EU LISA. A Special Case in the European Approach to Artificial Intelligence

Giulia Maria Gallotta
Education Science, Psychology and Communication Science Dept.
University of Bari "Aldo Moro"
Via Scipione Crisanzio, 42
70122 Bari
Italy

Abstract:

eu-LISA, the EU Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, is one of the most recent and more ambiguous application of Jean Monnet's functional method of integration. At first sight, its core business is about the implementation and management of EU databases in the field of free movement of persons and migration control. In fact, it is more and more becoming one of the main tools in the EU policy of closure towards irregular migrants, irrespective of their eventual right to asylum and protection. In this sense, I analyze eu-LISA as a new and further step towards the depersonalization of irregular migrants or rather their transformation in alphanumeric data, which can be easily erased. All this is realized through technical tools that do not draw attention from European public opinion.

1. The process of European integration began in the 1950s following the intuition of J. Monnet: the only antidote to the outbreak of new wars in Europe would be the construction of effective, efficient and lasting forms of cooperation among European states. These forms of cooperation would be all the more effective, efficient and lasting the more they satisfied two precise criteria: on the one hand, creating and consolidating de facto solidarity, i.e. concrete social and economic ties between civil societies and the productive fabrics of the States involved. Secondly, they should operate in technical areas which, by concealing the highly political and long-term project of the creation of a European federal union would discourage public opinion in the broad sense of citizens, associations and political parties, from being interested in them precisely by virtue of their technical nature. In this sense, it is worth underlining that today there are several scholars who believe the 'crisis' of the integration project also depends on the fact that the challenges it has to face are eminently political in nature and urge citizens to take sides for or against possible solutions in rather partisan terms, reducing the leeway for compromise of the respective national governments (Börzel 2016; Kamkahji Radaelli 2017; Brack Gurkan 2020).

However, this concerns the major issues that the EU must address above all, such as the management of migratory flows, the energy transition, the war in Ukraine, the rights of individuals and workers in the increasingly deregulated and disintermediated world of work ushered in by new communication technologies.

There are also new spheres of EU action in which Monnet's functional logic still prevails, i.e. sectors in which the attention of both scholars and public opinion and the control of the European Parliament are decidedly weak and incomplete, precisely because of their extremely technical nature.

One of these is eu-LISA, the EU Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Eu-LISA was founded in 2011 with the aim of relieving the Commission from the task of implementing and managing the databases linked to the development of the Schengen area of free movement of persons, i.e. the SIS (Schengen Information System, which concerns data on persons with criminal convictions or under investigation in Europe), the VIS (Visa Information System, i.e. the collection of both biometric data and fingerprints of those applying for a visa to enter the EU and of the applications themselves and their outcome) and EURODAC (system for collecting biometric data and fingerprints of irregular migrants arriving in the EU). In this sense, eu-LISA is responsible for all the operations necessary to guarantee the correct functioning and full usability of these databases 24 hours a day, seven days a week. This task is accompanied by that relating to the design, development and management of new large-scale IT systems that the EU institutions or technological developments may make necessary (Reg. 2011, art.1) with a view to exploiting possible synergies among databases themselves (Glouftios 2021). In this sense, as far back as 2018, a new regulation extended the data systems, object of design and implementation by eu-LISA to EES (Entry/Exit System, for registering all those who legally cross EU borders), ETIAS (European Travel Information and Authorization System, which verifies the non-dangerousness for the EU of citizens legally coming from countries exempt from visa obligations) and dublinet (connection system for decisions relating to applications for protection pursuant to the Dublin regulation).

In 2019, ECRIS-TCN was added to these, i.e. the European criminal records information system, which allows the judicial offices of the Member States to access information on any criminal convictions of non-EU citizens, issued in any EU Member State.

With respect to these databases, eu-LISA engineers are concerned with ensuring an «effective, secure and continuous operation…the efficient and financially accountable management…an adequately high quality of service for users…continuity and uninterrupted service…a high level of data protection» (Reg. 2018, art.2) and training actions for personnel who in the Member States use these same databases and the relative search and data entry interfaces. It is, therefore, a technical agency, which limits itself to managing, maintaining and possibly developing the IT architecture necessary to guarantee the exchange of data and information among the competent authorities of EU Member States. And in this sense, it is on the latter that the responsibility essentially falls for the correctness of the data entered, for their quality and for respecting the right to privacy of the data subjects, the responsibility of eu-LISA being limited to the exchange of data in its communication networks.

