but behind the formal consensus, it has been presented by the actors of EU-LISA as a paradigm change. It was an internal critique of the ways the borders are managed operationally by Frontex and the national border guards which has emerged mezzo voce. Stopping people at the borders and rendering these ones as electronic and physical walls, more and more militarised, with persons wounded or sent back in dangerous place (countries of origins or transits which are dictatorships and racist against migrants) as well as helping these places to train their forces to detain and torture, enslave or send back (almost to death in the desert) the peoples whose only crime has been to try to cross a border, is not only inefficient in terms of stopping or deterring people to move, but it creates on the contrary resistance, and the will to overcome the difficulties by the candidates to depart, especially if they are forced to flee combats (see Emma McCluskey). In addition, and even more importantly, in the views of these high-tech managers, it gives a bad image of the EU in terms of high value standards on human rights. It is impossible to continue to deplore low level standards of human rights in the countries of departure or to criticise Australia and the Unites States of Donald Trump, while reproducing at a more or less, lower scale their policies.

Violence is too strong and need to be diminished; some cynical agents adding that it needs to be at least less visible and more symbolic than obviously coercive. They propose, along the lines of the shift operated from extraordinary renditions to large scale surveillance of people by interceptions of personal data to do the same strategy at the border controls, and to develop smarter ways of control, less visibly coercive.

Instead of controlling persons at the borders, it is better to filter them before they arrive, to reinforce the visas procedures, the possibility to depart and to take the plans without previous authorisation. This allows to accept almost the 90% of people who are not considered as dangerous via check of their data online in order to focus on smallest numbers of persons when they cross borders. IDM is seen as an e-bordering using the frontier of the cyber space as the first and foremost line of control. Physical borders are not the first but the last line of 'protection'. Borders are smart when they are the results of a process of better identifications, not only of the flow of people arriving, but of each individuals, and it can be done only via statistics, profiling, predictive algorithms who use machine learning and common sense of border guards as two technologies (high and low) working simultaneously to help from the extraction of previous large batch of data to create profiles on people suspects to be 'like them', like the illegal ones, even if they are completely unknown, by the magic of discovering the weak signals of a group of correlations inside the mass of data which has been processed (Duez D.2017).

But this smart border management needs to connect all the data available and coming from very diverse part of bureaucracies and private (forced or complicit) partners in order to 'join the dots' and identify the potential weakness of each persons against different criteria. What is

therefore absolutely central is to link and to render compatible the different records of information in terms of additional information which can be gained (but not redundant) and in terms of automated formatting. Interoperability is the generic name (beyond the technical signifier) given to this so-called smart way to connect the dots and to avoid continuing to work in 'silos' with segmented information networks. The five instruments of interoperability are not tools, they implement the political technology for the datafication of internal security which help to the de-responsabilisation of the national politicians and the rise inside the field of security of non-traditional professionals of security, less oriented towards coercion but more indifferent to people.

The transformation of the dynamic of the field of security towards technologies and digital tools is therefore one of the key elements explaining that a narrative concerning security technologies as neutral tools allowing to detect suspects in advance, to prevent violent events, to potentially predict them, has developed recently. Even if the war on Terror has ideologically played a role by justifying this preventive approach, its persistence is correlative to the structural development of a private industry specialised on the domain of civil-security on one hand, and on the other to the rise of digitisation and forms of cybersurveillance by this transnational guild of digital technologies managers.

IDM versus IBM: Two different projects? A field dynamic

If the structuration of fights creates uncertainty about the two lines of thought derivating from their different practical logics, a trend in favour of preventive discourse and beliefs is visible in the last fifteen years. The actors of digital technologies have not only challenge the traditional conception and practices of detective policing, of criminal justice, presumption of innocence, they have also rendered almost obsolete the former groups of EU border guards who were seen as the reformers, when they proposed to push the border controls in the physical spaces of the neighbouring countries of the EU and into the countries of origins. This guild of policing at a distance mainly composed of border guards 'new style' and foreign affairs civil servants were (and are) still centrally interested in moving the practices of control of entry of their territory by a management of borders at distance done by consulates and private entities, with more or less explicit conditionalities between the EU and its neighbours on aid for development with counterpart on obedience to readmission agreements. But they do not represent anymore the future. They continue to play with extra-territorial logics, with territorial state borders controls, certainly displaced from the EU borders and managed at a distance, but this displacement is only geographical and the moves are towards other places similar to state borders and that geopolitics is still capable to imagine.

