A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage

Rocco Bellanova & Denis Duez*

Most of the academic research on the developments of EU Justice and Home Affairs (EU JHA) tends to overlook the role played by technologies in their relations with classical 'human' and institutional actors. This is particularly problematic because in official discourses, technologies are requested, designed, and built as cornerstones of European security and its external dimension. Still, apart from 'technicalities', their use and design are generally assumed as politics-free. On the contrary, this contribution brings technologies to the forefront of the research and reframes them in terms of socio-technical assemblages. From this perspective, it analyses the role of the 2011 EU Passenger Name Record project in the making of European security and its external dimension. The lesson learned is that human institutions are neither the only players nor the passive victims of technological determinisms. Rather, focusing on a socio-technical assemblage means to inquire the effective participation of different actors and thus critically discuss the making of European security in terms of politics.

1 THE EU JUSTICE AND HOME AFFAIRS AND ITS EXTERNAL DIMENSION: A 'DENSE SOCIO-TECHNICAL ENVIRONMENT'?

Even a superficial overview of the main documentation related to EU Justice and Home Affairs (EU JHA) uncovers a panorama densely populated by different kinds of technologies, ranging from large databases collecting millions of personal data to devices for videoconferences. In the Stockholm Programme, entire chapters focus on how technologies shape contemporary and global societies, how they create new cyberspaces where the European citizens deserve to be protected, how the

* Rocco Bellanova, Assistant and researcher of the *Centre de Recherche en Science Politique* at the *Facultés universitaires Saint-Louis* (Brussels, Belgium) and researcher of the Law, Science, Technology and Society at the *Vrije Universiteit Brussel*. Denis Duez, Lecturer in political science and European politics at the Institute for European Studies of the *Facultés universitaires Saint Louis*. The authors thank Xiana Barros Garcia, Katja de Vries, Daniel López Gómez and Raphaël Gellert for their comments and advice on earlier versions of the article. Helena Carrapiço and Florian Trauner deserve a special mention, both for organizing two productive workshops in Vienna and for carefully (and patiently) supporting the authors in the drafting of the article. The authors would also thank the Institut für europäische Integrationsforschung of the Österreichische Akademie der Wissenschaften for providing economic support to the participants of the workshops, as well as the ARC project on the 'Europeanisation du droit, des politiques publiques et des normes sociales' of the Facultés universitaires Saint-Louis. Obviously, all errors and omissions are the sole responsibility of the authors.

Bellanova, Rocco & Duez, Denis. 'A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-Technical Assemblage'. *European Foreign Affairs Review* 17, Special Issue (2012): 109–124.
© 2012 Kluwer Law International BV, The Netherlands

tools at the disposal of EU-related actors should be 'updated', and how 'necessary technological tools' should be mobilized.[1] In the EU Internal Security Strategy, technologies are further proliferating.[2] As in the Stockholm Programme, they are both defining and threatening society: while they are 'opening up' borders and societies, they are also exploited by criminals, terrorists, and traffickers. In the guidelines for action, the quasi-omnipresence of technologies becomes impressive: adoption of a 'proactive, intelligence-led approach' based on information processing; development of a comprehensive model for information exchange; integrated border management, and so forth.

The above overview already brings up three important remarks concerning the role of technologies in the JHA external dimension. First, their range and their use create and enhance spaces that cross and redefine EU external borders (databases, cyberspaces, 'global societies'), and they potentially provide a resource to ensure an adequate control over new and old borders. Second, the same representations of technologies, and their actual and foreseen uses, participate to the 'logics of expansion and diversification' of the JHA external dimension presented by Trauner and Carrapiço in the Editorial of this issue, in terms of policies, geography, and actors. Finally, the role of technologies tends to be controversial not only because it is not fully mastered by institutional actors but also due to the implicit challenges foreseen in their full deployment in terms of resources and respect for fundamental rights (as demonstrated by the emphasis on the need to safeguard privacy and data protection).

Therefore, it seems legitimate to qualify the EU JHA and its external dimension not only as a 'dense institutional environment'[3] but also as a 'dense socio-technical environment'. If this is the case, how do socio-technical assemblages contribute to the 'making' of European security and its external dimension? And what can we learn in accounting for technologies in terms that go beyond common approaches?