This is what the Agency itself takes care to reiterate in its strategic guidelines. The statement that «its primary mission [is] to dedicate itself to continuously adding value to the Member States, supporting through technology their efforts for a safer Europe» (eu-LISA 2017: 3) recurs on almost every page both in the eu-LISA long term strategy and in the medium term one and accompanies the indication of the planning and implementation of the information systems that the agency carries out. It is a technical and reliable agency, therefore, which manages IT systems in the interest of the Member States, systems which are absolutely neutral, as technological tools.

However, suffice to look a little deeper to realize that appearances may be deceiving. As Glouftsios writes, large-scale computer systems are «objects that create the grounds on which other objects operate; they are things and also the relation between things» (Glouftsios 2020: 453). From this point of view, eu-LISA is not only the agency that designs, manages and guarantees the functioning of EU databases and the network for their supply and for the exchange of their information between Member States. It is also the device which, in concert with Member States technicians, for example, defines the criteria on the basis of which the data, feeding the various IT systems, are codified and catalogued, thus dictating which of the various possible criteria are relevant for the orderly storage of data and for their retrieval and which criteria are not. From this point of view, the report, published by the Union Agency for Human Rights in 2020 on artificial intelligence systems, underlines how precisely these apparently technical configuration operations present a high risk of transferring to the EU level prejudices or biases of programmers or of those who, at a national level, enter data into EU databases, if it is to be their operations that provide the prototype for processing EU IT forms (FRA 2020). Furthermore, eu-LISA designs IT systems and verifies their correct functioning, but their physical implementation, such as the supply of digital data storage spaces, is entrusted to external companies through calls for tender. The resulting contracts contain precise obligations regarding data protection and confidentiality that the contractors must respect but it is clear how these activities can give rise to a potential grey area in which data could be used for other purposes than those allocated by EU institutions (Glouftsios 2021).

2. Nonetheless, the IT systems managed by eu-LISA are very efficient in carrying out their tasks. The amount of information exchanged and the speed of the exchange itself have created undoubted advantages for the Member States and their border or judicial authorities and this generates an important incentive for the multiplication of IT systems themselves. In this sense, in 2019, the EU adopted new regulation which foresaw the creation of a system of interoperability among the databases, managed by eu-LISA, i.e. the development of a single interface for research and cross-comparison of the data contained therein. It is, without doubt, a tool that will allow national operators to save a considerable amount of time, as they will be able to cross-check biometric data, visas or international protection requests and the criminal records of persons subject to checks through a single search portal, whether they are more or less regular migrants, long-term residents or simple non-EU visitors. Interoperability, however, also poses several problems. First of all, it strengthens the link between migration and crime that has always underpinned policies for managing migration flows and contributes to framing migration issues in terms of security protection for the receiving states rather than welcoming those who arrive. Furthermore, interoperability relies on the recording and conservation of the increasingly extensive biometric data of individuals, with respect to which the same EU rules impose particular obligations of protection, given their extremely sensitive nature. However, is a migrant who has arrived by chance at the borders of the EU able to understand what use will be made of the data that s/he is obliged to provide to border police? Will eu-LISA be able to guarantee the confidentiality of these data in the mass exchange of communications among various national authorities? Who will be concerned with their cancellation in keeping with the terms prescribed by EU rules? (Aden 2020) How can we remedy inaccuracies that can arise from the very cross-referencing of biometric data, given the difficulties encountered in matching these data and the identities of individuals, especially in the case of specific ethnic groups (FRA 2020)? In a 2020 essay, Leese analyses this growing reliance on individuals' biometric data as the latest stage in a long historical process that has developed parallel to the assertion of state sovereignty and which is based on the authorities' constant refinement of identification techniques for people present on its territory in order to obtain resources through taxation, defence tools through compulsory conscription and, especially since 11 September

2001, information to prevent threats to national security (Leese 2020; Glouftsios & Bellanova 2020). As Bigo points out, the problem is that in the name of security, i.e. of a largely shareable value that is expressed through the use of highly technical tools, any separation between databases is overridden in a growing and tendentially inextricable multiplication of both the actors who have access and of the sensitive data itself circulating in a system, where the rules concerning their protection do not always have a univocal imputation centre (Bigo 2020). And while it may be difficult for a foreigner with a visa to understand what use is made of his/her personal and biometric data, one can only imagine what a migrant who arrives by chance at the borders of the EU after a long and tormented journey might understand, especially when his/her chances of entering the EU are closely bound up in the collaboration shown, including providing one's own biometric data.