On the contrary, the inclusion of digital technologies adds to this existing layer on space, a temporal dimension where speed, anticipation is central. The interest on the data double and their identification ex-ante precede even the control of persons. Of course, the logics may be combined, and this is why data management continue to use the state territorial borders as a place for extracting (with a certain degree of discretionary power) data from the people who want to travel, but their priority is to build algorithms about criteria of dangerosity and calculation of scores in a scale of risk and suspicion, suggesting individuals who have not yet done anything but look like others which have been criminals (Bigo in Cassin 2013). Nevertheless the logic of algorithms will not be a direct profiling of identified people but the detection of anomalies (Aradau and Blanke 2017). The predictive argument here is therefore not one based on the past of an individual but with its adequacy concerning a given profile of behaviours reading the future as a future already done, as a future perfect (Bigo 2010).

The impact of this emergence for the field of the EU internal security professionals

The entry of the 'guild of digital technologies' into the field of professionals of security after the concentration of different networks into the EU-LISA agency on one side and the ESRIFF group of companies on the other side, has allowed them to compete with policemen, border guards, migration, and asylum officers to frame the practices of security today. An example of this impact of these professionals of digital technologies, to succeed to have their share of budget via the topic of artificial intelligence specifically dedicated to policing and border management as well as intelligence prevention, all of those being merged with the future projects of the programs of an interoperability at the scale of the global North. This guild of digital technology has supported the lines of predictive policing, artificial intelligence, and redefinition of justice and punishment, which were already supported mainly by military and signal intelligence services, and by some border guards and counter terrorist police forces. This support is certainly more important than the legacy of the discourse of the war on terror of 2001 and 2004, or the theme of the penal law of the enemy and permanent state of emergency reinvented after 2015 in Europe. It has given a knowledge claim of credibility of prevention by technologies of machine learning and profiling with predictive features. It has created new incentives for a digital economy interested into dual technologies but also war and defense, including spatial activities (see Larsson in this volume). The clash of conception and strategies between this preventive line of speculative security and surveillance mechanisms and the more traditional visions of criminal justice, border controls on foreigners, ending up with a so called dilemma between security and privacy has almost replaced in the remnant political discussions the previous heated debates between security and freedom of movement for EU citizen and third country nationals residing inside the EU which were so central until the 2000s. Now freedom, solidarities with refugees are seen under this paradigm of technologies of identification and prediction via the interconnection between different parts of the cyberspace controlled by hybrid of public-private bureaucracies, which present themselves as the path towards the future of democratic societies.

Conclusions: Security as commodity for the digital economy?

Security has been transformed by its technologisation into a commodity. Lucia Zedner was among the first to analyse this move and to connect it with the turn towards a pre-crime logic necessity to find way to predict which looked scientific (Zedner 2007). Interoperability of JHA databases is the first node into a series of even more interconnected elements, including the integration of PNRs in Europe and on both side of the Atlantic, as well as the development of integration of data bases not yet integrated because they were not managed by EU-LISA (Prum DNA data base, ENISA) or coming from Defense and foreign Affairs on one side (Eurosur, EU piracy, GPS-Navy, Nato Marsur) and of the Welfare and big cities bureaucracies on the other (Bigo 2015; see Ragazzi, in this volume).

As a commodity, security is on sale and has a market which generates profit. EU-LISA is both a broker and a stock exchange place for these technologies. Nowadays smart borders, IDM, interoperability between data bases, algorithms, artificial intelligence technologies (AI) are the new keywords for any project regarding the current developments on intelligence, policing, borders, migration, and asylum matters.

Are technologies serving security professionals or is security colonised by engineers and data analysts transforming its efficiency but also its meaning and practices? If it is too soon to conclude, what is almost certain after this research on interoperability is that the role of the actors

managing technologies (especially digital ones) is becoming more visible and more important than before. Public partners coming from Ministries of interior and justice, or Ministries of defense and foreign affairs are keen to find private firms who have developed technologies serving the purpose of identification of people and prediction of their behaviour. A race on different types of biometric identifiers less visible than before is re-opened moving from DNA analysis, scanned fingerprints to facial recognition by multiple cameras, ways of walking in a mob where people will be unaware they are checked. But this can work only if all the parameters of these biometric identifiers are digitalised in order to be compared between them and with other collected data. Beyond the IBM identification of people from their biometrics, the IDM collection and interception of data in large scale allows algorithms to do correlations and to build profiles who have some time self-correction through machine learning. But gathering so many heterogeneous types of data distributed in diverse data bases supposes to have the tools of interoperability we have described between data bases, in order to have either simultaneous checks in different data bases on screen, or to get results against an integrator module that has already filtered suspicious cases from previous data sets.