The following three sections address these questions in reverse order. First, we present the main framing of technologies in International Relations and European Studies dealing with the construction of the EU JHA and its external dimension. We propose to adopt a different set of concepts and assumptions, drawing from the toolbox of Actor-Network Theory. We then apply them to a specific case study: the EU proposed Passenger Name Record (PNR) setting, which is the core

---

1 Council of the EU, The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens (Brussels: Council of the EU, 2010).

2 Council of the EU, Draft Internal Security Strategy for the European Union: 'Towards a European Security Model' (Brussels: Council of the EU, 2010).

3 S. Wolff et al., 'The External Dimension of Justice and Home Affairs: A Different Security Agenda for the EU?', *Journal of European Integration* 31, no. 1 (2009): 17.

section of the article. Finally, on the basis of this analysis, we sketch an alternative picture of the making of European security. Such an effort does not claim to fully substitute all the work framed in different theoretical approaches but aims at proposing a more 'technologically aware' view on the deployment of the EU JHA external dimension.

2 FRAMING AND REFRAMING TECHNOLOGIES

2.1 Accounting for technologies

Questions concerning the relations between EU JHA and technology appear far from the *foci* and concerns of most grounded European Studies and International Relations. However, as said above, it is important to note that the deployment of many technologies, and even their mere proposition, has sparked several harsh debates at societal, political, and inter-institutional levels. Among the most discussed cases are the retention of telecommunications data, the transatlantic transmission and processing of financial information (the so-called SWIFT affair) and travellers' data (the so-called PNR case described below), as well as the case of the deployment of body scanners.[4] Still, most of the classic approaches in political sciences have overlooked technologies, or quickly relegated their role to the domain of 'technicalities', far behind the human institutions and the purely social relations among them. With reference to two of the cases presented above, the decision over the transmission of financial and passengers' data becomes mainly a question of consolidation of new institutional powers or of norms exportations.[5] There, technologies rest on a purely ancillary or intermediary position in front of human institutions, external to the 'real' world of institutional relations, policymaking, and politics. When they are part of a 'dossier', they do not imply any specific feature; the dependent variables lie always elsewhere.

While 'hegemonic' in research terms, these approaches to technologies are increasingly challenged by more critical approaches such as Critical Security Studies and International Political Sociology. Indeed, their focus on 'daily practices' of security professionals (as discussed in the Editorial by Trauner and Carrapiço) has increasingly attracted the attention of several researchers towards topics where technologies have a prominent role, such as 'smart border controls'

---

4 On Society for Worldwide Interbank Financial Telecommunication (SWIFT) and body scanners, see relevant articles in this issue.

5 Concerning financial data, see J. Monar, 'The Rejection of the EU-US Swift Interim Agreement by the European Parliament: A Historic Vote and Its Implications', *European Foreign Affairs Review* 15, no. 2 (2010): 143–151. On passengers' data, see J. Argomaniz, 'When the EU Is the "Norm-Taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms', *Journal of European Integration* 31, no. 1 (2009): 119–136.

axed on the use of biometrics,[6] or where new technologies modify previous practices, as in the case of the creation of databases for asylum seekers or visa applicants.[7] This interest in technologies has been further reinforced by a certain convergence with Surveillance Studies and by insight of public policy research and legal analysis.[8] However, even in these cases, the relation between technologies and human institutions remains strongly centred on the latter: technologies are framed as policy tools, mainly dangerous for individuals, either enabling rationalities of subjugation or depoliticizing the European polity.[9]

2.2 Accounting for socio-technical assemblages

While the aforementioned critical theoretical approaches are driving technologies back to the forefront of the academic analysis, most of this newly acquired presence remains more 'symbolic' than 'material'. Technology's 'stuff', its specificities, its 'physical' functioning, and its everyday interaction with other actors are still eluded in most of the accounts.[10] Following the examples of other researchers, this lack of proper 'representation' of technologies in the critical approaches can be partially corrected by drawing insight from the Actor-Network-Theory approach.[11]

Therefore, three assumptions permit to reframe the relation between technologies and human institutions. The first posits all elements, both human and non-human, as 'actants', an actant being '[w]hatever acts or shifts actions'.[12] This

---

6 B.J. Muller, *Security, Risk and the Biometric State: Governing Borders and Bodies* (London/New York: Routledge, 2010).

7 D. Bigo & E. Guild (eds), *Controlling Frontiers: Free Movement into and within Europe* (Aldershot: Ashgate, 2005).

8 For the integration of securitization theory and public policy analysis, see T. Balzacq, 'The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies', *Journal of Common Market Studies* 46, no. 1 (2008): 75–100. For an example of collaboration between Surveillance Studies and International Relations critical postures, see M.B. Salter, *Politics at the Airport* (Minneapolis: University of Minnesota Press, 2008). For a law approach, see V. Mitsilegas, 'Contrôle Des Étrangers, Des Passagers, Des Citoyens: Surveillance et Antiterrorism', *Cultures & Conflits* 58 (2005): 155–182.