In fact, what seems to emerge is an enormous system of archiving and managing the sensitive data of non-EU citizens and above all of irregular migrants, in conditions of data protection which the privacy appears questionable, due precisely to the high number of subjects granted access to it, seem dubious at the very least.

3. This is all the more noteworthy when compared with the EU acts on Artificial Intelligence (AI). A 2017 EP resolution on robotics was the first to address the issue of developing machines capable of acting instead of humans in delicate areas of social interaction, such as care, health or the adoption of decisions with major consequences for the recipients. It stated that any development on the subject should be informed with the principles of «human safety, health and security; freedom, privacy, integrity and dignity; self-determination and non-discrimination, and personal data protection» (EP 2017: 10). The European Commission and in turn the Council have, since then, constantly developed a so-called anthropocentric approach to AI.

In particular, the European Commission articulated its position in three communications adopted in a rapid sequence, between 2018 and 2020.

In the first, the focus is on the consequences in terms of economic growth that developments in the field of AI can guarantee for the EU and on the delay of European investments in this field compared to the main international competitors, China and the USA in particular. In this sense, the Commission underlines the need for the EU and its Member States to act on two fronts. On the one hand, it is a question of promoting training actions and educational paths which enable EU citizens to acquire the knowledge and skills necessary both to profitably enter the new information economy but also to direct its developments thanks to the high quality of European human capital. On the other hand, the Commission underlines how essential it is to establish a regulatory framework for the development of AI which respects and protects the fundamental values of the EU and which is capable of directing its developments on an international level, claiming a sort of potential standard-setter role (European Commission 2018). What these values are is specified in a brief communication in 2019, in which the Commission takes up the text of art. 2 of the Lisbon Treaty, according to which the EU is founded on the «values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities» (European Commission 2019: 2). In addition to compliance with these values, AI systems must support precise requirements regarding their functioning, which allow citizens to trust and appropriate them on a personal and economic level. Among these requirements, a key role is entrusted to the scope for human intervention, data confidentiality and the protection of «diversity, non-discrimination and fairness» (ibid.:3) and to the accountability of AI systems, i.e. the ability to justify the results generated by their respective algorithms.

What this means is well articulated in a 2020 communication. Here, the starting point is the potentially opaque nature of AI. This opacity concerns both the understanding of the functioning and logic of the algorithms that regulate the learning processes of AI systems and the possibility that the amount of data that feeds them, coupled with the calculation capabilities and the algorithmic associations that substantiate their operations bring about non-transparent decision-making processes or decisions that reflect discrimination of various kinds or that AI is used for criminal activities. In this sense, it is not just a question of promoting high-profile research, the diffusion of AI among SMEs and public-private partnerships to finance AI research and diffusion, what the Commission defines as an "ecosystem of excellence" (European Commission 2020: 3).

The aim is to create a regulatory system that does not limit itself to protecting «human dignity and privacy protection» (European Commission 2020:2) for Europeans but provides project and operational standards for any designer/supplier/user of AI systems who wishes to operate or sell them in the EU. In this sense, the Commission underlines how the data that feed and train AI systems must respect the privacy of those from whom they come and the absence of bias must be verified, as well as scope for human verification always being foreseen, such as the correction of data and/or results, especially in the case of algorithmic decisions that can have major consequences on individuals, such as those in health, judicial matters or on the provision of subsidies or bank loans. Above all, every AI system must be understandable and the process that leads to the observable final outcomes must be explainable (ibid.).

In the space of two years, with these three communications, the Commission has therefore traced the lines and principles that must guide the AI development and diffusion in the EU and which should be its flag in trade relations with international partners. And these all find their roots in the need to combine attention to keep pace with the development of technologies that evolve much faster than legislators are able to regulate them with that of the important consequences that these same technologies are likely to have on people not only in terms of obsolescence of their skills on the labour market but also of surveillance of the most disparate activities and influence on personal opinions and socially relevant behaviours. But also be careful that information technologies, like all technology, are at the service of individuals and do not harm their fundamental right of dignity and guarantee respect for privacy.