Huge amount of money is now devoted on both side of the Atlantic and in Australia around these technologies of identification and interoperability with the hope to get accurate predictions and to prevent dangerous actions before they happen by following weak signals. The EU on its Horizon Europe 2021–2027 (following Horizon 2020 research project) dedicates under the topic of Artificial Intelligence, 7 billion for helping European companies to develop these researches on digital technologies for internal security purposes.

But why? Are these investments justified? Would digitisation of data with its gain on speed of information and its pretense to predict future events, will be a solution in the search of suspects of political violence, crime, trafficking, illegal movements of travelers? This is the promise sold by the professionals of digital technologies, but how far can we believe their stories when their narratives is not based on the past and evaluation of their (in)adequacies, but on the miracles of not yet in place technological solutions to insecurities of all sorts? Are politicians unaware of the risk to create a new kind of fortune tellers, well paid for poor results? May be not, but they may think that in that case, each time events happen, taking them by surprise they may escape to focus on the political root causes of these events (bombings related to escalations in conflicts and called terrorist attacks, escape in large numbers of dangerous zones and attempts to arrive in other countries for a small proportion of them called flows of migrants), and to present to the population than the failure of today can be solved only by the present technologies who claim to control, manage, prevent the situation, in order to protect their nation, their way of life, and by investments in even more sophisticated technologies in the years to come. This logic has been explained by Paul Watzlawick in his famous book, how to succeed to fail.

Technological commodity of security: A de-responsibilisation of politicians?

At the heart of this move towards the digitalisation of mechanisms of control, one can identify a trend inside the (in)securitisation process to abandon responsibility in practice while inflating rhetoric around danger and unease by the professionals of politics (Bigo 2002). Political judgements taken in the name of sovereignty concerning what kind of threats have to be prioritised, have been avoided. To limit this tendency of governments, often back-bencher politicians have tried to repoliticise the debates but often the politics of security has been reduced to controversies around what tools are the best to create technological and automated solutions (for a debate see Neal 2018). And, in a way, this mimics the discussion on the drones and more generally the

rise of an authoritarian liberalism (Chamayou 2018). Guilt and responsibility of the highest levels are redistributed on other groups, especially when situations do not ameliorate, but on the contrary, are worsened by the use of these technologies theoretically so 'smart'.

This creates a huge convergence, despite political ideologies and public policies diverging on the naming of these so-called crisis to build in more technologies and to justify them as solutions for any type of events considered as a threat, as a risk or a danger. Western governments are rarely in agreements, except for pushing the idea that technologies of identification on suspects will solve security problems, and that a healthy competition between major firms to do research for high tech projects on these domains is central for 'innovation'. But each coalition of actors (private companies, public bureaucracies of control, international organisations) consider that its competitor is trying to have an unfair dominant position and ask for more resources in a kind of escalation in the name of the better protection of an 'homeland' regarding the other places.

Crucially, the later argument of an economic and symbolic competition almost always trumps the claims that these technologies may be legitimate against violence but need to be proportionate in order of not breaching (at least not too much) privacy, as this competition involves huge economic (and political) interests in new developments of the 'digital' revolution. It explains why, at the end of the day, parliamentarians in many countries and in the EU accept to vote in favour of these tools, despite the risk for privacy and rule of law.

One element which helps enormously EU-LISA was that the EU council and the EU commission have been both very keen to set up their own industry versus the one of the United States, considered as dominant. They may have done that differently, as the council of the EU has sang the music of pooling sovereignties against the giants (the United States, the Gafa) while the EU Commission has refused to be seen too much as a political actor, centralising the different regional strength. But, the strategy of the later has therefore been to pretend that the different DGs were just experts, technical providers helping the different national governments, their police and border forces to choose the best technology fitting their multiple purposes. The DGs research and industry have presented themselves as 'mediators' interacting with the diverse private actors in order to constitute an efficient European pole of security industries and services allowing growth inside the EU via the development of dual technologies going from drones of surveillance, artificial intelligence helping search of suspects, indicators of frauds to identity, or more banally better interconnections between data bases in order to 'joint the dots'. In total security claims have been merged with technological innovations and growth arguments to resist counter claims that the project of an IDM was not solving security but creating new problems and in addition a web of technologies of large scale surveillance transforming the nature of democratic regimes in the EU and in the global North.