9 Balzacq, 2008, *supra* n. 8.

10 In this sense, we feel close to the remarks on the yet poor understanding of the 'stuff' of politics advanced by B. Braun & S.J. Whatmore, 'The Stuff of Politics: An Introduction', in *Political Matter: Technoscience, Democracy, and Public Life*, ed. B. Braun & S.J. Whatmore (Minneapolis: University of Minnesota Press, 2010), ix–xl.

11 See W. Walters, 'The Power of Inscription: Beyond Social Construction and Deconstruction in European Integration Studies', *Millenium: Journal of International Studies* 31, no. 1 (2002): 83–108, as well as B. Prainsack & V. Toom, 'The Prüm Regime. Situated Dis/Empowerment in Transnational DNA Profile Exchange', *British Journal of Criminology* 50, no. 6 (2010): 117–135.

12 M. Akrich & B. Latour, 'A Summary of a Conventient Vocabulary for Semiotics of Human and Nonhuman Assemblies', in *Shaping Technology/Building Society: Studies in Sociotechnical Change*, ed. W.E. Bijker & J. Law (Cambridge: The Massachusetts Institute of Technology Press, 1992), 259.

definition is largely borrowed from Greimas' semiotics,[13] and it establishes a principle of symmetry in the study of the elements. While this grants a form of agency to all elements, it does not automatically imply intentionality: '*any thing* that does modify a state of affairs by making a difference is an actor – or, if it has no figuration yet, an actant . . . [t]his, of course, does not mean that these participants "determine" the action'.[14]

According to the second assumption, '[a] machine can no more be studied than a human, because what the analyst is faced with are assemblies of human and non-human actants where the competences and performances are distributed; the object of analysis is called a setting or a setup'.[15] Settings and set-ups are generally called socio-technical assemblages: heterogeneous systems composed of elements that are both material and immaterial, both physical and textual.[16]

The third assumption presupposes that between the elements of the setting, there are forms of mediation rather than intermediation: '[Mediators'] input is never a good predictor of their output; their specificity has to be taken into account every time. Mediators transform, translate, distort, and modify the meaning or the elements they are supposed to carry'.[17] This forces us to step back from the usual dichotomy 'subject/object', in which one element is mastering the other, because no element is assumed to carry an essential and transcendental meaning or function in itself.

Finally, it is important to note that, from a methodological point of view, following socio-technological assemblages generally implies a more inductive orientation rather than a more classical deductive approach. Indeed, the presumption is that descriptions can be powerful analytical tools.

In the following section, these assumptions are used to analyse the contribution of a specific socio-technical assemblage to the making of European security: the EU PNR system, a proposed '(policy) instrument' to prevent, detect, investigate, and prosecute terrorist offences and serious crime.[18] The choice of this prospective setting is particularly pertinent because it is presented as an advanced

---

13 See A.J. Greimas & J. Courtés, *Sémiotique: Dictionnaire Raisonné De La Théorie Du Langage* (Paris: Hachette, 1979), 3.

14 B. Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (New York: Oxford University Press, 2005), 71–72 (italics in original).

15 Akrich & Latour, 1992, *supra* n. 12, 259.

16 Hereinafter, 'socio-technical system', 'setting', and 'assemblage' are used synonymously.

17 Latour, 2005, *supra* n. 14, 39.

18 European Commission, Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, COM(2011) 32 Final (Brussels: European Commission, 2011) (hereinafter 'EU PNR Proposal').

technologically mediated practice to fight against (mostly) external threats by monitoring international commercial travels.[19]

3 THE PASSENGER NAME RECORD SETTING(S)

Before attempting any description of the EU PNR setting, two premises on the scope of the case study are due. First, there is no 'single' PNR setting, but several different ones, even if not all are actually fully implemented.[20] Second, historically PNR systems were merely conceived as a solution to smooth booking activities of air carriers facing an increasing volume of travellers. In this type of settings, travellers' data were designed as an essential element to provide a flight service (especially for large companies).[21] Only later the 'commercial' PNR system began to be increasingly used by non-commercial actors such as law enforcement agencies, especially in the United States, as part of their practices against organized crime.[22] Since then, other security-oriented settings have been adopted in Canada, Australia, the United Kingdom, and other countries.[23] Finally, in February 2011, the European Commission proposed, for the second time, the adoption of a PNR setting for the EU.[24] The following description is based solely on the 2011 project.