All subsequent EU acts are merely applications of these principles to specific cases. The 2021 *Digital Act* proposal, for example, clearly indicates which AI systems are prohibited in the Union and which ones are considered high-risk and are, therefore, subject to precise requirements in terms of design and pre and post use controls on the EU market. Prohibited AI systems include all those systems which, through subliminal techniques or by exploiting the fragility of the subjects to whom they are addressed, are able to «materially distort their behavior in a way that causes or is likely to cause that person or another person physical or psychological harm» (European Commission 2021: art. 5.a) or which may be used for purposes of social evaluation of the behaviour of individuals or groups, the use of remote biometric identification tools in real time in confined spaces, with specific exceptions relating to the protection of safety or of victims of crime. For AI systems considered high-risk, on the other hand, in addition to a vague definition that identifies them on the basis of the degree of danger with respect to their ability to negatively influence the enjoyment of fundamental rights by individuals, the Commission attached two lists, in which they are presented in a non-exhaustive way (European Commission 2021, Annex III). These include, for example, AI systems that can be used to assess the creditworthiness of individuals or their compliance with rules for receiving subsidies or their assessment in education/training institutions or in criminal proceedings or, with relation to migration management, to assess the applicants' compliance with the criteria for benefiting from an international protection status or the veracity of their statements or of documents produced in support of their applications (ibid.). For these systems, there are precise procedures that regulate their supply and use on the EU market and systems for monitoring their operation. An article is also dedicated to AI systems that interact with people and provides for the obligation to make known the artificial nature of the interlocutor, especially in cases where the latter may record and identify emotions or generate deep-fake content (ibid.: art.52).

These are regulatory proposals still subject to discussion between the Council and the European Parliament and no communication has binding effect. However, they clearly outline the perimeter within which AI should develop in the European Union. This will have to express/expand its potential within precise criteria of respect for those rights of individuals, which are the identity card of the EU, and of transparency as regards their use and their operational algorithms[1]. If we think that eu-LISA does not use AI systems but is a simple network that connects data without containing it itself (Bigo 2020), as demonstrated by the fact that the privacy protection obligations fall on the Member States, and that the Commission has recently adopted two regulations governing the rules of use and circulation of these data[2] to ensure transparency of use and confidentiality, objectively there seems to be nothing to worry about. Eu-LISA is a technical tool which, thanks to its efficiency, guarantees rapid exchanges of data between various national authorities, facilitating and streamlining their work.

4. Does this mean that everything is alright? Not really. Or rather not necessarily. It may be for EU citizens, as they will be able to rely on ever more refined devices to protect their safety. Less so for those who want to enter the EU legally and who will have to go through increasingly complex identification/visa issuance procedures. Definitely much less for the so-called irregular migrants, those who arrive at the European borders without a visa or other documents to guarantee access and must therefore prove they possess the requisites to enjoy refugee status or subsidiary protection. June 2013 *Directive on procedures for granting and withdrawing international protection status* already includes the lack of cooperation by individuals in the collection of biometric data among the grounds for rejection. This means that the data processed by eu-LISA are constantly growing. And with them, the temptation to use them.

In this sense, a project by the University of Manchester, financed with *Horizon 2020* funds, made it possible to develop iBorderCtrl, an EU border control system which, on the basis of a facial recognition system, should be able to detect false statements in the answers to questions about the origin, duration and reasons for travel, addressed by an avatar to each traveler bound for the EU. The level of falsehood that the system identifies in the answers

[1] For the sake of completeness of the topic, it is only appropriate to underline how the EU's anthropocentric approach to AI is the object of a certain degree of irony on the part of scholars who compare it to the much more aggressive development and diffusion strategies of China and the USA, to date the only players to contend for digital supremacy (Rida Nour, 2019).

[2] Reference here is to the *Data Governance Act*, which came into force on 23 June 2022, and which regulates the use and reuse of publicly sourced data to create European data spaces in strategic sectors, and to the *Data Act*, proposed by the Commission in February of same year, which regulates the use and reuse of data generated by the internet-connected components of consumer products (so called Internet of Things).

provided, picking up on variations in microfacial expressions of the interviewee, is the basis for the attribution of a QR code which indicates the degree of danger of the subject in question.

In other words, the QR code assigned by iBorderCtrl is intended to provide an indicator of the interviewee's willingness to enter the EU illegally and therefore constitutes the basis on which border guards may deny access to EU territory or subordinate it to detailed interviews with flesh-and-blood officials (Jona 2021).