Notes

1. COM(2016) 194 final, 6.4.2016. The system will electronically register the time and place of entry and exit of third-country nationals, and calculate the duration of their authorised stay. It will replace the obligation to stamp the passports of third-country nationals which is applicable to all Member States. The objectives of the EES also include prevention of irregular immigration and facilitating the management of migration flows. The EES will contribute to the identification of any person who does not fulfil or no longer fulfils the conditions of authorised stay on the territory of Member States. Additionally, the EES should contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences.
2. COM(2016) 731 final, 16.11.2016.

3. COM(2016) 7 final, 19.1.2016.
4. Cf the PE Optimity report p. 13. The description and analysis of these different tools came from discussions with Niovi Vavoula. Her PhD has made the demonstration of the legal elements which goes against a blind faith into the interoperability pure technicality. I do not develop here this part of the argument but it is a must read for anyone who want to develop a legal analysis.
5. Clearly the purpose of the MID to combat identity fraud is not supported by the legal basis for Eurodac on refugees.

References

Adler-Nissen, Rebecca. 2012. *Bourdieu in International Relations: Rethinking Key Concepts in IR*. Abingdon: Routledge.

Anderson, Malcolm. 1989. *Policing the World: Interpol and the Politics of International Police Co-Operation*. Oxford: Clarendon Press.

Anderson, Malcolm and Monica Den Boer. 1994. *Policing Across National Boundaries*. London: Pinter publications.

Aradau, Claudia and Tobias Blanke. 2017. "Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data." *European Journal of Social Theory* 20 (3): 373–391.

Balzacq, Thierry and Sarah Léonard. 2013. "Information-Sharing and the EU Counter-Terrorism Policy: A 'Securitisation Tool' Approach." In *European Security, Terrorism and Intelligence*, edited by Christian Kaunert and Sarah Léonard. London: Palgrave Macmillan, 127–142.

Basaran, Tugba, Didier Bigo, Emmanuel-Pierre Guittet, and RBJ Walker. 2016. *International Political Sociology: Transversal Lines*. Abingdon: Routledge.

Bigo, Didier. 1996. *Polices en réseaux: L'expérience Européenne*. Presses de la Fondation nationale des sciences politiques. Paris

Bigo, Didier. 2002. "Security and Immigration: Toward a Critique of the Governmentality of Unease." *Alternatives: Global, Local, Political* 27 (1): 63–92

Bigo, Didier. 2006. "Security, Exception, Ban and Surveillance". In *Theorizing Surveillance. The Panopticon and Beyond*, edited by David Lyon. Devon: Willan Publishing, 46–68.

Bigo, Didier. 2010. "The future perfect of (in) security (P8): pre-crime strategy, proactivity, pre-emption, prevention, precaution, profiling, prediction and privacy." www. interdis ciplines. org/paper. php (accessed on 23 June 2020).

Bigo, Didier. 2013. "Sécurité maximale et prévention? La matrice du futur antérieur et ses grilles." In *Derrière les grilles: sortir du tout évaluation*, edited by Barbara Cassin. Fayard: Mille et une nuits.

Bigo, Didier. 2014. The (in) securitization practices of the three universes of EU border control: Military/Navy–border guards/police–database analysts. *Security Dialogue* 45, nº 3: 209-25.

Bigo, Didier. 2015. "Electronic Large-scale Surveillance and Watch Lists: The Products of a Paranoid Politics? Vigilancia electrónica a gran escala y listas de alerta: ¿Productos de una política paranoica?" *REMHU: Revista Interdisciplinar da Mobilidade Humana* 23 (45): 11–42.

Bigo, Didier. 2016. "Sociology of Transnational Guilds." *International Political Sociology* 10 (4): 398–416.

Bigo, Didier. 2020. "The socio-genesis of a guild of 'digital technologies' justifying transnational interoperable databases in the name of security and border purposes: A reframing of the field of security professionals?" In *Freedom, Technology, Surveillance Paradoxes in the Making. International Journal of Migration and Border Studies* 6, nº 1-2 (1 janvier 2020): 74-92.