---

19 *Inter alia*, see Council of the EU, The Stockholm Programme: An Open and Secure Europe Serving and Protecting Citizens (Brussels: Council of the EU, 2010), 39, and Council of the EU, Draft Internal Security Strategy for the European Union: 'Towards a European Security Model' (Brussels: Council of the EU, 2010), 5 and 17.

20 While a comprehensive list of Passenger Name Record (PNR) systems already proposed or implemented is not publicly available, the Commission generally refers to the United States of America, Canada, Australia, South Korea, United Kingdom, Denmark, France, Belgium, Sweden, and the Netherlands; see European Commission, The 2011 Commission Impact Assessment Accompanying the EU PNR Proposal, SEC(2011) 132 (2 Feb. 2011) (hereinafter 'EU PNR Impact Assessment'), 14.

21 A prominent private company in the field defines PNR as 'the complete set of booking data captured by airlines or their representatives – travel agents, GDSs, etc. A PNR contains the travel record of a passenger or a group of passengers travelling together', SITA, 'iBorders API – PNR: Get Pre-arrival Passenger Progiling and Risk Assessment', <www.sita.aero/product/iborder-–-iapi>, 30 Mar. 2011.

22 The current comprehensive and automated processing of PNR by the US Department of Homeland Security has its legal basis in the Aviation and Transportation Security Act of November 2001. Since then, three agreements had to be negotiated with the EU to ensure that the processing of data was not conflicting with the European data protection system; see V. Papakonstantinou & P. De Hert, 'The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic', *Common Market Law Review* 46, no. 3 (2009): 885–919. A fourth agreement has been negotiated after the entry into force of the Lisbon Treaty.

23 In particular, the EU has signed PNR agreements with Canada (2005) and Australia (2008). As in the case of the 2007 EU-US PNR Agreement, these two agreements are undergoing a process of renegotiation under post-Lisbon rules.

24 The first Commission proposal for an EU-wide PNR system was European Commission, Doc. COM(2007) 654 Final of 6 Nov. 2007.

3.1 The EU PNR setting workflow

A possible description of the EU PNR setting workflow is the following:[25] an individual organizes an EU-bound travel, a trip that implies both an EU and non-EU airport. At the moment of the tickets purchase, a series of data are generated, ranging from the dates of the flight to the credit card number of the prospective traveller. The ensemble of these data are commonly called Passenger Name Record, and they are collected, stored, and processed for economic and services purposes in one or more databases (either those of the air carrier or those of the bigger computer reservation systems). Then, 24 and 48 hours before departure, and again after the boarding procedures are finalized, the data are 'pushed' to the relevant Passenger Information Unit (PIU), a specific agency in each EU Member State that collects, stores, and processes up to nineteen fields of the data generated at the moment of the acquisition. There, at least three immediate actions take place: data are stored in a database, data are automatically matched against other relevant databases or specific queries, data are run against predetermined criteria. In the event that one of the last two operations brings about a 'positive' result or match, the automatic processing is double checked 'manually' by a human being. If the result continues to be 'positive', the data are sent to a different authority (or to another PIU) that will act upon the individual linked to, or identified by, the data. If 'false positives' occur, they are reported back to further tune the construction of assessment criteria. Also, a second set of operations may take place. On the one hand, PNR data are processed again to update or create new assessment criteria against which future PNR data will be run. On the other hand, if a formal investigation is launched, specific PNR data can be requested and processed again to track the past movement of selected individuals and their possible connections to other people.

3.2 The main elements

A description of the potential functioning of the EU PNR setting immediately highlights the complexity assemblage. Indeed, the core elements of the PNR assemblage are multiple and protean. A non-exhaustive list of elements would include:[26]

---

[25] The description is based on the text of the EU PNR Proposal, in particular on Arts 3–9, and on the EU PNR Impact Assessment.