Although iBorderCtrl has only been tested for a limited time period and in a few precise legal access points to the EU, it is not hard to understand how much its operation violates the Commission's own guidelines on AI, especially those relating to the prohibition of tools that attribute a social score to users when this risks having important consequences for their lives and indications relating to the limitations on the use of real-time remote biometric identification tools. Furthermore, scholars have demonstrated both the statistical unreliability of the results processed by iBorderCtrl in the transition from tests on a few people to its large-scale use and the underlying ambiguity of an AI system that is designed to solve the difficulties in identifying of potentially irregular migrants based solely on the association lying-guilt-facial expression, which the system for facial recognition of emotions is modelled on (Sánchez-Monadero Dencik 2022).

Questions have been addressed to the Commission by (a few) MEPs about iBorderCtrl. However, in my opinion, this is only the tip of the iceberg. The real issue is that of the use that is (or could be) made of the large amount of biometric data that eu-LISA accumulates. As far back as 2016, Leese spoke in this regard of a European system of bio-politics in the Foucauldian sense of the expression, i.e. assuming that the rule of free movement in the EU is the value to be protected, the great mass of data would become the security sieve through which to separate good migrants from bad in an incessant midway between security and freedom that would become the criterion for policies of greater or lesser openness (Leese 2016). More recently, L. Chouliaraki and M. Georgiou explicitly defined the European area as a «biopolitical regime of border» (Chouliaraki Georgiou 2022: 9), i.e. a regime which, starting from data on single bodies, single identities and single emotions aims not only to select who can enter and who cannot but also to produce knowledge on who might become dangerous, once admitted. This process, rooted in an essentially security-based approach to migration, intersects with narrative practices by online and mainstream media which blend narratives on migrants as fragile victims with those on migrants as criminals, denying their individuality and willingness/ability to integrate and consequently contributing to generate feelings of confusion and threats towards migrants themselves in the public opinion. According to the researchers, all this contributes to making it appear as «natural and necessary practices of protection for Western citizens, territories, markets and cultures» (ibid.). That is to make it appear as natural protection practices which essentially take the form of measures of closure towards migrants, implemented through increasingly technological procedures and which, by virtue of their technical and impersonal nature, are hardly perceived by ordinary citizens in terms of their discriminatory value.

In *Surveiller et Punir*, Foucault analyzed Bentham's idea of a Panopticon in terms of a device which, through «a certain programmatic arrangement of bodies, surfaces, lights, gazes […] manufactures homogeneous effects of power»[3] (Foucault 1976: 220). Through the interoperability of its databases and the accumulation of personal and biometric data of anyone and for whatever reason requesting access to EU territory, the EU could achieve a level of control over all those who ask to enter its territory, on more or less regular ground, which is much broader and more subtle, i.e. to use the biometric data collected in its databases to feed AI systems that measure individual intentions to enter the EU illegally. Without even the need to create a particular architecture of the places where such control is exercised. All this in the indifferent acquiescence of citizens who are ever less aware (and perhaps ever less interested in knowing?) of what is happening at their borders.

5. An Italian popular adage goes that appetite comes while eating. In the case of eu-LISA, it is precisely its efficiency that leads to a multiplicity of cases in which the Commission deems it useful to use it, as the proposal on interoperability demonstrates. eu-LISA itself tends to put itself forward as an interlocutor in ever new areas of operation. In this sense, its strategic guidelines for 2018-22 contain a brief analysis of the context in which the agency conducts its collaboration and provides its support to EU and State institutions: «areas of border management, internal security and migration management have been going through a major transformation, moving from the physical to the virtual world and converging rapidly at the same time. They are more and more dependent not only on available physical resources, but on data and information too» (eu-LISA 2017:6). That is, the management of borders, migration and internal security of the EU requires the development of increasingly integrated and flexible IT networks at EU level to guarantee sophisticated tools for responding to concrete or even just statistically probable threats.

This, however, brings us to the issue of the political objective hidden behind technical cooperation, mentioned at the outset as one of the salient features of the European integration process. Indeed, eu-LISA seems to simply reiterate the strategy, launched by the Commission in its 2016 communication on EES and ETIAS as tools of the

[3] Author's translation.

new smart borders system. What is different, however, is the breadth of data available today and the greater sophistication of the algorithms through which they are processed.