Bossong, Raphael and Michael Rhinard. 2016. *Theorizing Internal Security in the European Union*. Oxford: Oxford University Press.

Brouwer, Evelien. 2008. "Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System." *Immigration and Asylum Law and Policy in Europe* 15: 1–596.

Carrera, Sergio, Steven Blockmans, Jean-Pierre Cassarino, Daniel Gros, and Elspeth Guild. 2017. "The European Border and Coast Guard: Addressing Migration and Asylum Challenges in the Mediterranean?" *CEPS Task Force Reports*. Available at https://www.ceps.eu/ceps-events/ /

Carrera, Sergio and Valsamis Mitsilegas. 2017. "Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights on Countering Terrorism and Crime." *Centre for European Policy Studies*. CEPS-Bruxelles

Chamayou, Grégoire. 2018. *La société ingouvernable. Une généalogie du libéralisme autoritaire*. Paris La Fabrique.

Collantes-Celador, Gemma and Ana E. Juncos. 2012. "The EU and Border Management in the Western Balkans: Preparing for European Integration or Safeguarding EU External Borders?" *Journal of Southeast European and Black Sea* 12 (2): 201–220.

Deflem, Mathieu. 2000. "Bureaucratization and Social Control: Historical Foundations of International Police Cooperation." *Law and Society Review* 34 (3): 739–778.

Den Boer, Monica. 2011. "Technology-Led Policing in the European Union: An Assessment." *Technology-Led Policing: Journal of Police Studies* 3 (20): 39–56.

Den Boer, Monica. 2013. "Towards a Governance Model of Police Cooperation in Europe: The Twist Between Networks and Bureaucracies". In *International Police Cooperation: Emerging Issues, Theory and Practice*, edited by Frederic Lemieux. Willan Publishing, Milton Parl, UK. 42–61.

Den Boer, Monica and Neil Walker. 1993 "European Policing after 1992." *Journal of Common Market Studies* 31 (1): 3–28.

Duez, Denis. 2017. "Des smart borders aux clôtures barbelées: la revanche du low-tech?" *Cahiers de la Sécurité et de la Justice* 4 (38): 168–176.

Glouftsios, Georgios. 2018. "Governing Circulation through Technology within EU Border Security Practice-Networks." *Mobilities* 13 (2): 185–199.

Guild, Elspeth. 2006. "International Terrorism and EU Immigration, Asylum and Borders Policy: The Unexpected Victims of 11 September 2001." In *Public Policy and the New European Agendas*, edited by Fergus Carr and Andrew Massey. Edward Elgar Publishing, Cheltenham. 233–248.

Guild, Elspeth and Didier Bigo. 2005. "Policing at a Distance: Schengen Visa Policies." In *Controlling Frontiers. Free Movement into and within Europe*. Burlington: Ashgate.

Guild, Elspeth. (2019). Counter-Terrorism Resolutions and Initiatives by Regional Institutions: EU and European Court of Human Rights. *International Human Rights and Counter-Terrorism*, 109-124.

Guild, Elspeth. Forthcoming 2020. *Anti/Counter-Terrorism and Human Rights in Europe, Queen Mary report*. Paris: L'Harmattan. Available at https://www.qmul.ac.uk/law/media/law/docs/events/QMUL-Report-July-2018.pdf (accessed on 23 June 2020)

Guild, Elspeth and Sergio Carrera. 2013. "EU Borders and Their Controls: Preventing Unwanted Movement of People in Europe?" *CEPS Essays* 6.

Illamola Dausà, Mariona. 2015. "Eu-Lisa, the New Model of Operational Management of the Various EU Databases." *Revista Cidob D'afers Internacionals* 111: 105–126.

Johnson, Loch K. *A Season of Inquiry Revisited: The Church Committee Confronts America' Spy Agencies*. Kansas U press, 1986.

Kauppi, Niilo. 2013. *A Political Sociology of Transnational Europe*. Colchester: ECPR studies.

Kauppi, Niilo and Mikael Rask Madsen. 2013. *Transnational Power Elites*. Routledge.

Liang, Hsi-huey. 1992. *The Rise of Modern Police and the European State System from Metternich to the Second World War.* Cambridge/New York: Cambridge University Press.