[26] This list is based on the text of the EU PNR Proposal, the EU PNR Impact Assessment, the opinions of the European Data Protection Supervisor (EDPS) (Doc. 52011XX0622(02) of 25 Mar. 2011), Art. 29 Working Party (WP) (Doc. 00664/11/EN WP181 of 5 Apr. 2011), and the EU Agency for

- *human actants and institutions:* air carriers, regional and international organizations representing air carriers, travellers, Member States' PIUs, national relevant law enforcement agencies, the European Commission and its DG Home Affairs, the European Data Protection Supervisor, Article 29 Working Party, the EU Agency for Fundamental Rights, the European Parliament and its LIBE Committee, the Council and its DG H, and so forth.
- *non-human actants and systems:* PNR data, registration systems, standards for encryption and transmission of data, a communication system between air carriers or other registration systems and Member States' PIUs, other 'relevant' (but still unnamed) databases in the EU and Member States, a system of automatic comparison between the PNR data collected and the databases, another system of automatic comparison between the collected PNR data and the predefined criteria for the goal of assessing risk, a third system contributing to the construction of meaningful criteria operating on PNR data, and so forth.

Several other key elements are relevant for the design and deployment of the setting: definitions of 'threat' and of 'insecurities'; national and European regulations and laws concerning, that is, privacy, data protection, serious crime, and terrorism; and even the entry into force of the Lisbon Treaty, which implied the reframing of the previous Commission proposal into a new legal instrument and thus modified the formal relations among EU institutions on this 'dossier'. The presence of this last set of elements, which do not sit comfortably in a dyad human/non-human, underlines the intrinsic heterogeneity of the elements and of the articulations within and outside the setting. Many of the human elements are continuously translated, and inscribed, into non-human elements such as data, which are 'read' by both machines and other humans. Conversely, without enrolling a large number of human elements, the core functions of the assemblage would not 'run', the processing systems would not be fed, no comparison or correlation would be possible. The goal of the EU PNR system is apparently human centred, especially when compared to the goal of body scanners that are supposed to detect non-human elements such as bombs. However, human and non-human elements cannot be disjointed without betraying the claimed goal. Likewise, the assemblage would possibly not work without the continuous action of translation of all the actants – inscription, composition, and folding.

3.3 Controversies

Even if still at the stage of project, the EU PNR setting is already traversed by several controversies. Following the 'workflow' of the system, a tentative list of

Fundamental Rights (FRA) (Opinion 1/2011 of 14 Jun. 2011). The participation of 'classical institutional actors' is deduced from standard procedures for the attribution of 'dossiers' within the European institutions.

critical issues can be drafted.[27] They can be roughly divided into two main sets, whose elements strongly interact and overlap among them:

- *controversies concerning the collection of data:* they mostly concern the scope of the collection exercise – how many passengers should be 'inscripted' (Is it a generalized collection of personal data of 'innocent people' or only ad hoc collection in case of reasonable suspicion?), how much data should be translated for each passenger (What are the most relevant data fields, and how intrusive can the measure become?), what is the geographical scope of the setting (Is it all flights, including intra-EU, or only those between EU and non-EU airports? Or is it 'international flights' *plus* specific intra-EU routes?). This set of controversies includes also the debates on the system of communication of PNR data between air carriers and PIUs and the adequate level of encryption of the transmitted data. Many of these controversies also engender questions on the economic impact of the measure as such and of specific design solutions;
- *controversies concerning the 'processing of data':* they revolve around the nature of PIUs, their competences, their limitations, and supervision. They also include the 'onward' transmission of PNR data to other PIUs, Member States agencies, and third countries actors. Particularly important are those concerning the processing operations of PIUs, the storage of data (retention period, masking, and retrieval of data), the creation and update of assessment criteria, and the matching with unnamed databases.

This list does not intend to be exhaustive and, given the limits of space and scope of this article, it is not possible to present here the different positions taken by the main actants on all controversies. The goal of this list is rather to further unpack the EU PNR setting beyond the usual terms of social or institutional relations. These controversies are not mere technicalities, which can be systematically solved by a neutral 'technological fix' or by a 'legal trick'. All of them create possible bifurcations in the deployment of the setting, and in some cases they question its deployment *tout-court*. As described below, their resolution implies different degrees of participation, and different configurations, of the elements presented above.

---

[27] The list of controversies is based on EDPS, Art. 29 WP, and FRA, *supra* n. 26; on the EU PNR Impact Assessment; and on available documents of Council's debates and position papers of private companies: see, that is, Council, Doc. 9103/11 of 15 Apr. 2011; UK delegation, Doc. 6359/1 of 10 Feb. 2011; German delegation, Doc. 8118/11 of 25 Mar. 2011; SITA, 2011, *supra* n. 21; ERA, ERA (European Regions Airline Association) Response to European Commission Impact Assessment Questionnaire on a Common EU Approach to the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes (Woking: European Regions Airline Association, 2007).