The Commission itself, in its *Report on migration and asylum* of October 2022, reiterates how the active contribution of eu-LISA and the goal of interoperability among its databases are necessary for «improved means to control entry into the EU and to manage risks related to security, health or irregular migration» (European Commission 2022: 13). Legitimate objectives which, however, are focused mainly on us and on our safety. In this sense, some scholars have pointed out that the main shareholders of eu-LISA are the Commission and the Member States and that this helps explain the mix of meeting the security needs of the latter and the values of transparency, efficiency and protection of privacy, which eu-LISA is required to comply with and be functional to (Bircan Korkmaz 2021: 3). Others point out, however, that the development of eu-LISA has brought to the fore a group of IT experts/technicians/engineers who, with the silent support of the major contractors of eu-LISA's services, aim to expand their influence on and within European institutions (Jeandesboz 2021; Bigo 2020).

What I personally find disturbing is that, through eu-LISA, the EU is endowing itself with the tools to take new and substantial steps in the direction of closing its borders to migrants. Already for those who request legal access to the EU territory, the steps to be taken in practice multiply and become increasingly complex, especially as regards the possibility of appealing against adverse decisions.

For those who arrive at our borders driven by war or hunger or persecution of various kinds or simply by the prospect of a better life, the systems managed by eu-LISA can become an insurmountable obstacle. Consider the so-called migrant crisis of 2013-2015. If IT tools had been used to assess the reliability of the documents and answers provided by individuals in support of protection applications, documents and answers that were provided after long and tormented journeys, after further long queues for the collection of biometric fingerprints and the filing of protection applications, after the stay in hotspots which in fact were and still are overcrowded detention camps, the rejection threshold would have been decidedly higher than it was. In this case, the only hope against adverse decisions would have been the presence of NGO activists to indicate possible ways of appeal. A presence that is rarely guaranteed within the hotspots and even less so in the numerous grey areas that are being created at EU borders.

Let us try to imagine what might happen when the entry screening procedure, envisaged by the September 2020 *New Pact on Migration and Asylum* comes into force. This foresees that upon arrival at EU border, migrants are subjected to interviews which aim to divide them into three large groups: those who are immediately repatriated, those whose application for protection is subject to an accelerated examination because they come from countries with low acceptance rates or because theirs are manifestly unfounded applications, those whose applications must be evaluated and who are allowed access to restricted and well-identified areas of the Union with a ban on leaving them (European Commission 2020). Let us imagine that a system such as iBorderCtrl is used, powered and educated through the data that runs in the eu-LISA networks. What would be the reliability of the results of resorting to such an instrument on individuals in a state of enormous psychological stress, when already in relatively normal conditions the results are not always reliable? How many cases of genuine *refoulement* at the border would there be, a practice that is prohibited by the international conventions on refugees that all EU Member States have signed?

I thus believe there to be two major problems. On the one hand, eu-LISA consciously contributes to the dematerialization of migrants, who from depersonalized subjects à la Fanon, i.e. defined through stereotypical categories developed by the host countries which facilitate their refoulement (Fanon 2015), increasingly become alphanumeric codes among many, faceless and without individual stories, for those who have no face and no history can be rejected without arousing any pity. On the other hand, eu-LISA allows for major technological developments which, due to their extremely technical nature, are not however the subject of discussion and scrutiny in European public opinion. In its strategic guidelines for 2021-27, we read that «the Agency will have to stay focused on its core operations (i.e. the development of new systems, operational management and development of the systems entrusted to it) […] it will have to continue to increase its contribution to Member States and the EU as a whole, capitalizing on its knowledge, experience and capabilities in the area of management of large scale IT-systems and services» (eu-LISA 2022:7).

This means helping to increase the quantity, quality and interoperability of personal and biometric data that eu-LISA is able to store, manage and make usable. And an enormous mass of constantly growing data in itself represents an invitation to make use of it for the most diverse purposes, not excluding the development of systems that exploit biometric data, which eu-LISA manages, to measure the will of anyone arrives at the EU border to stay there illegally. This is where space opens up for creating systems like iBorderCtrl and using them. This is where the technical nature of eu-LISA can become the tool for (indiscriminate?) *refoulement* practices at EU borders. We are not a "technological fortress" and eu-LISA is not the first building block but it is certainly the crucible in which this might be forged.