Mitsilegas, Valsamis. 2008. *Databases in the Area of Freedom, Security and Justice: Lessons for the Centralisation of Records and their Maximum Exchange*. Cambridge University Press.

Mitsilegas, Valsamis, Jörg Monar, and Wyn Rees. 2003. *The European Union and Internal Security Guardian of the People*. Palgrave Macmillan.

Monar, Jörg. 2002. "Justice and Home Affairs in a Wider Europe; The Dynamics of Inclusion and Exclusion." In *The European Union: Annual Review of The EU 2001/2002*, edited by Geoffrey Edwards and Georg Wiessala. Oxford, UK: Blackwell, 28–40.

Monar, Jörg. 2013. "The EU's Growing External Role in the AFSJ Domain: Factors, Framework and Forms of Action." *Cambridge Review of International Affairs* 3: 1–20.

Neal, Andrew W. 2018. "Parliamentary Security Politics as Politicisation by Volume." *European Review of International Studies* 5 (3): 70–93.

Sheptycki, James W. E (1998). Policing, postmodernism and transnationalization. *The British Journal of Criminology*, *38*(3), 485–503.
Scheptycki, James W. E. 2000. *Issues in Transnational Policing*. London and New York: Routledge.
Schiopu, Aura and Florin Bobin. 2015. "European Agenda on Security for 2015–2020, Instrument Supporting the Joint Action of the Member States against the New Challenges." *European Journal of Public Order and National Security* 2 (6): 33–36.
The US Commission Report of 9/11/2001. 2011. *Final Report of the National Commission on Terrorist Attacks upon the United States*. Government Printing Office.
Trauttmansdorff, Paul. 2017. "The Politics of Digital Borders." In *Border Politics: Defining Spaces of Governance and Forms of Transgressions*, edited by Cengiz Günay and Nina Witjes. Cham: Springer, 107–126.
Tsianos, Vassilis S. and Brigitta Kuster. 2016. "Eurodac in Times of Bigness: The Power of Big Data within the Emerging European IT Agency." *Journal of Borderlands Studies* 31 (2): 1–15.
Vavoula, Niovi. 2017. "Immigration and Privacy in the Law of the EU: The Case of Databases." PhD Thesis, Queen Mary University of London.
Wallace, Helen and William Wallace, eds. 2000. *Policy-Making in the European Union*. 4th ed. Oxford: Oxford University Press.
Whitaker, Roger. 2006. "A Faustian Bargain? America and the Dream of Total Information Awareness." In *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty and Richard Ericson. Toronto: University of Toronto Press, 141–170.
Zedner, Lucia. 2007. "Pre-Crime and Post-Criminology?" *Theoretical Criminology* 11 (2): 261–281.

See Annex Below:

Data are coming from the Study on Interoperability of Justice and Home Affairs Information System

Entity	*SIS II*	*EURODAC*	*ECRIS-TCN*	*VIS*	*ETIAS*	*EES*
Europol	Yes	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: access to ECRIS-TCN But not ECRIS in its current format	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: preventing, detecting and investigating terrorist and criminal offences
National law enforcement authorities	Yes	Yes: to check against latent fingerprints	No	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: preventing, detecting and investigating terrorist and criminal offences	Yes: preventing, detecting and investigating terrorist and criminal offences
Visa authorities	Yes	Yes	Yes: may apply to criminal records authorities for access	Yes	Yes: in the event of rejection after automated application process	Yes

[*continued*)

Entity	*SIS II*	*EURODAC*	*ECRIS-TCN*	*VIS*	*ETIAS*	*EES*
National border control	Yes	Yes	No	Yes	Yes: only for verification purposes	Yes
Immigration authorities	Yes	Yes	Yes: may apply to criminal records authorities for access	Yes	No	Yes
Asylum authorities	Yes	Yes	Yes: may apply to criminal records authorities for access	Yes	No	No
Eurojust	Yes	No	Yes access to ECRIS-TCN but not ECRIS in its current format	No	No	No
Judicial authorities	Yes	No	Yes: apply for access to criminal records data of an individual undergoing criminal proceedings	No	No	No
Central Authority for Criminal Records	No	No	Yes: storage of criminal records data	No	No	No
Customs officers	Yes	No	No	No	No	No
Vehicle registration authorities	Yes	No	No	No	No	No
Private organisations	No	No	Yes: if appropriate, can apply to view the criminal history of EU nationals during recruitment	No	No	No