3.4 *Two specific sets of operations*

Two sets of operations could provide already enough material to unfold specific associations among actants and to offer insight on the making of the assemblage.

The first set concerns the transmission of PNR data to PIUs. Apparently, this is a straightforward operation providing already collected data to one or more government agencies. However, this action could not be performed without the articulation and translation of specific actants. Indeed, PNR data are generally encrypted in different communication standards at the moment of the 'commercial' collection, and they are stored in different databases under the 'supervision' either of air carriers or large control reservation systems. Therefore, specific communication channels should be established between the relevant 'commercial' repositories and the PIUs, with the threefold necessity of avoiding excessive economic burden for air carriers, speeding up the transmission, and streamlining the standards to increase readability of PNR data by the PIUs. In the preparation phase of the EU PNR proposal, the issue of the initial transmission was deemed so complex that at least three models were analysed: a direct transmission from each air carrier (or control reservation system) to the relevant PIU(s), a transmission of PNR data from air carriers and the like to a central database to which PIUs would be granted direct access, or a hybrid model with a private company acting as a broker, which receives all PNR data and redistributes them to relevant PIUs.[28]

This set of operations is particularly important because it operates a fundamental distinction between the 'commercial' and the 'security' settings, partially kicking off the latter. At the same time, it does not only require the active participation of the private sector but it also implies negotiations with economic models and rationalities rather than merely imposing a securitizing imperative.[29] Therefore, analysing this set of operations highlights the relevance of the private sector in the making of the setting not only as a provider of 'techniques' such as profiling or link analysis but also as a constitutive and essential element of the

[28] Finally, only the centralized and the decentralized options were discussed in the EU PNR Impact Assessment. However, the hybrid model was presented as an option in the questionnaires of a study conducted by private firms on behalf of the EC Directorate General for Justice, Freedom & Security (DGJLS); see ERA, ERA Response to EC DGJLS Consultants' Questionnaire on EU Network for PNR Data (Woking: European Regions Airline Association, 2008).

[29] For example, the Association of European Airlines (AEA) does not only require the full coverage of new costs by public authorities but also advances the request to be 'closely involved and consulted to ensure that security needs are fully addressed and the efficiency of the air transport industry is improved by facilitating the journeys of bona fide travellers', Association of European Airlines (AEA), AEA Position Paper on Transfer of Airline Passenger Data (PNR) to Governments (Brussels: AEA, 2011).

socio-technical assemblage.[30] Thus, it obliges the analyst to take into consideration the processes of material and non-material negotiations between different rationalities instead of over-emphasizing the 'predator' capacities of 'securitization discourses'.[31]

The second set of operations is, to some extent, the very core of the PNR setting or, in the words of the Commission, its real added value.[32] Indeed, it concerns the processing of PNR data operated by PIUs. According to the proposal, three specific operations take place at that level:

(1) a 're-active' tracking of the connections among specific individuals and their travelling history and behaviour in order to solve already committed crimes (to obtain further evidence or establish connections with other individuals);
(2) a 'real-time' processing of PNR data for monitoring purposes of known suspects (criminals or terrorists), mainly consisting in the running of PNR data against existing databases (or watch lists) and specific information sent to PIUs, a match allowing for the identification of the *mala fide* traveller and the possibility to act at a distance to submit him/her to secondary screening;
(3) a 'pre-emptive' use of PNR data to unveil unknown suspects by running the data of all travellers against pre-established assessment criteria (a correlation operation).[33]

All these uses imply an action upon the collected data: PNR data are 'activated' by different data processing systems, and in that way they should permit to unveil known and unknown identities, intentions, behaviours, and patterns. Indeed, both the 'discovery process' and the 'knowledge generation processes' would not be possible without the active participation of PNR data, either as the output of a specific inscription process or as the 'fermenting agent' that permits to highlight still unknown connections. These descriptions offer a possible understanding of what PNR, *stricto sensu*, make. They 'translate' individuals into knowledge,[34] but they do so in different manners (different data protocols) that should be disciplined into common standards, without which it is too difficult to act upon them (as discussed in the analysis of the previous set of operations). Again, here occurs a

---

30 On the import of economic models and techniques from the 'economic world' into the 'war on terror', see L. Amoore, 'Algorithmic War: Everyday Geographies of the War on Terror', *Antipode* 41, no. 1 (2009): 49–69.