Bibliography

Aden, H. (2020). Interoperability Between EU Policing and Migration Databases: Risks for Privacy. European Public Law, 26:1, 93–108.

Bigo, D. (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? International Journal of Migration and Border Studies, 6:1/2, 74-92

Bircan, T. & Korkmaz, E.E. (2021). Big data for whose sake? Governing migration through artificial intelligence. Humanities and Social Science Communication [Online] Available: https://doi.org/10.1057/s41599-021-00910-x (January 18, 2023)

Börzel, T. A. (2016). From EU Governance of Crisis to Crisis of EU Governance: Regulatory Failure, Redistributive Conflict and Eurosceptics Publics. Journal of Common Market Studies, 54 annual review, 8-31

Brack, N., Gurkan, S. (eds.). (2020). Theorising the Crises of the European Union. London: Routledge

Chouraliaki, L. & Georgiou, M. (2022). The Digital Border. Migration, Technology, Power. New York: New York university Press

European Commission. (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, COM(2018)237 final, Bruxelles, 25.4.2018

European Commission. (2019). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence, COM(2019)168 final, Bruxelles, 8.4.2019

European Commission. (2020). White Paper On Artificial Intelligence. A European approach to excellence and trust, COM(2020) 65 final, Bruxelles, 19.2.2020

European Commission. (2020). Proposal for a regulation of the European Parliament and of the Council introducing a screening of third country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817, COM(2020) 612 final, Brussels, 23.9.2020

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, Bruxelles, 21.4.2021

European Commission. (2021). Annexes to the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final, Bruxelles, 21.4.2021

European Commission. (2022). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Report on Migration and Asylum, COM(2022) 740 final, Brussels, 6.10.2022

eu-LISA. (2017). Strategy 2018-2022 [Online] Available https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Strategy%202018-2022.pdf (December 5, 2022)

eu-LISA.(2022). eu-LISA Strategy 2021-2027 [Online] Avalable https://www.eulisa.europa.eu/Publications/Corporate/eu-LISA%20Strategy%202021-2027.pdf (December 5, 2022)

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics, P8_TA(2017)0051 [Online] Available https://europarl.europa.eu (November 12, 2022)

European Union Agency for Fundamental Rights. (2020). Getting the Future Right. Artificial Intelligence and Fundamental Rights, Luxembourg: POEU

Fanon, F. (2015). Pelle nera, maschere bianche. Pisa: ETS (ed.or. Peau noire, masques blanches, 1952, Seuil. Paris)

Foucault, M. (1976). Sorvegliare e punire. Torino: Einaudi

Glouftsios, G. (2021). Engineered Digitised Borders. Designing and Managing the Visa Information System. Singapore: Palgrave Macmillan

Glouftsios, G. (2021). Governing border security infrastructures: Maintaining large scale information systems. Security Dialogue, 52:5, 452–470

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

Jeandesboz, J. (2021). European Union information system for border and migration enforcement: trajectories, programmatics and uses. G. Udson, I. Atak (eds.), Migration, Security and Resistance. Global and Local perspectives (pp. 47-65). London: Routledge

Jona, L. (2021). La "macchina della verità" alle frontiere di cui l'Europa preferiva non parlare [Online] Available https://www.wired.it/attualita/tech/2021/04/27/iborderctrl-europa-frontiere-sorveglianza/ (December 10, 2022)

Kamkhaji, J.C. & Radaelli, C.M. (2017). Crisis, Learning And Policy Change In The European Union. Journal of European Public Policy, 24:5, 714-734

Leese, M. (2020). Fixing State Vision: Interoperability, Biometrics and Identity Management in the EU. Geopolitics, 27:1, 113-133

Leese, M. (2016). Exploring the Security/Facilitation Nexus: Foucault at the “Smart” Border. Global Society, 30:3, 412-429

Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. GUUE L 286, 1.11.2011, 1-17

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011. GUUE L 295, 21.11.2018, 99-131

Rida Nour, M. (2019). Geopolitique de l’intelligence artificielle: Les enjeux de la rivalité sino-americaine. Paix et Sécurité internationale, 07, 231-259

Sánchez-Monedero, J. & Dencik, L. (2022). The politics of deceptive borders: ‘biomarkers of deceit’ and the case of iBorderCtrl. Information, Communication & Society, 25:3, 413-430

Keywords: European Union – Artificial Intelligence – data – migrants – depersonalization