31 In most of the documentation quoted above, the relation between costs and design of the system recurs as one of the key issues at stake.

32 See the Explanatory Memorandum preceding the text of the EU PNR Proposal.

33 See Art. 4 EU PNR Proposal and EU PNR Impact Assessment, 9–13.

34 Walters, 2002, *supra* n. 11.

multiplication and translation of actants: a steady proliferation, fragmentation, and re-articulation of the 'electronic body' of travellers, both in synchronic and diachronic terms, ending up in both commercial and law enforcement databases for every travel, each time re-inscripted, with 'marginal' modifications.[35]

The active role of the PNR data is particularly evident in the fourth use of these data operated by PIUs. Indeed, according to the proposal, their further stocking for a period of five years after the initial retention permits the use of PNR data for the construction of new assessment criteria or for their update.[36] There, PNR data are not only the yeast of existing databases or profiles but also strong contributors to the generation of a 'knowledge' that is largely disconnected from the individual firstly inscripted by the setting. At this point, the first chain of relations – traveller→PNR data→knowledge→action – is coupled with a second, in which the processing system brackets the initial element, the travellers, to make the PNR data produce a knowledge linked to other future individuals, contributing to refine the modes of inscription and 'calculation' for subsequent travellers.

Finally, the description of this second set of operations highlights the relevance of the processing systems in the EU PNR setting. There, many actants are connected: passengers are translated into PNR data; databases and watch lists are searched; PIUs process, connect, store, and create data and information; assessment criteria embed definitions, analyses, and perceptions of the threats; profiling (or risk assessment) software operates measurement and detection of correlations.[37] Indeed, it is not surprising that these 'actions upon the actions' have attracted so many controversies and especially those concerning the relation among discrete elements: the retention period of PNR data in PIUs' databases (immediate erasure or stocking?), the nature of data processing (profiling, risk assessment, or link analysis?), the quality of 'masking' (full anonymization or enhanced encryption?), the sifting of sensitive data (full erasure of 'sensitive data' or mere non-processing?), the ability of 'data subjects' to access their data (direct or indirect access?), the role of data protection authorities in the auditing of PIUs' activities (internal audit or external audit?).

The unpacking of this set of operations and controversies offers a different perspective on the relations between 'mobility' and 'security', as well as between 'behaviour' and 'control'. On the one hand, mobility and security are not framed as conflictive per se. On the contrary, the socio-technical assemblage not only

---

35 On the 'proliferation' of electronic bodies or data doubles, see K.D. Haggerty & R.V. Ericson, 'The Surveillant Assemblage', *British Journal of Sociology* 51, no. 4 (2000): 605–622.

36 Article 9(2) EU PNR Proposal.

37 As an introduction to profiling, see S. Gutwirth & M. Hildebrandt, 'Some Caveats on Profiling', in *Data Protection in a Profiled World*, ed. S. Gutwirth et al. (Dordrecht: Springer, 2010), 31–41.

operates on mobilities but also continuously translates them into different streams of knowledge that aim at making sense of any possible tensions.[38] On the other hand, the EU PNR setting would work in a manner that does not constrain *ex-ante* behaviour but rather presupposes a certain 'freedom' in acting 'as a passenger' in order to obtain more valuable data and to 'kick-off' the rest of the setting. This does not mean that individuals are not controlled, but this 'control' is less focused on enforcing a set of prohibitions (as in the case of 'no-fly' lists) than on operating a *mise en discours*. In this case, the aim is to identify specific patterns and to facilitate their 'readability', to allocate limited resources in a supposedly high tailored manner.[39]

4 A DIFFERENT VIEW ON THE 'MAKING' OF EUROPEAN SECURITY

4.1 The powers of an EU PNR setting's description

Such a tentative description of the proposed EU PNR system as a socio-technical assemblage brings up some important considerations pushing further the logics of expansion and diversification discussed by Trauner and Carrapiço in their Editorial. Firstly, a very important number of heterogeneous actants participate in the making of European security. This number tends to grow in order to bypass interferences, to pursue the stated goal of the project, and to satisfy specific needs, as in the case of the initial transmission of PNR data. At the same time, accepting the principle of symmetry between human and non-human does not only increase the number of the latter category but also further highlights and clarifies the role of many human elements, and especially private companies (air carriers, computer reservation systems, data brokers).

Secondly, and particularly relevant for the JHA external dimension point of view, the controversies around the scope of the EU PNR setting highlight several possible spatial geographies, only apparently reproducing the most obvious external borders of the EU. On the one hand, even the data of EU citizens will be stocked in PIUs' databases and processed in the same way as those of non-EU citizens. On the other hand, a possible extension of the scope of data collection to intra-EU flights, or the selection of specific intra-EU routes, would create a

---

[38] Analysing the 'SWIFT affair', Amicelle comes to similar conclusions, underlining how the mobility of financial information allows for the deployment of practices of control and surveillance; see A. Amicelle, 'The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and "Swift Affair"', *Research Questions* 36 (2011): 19.

[39] Such an approach to 'control' is close to the one described by Foucault in his *dispositif de sécurité*, in M. Foucault, *Security, Territory, Population: Lectures at the Collège De France 1977–1978* (New York: Picador, 2007), 29–86.

geography that bypasses, once and for all, the internal/external dichotomy and mostly draws on other criteria: means of transportation, availability of data, identification of risky patterns.

Thirdly, it is possible to define, at least in this specific case, the process of construction of the EU JHA and its external dimension as a sort of 'symbiotic' process between differently oriented settings. When explaining the workflow of the setting, it becomes clear that an important part of the security-oriented setting relies on the pre-existing core articulations of another socio-technical assemblage, which is mainly economic oriented. Furthermore, when compared to other security settings (to be) operated in the field of aviation security as the body scanners, the PNR setting results rather invisible, mostly 'hidden' behind the reservation system. Then, the 'symbiotic' process tends to become 'parasitic' in its articulation to individuals: they are asked to just 'behave freely' as travellers but within an 'enhanced' setting, in which their behaviour, firstly inscribed commercially, can be then translated into a security-oriented form of knowledge through a series of unperceived articulations (from the point of view of the individuals).

4.2 A comparison with the relevant literature

These first considerations are already pretty far from those that emerge in the few non-juridical articles that were published on the (EU) PNR.[40] However, some further differences can be advanced when comparing the previous description to two relevant works in the field, coming from different 'schools'.

In the first case, when compared to a framing of the EU PNR setting as a 'securitizing policy tool',[41] the analysis in terms of socio-technical assemblage shows that 'securitization' is not the only discourse supporting and supported by actors and actants. Rather, it is often challenged by, and negotiated with, the rhetoric of economic benefit maximization, with a special focus on the costs of implementation for private companies and a justification of the measure as a more targeted use of police workforce. From the 'policy instruments' perspective, the system seems fully instrumental to securitization, a quite pure 'intermediary' of a transcendental rationality of (in)security, which already implies specific

[40] To some extent, we share some commonalities with the mode of analysis of juridical articles on (EU) PNR systems, in particular a strong attention for the specific features of the system; see E. De Busser, 'EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal?', *Utrecht Law Review* 6, no. 1 (2010): 86–100, and F. Boehm, 'EU PNR: European Flight Passengers under General Suspicion: The Envisaged European Model of Analyzing Flight Passenger Data', in *Computers, Privacy and Data Protection: An Element of Choice*, ed. S. Gutwirth et al. (Dordrecht: Springer, 2011), 171–189.

[41] Balzacq, 2008, *supra* n. 8.

consequences. From this point of view, the making of European security remains fully on the shoulder of human elements, with no explicit feedback from non-human ones.

In the second case, the 2007 proposed EU PNR project is used to describe the EU as a 'norm taker',[42] with a full framing of the prospective setting in terms of norms. Here, the distance with the previous description is even stronger not because norms have been fully discarded in our account but because they tend to obliterate all the other elements. From a neo-institutional perspective, there is no need to analyse neither the specific EU setting nor the challenging articulations needed to translate 'over the Atlantic' a supposedly identical system. Taking such a shortcut and assuming one system as the substantial copy of the other risks to fully overlook the main actual difference: the ongoing functioning of the US one and the 'chimera', non-implemented, status of the EU one. Furthermore, as discussed above, many elements of the EU PNR system are still to be selected and articulations are still to be decided and definitely folded. These are not mere technicalities, but it is where many controversies are deployed and where solutions are still discussed. The differences between the declination of the PNR setting in the EU-US case and the EU proposal could be marginal, but they have potentially impressive consequences 'on the ground' and on institution building. Thus, stating that in the case of the PNR the 'EU is a norm taker' does not fully describe either the PNR setting itself or the making of European security.

5 CONCLUSIONS

Thus, why is it so important to broaden our analysis to embrace even material elements rather than resting on ideas and social relations? And what does the 2011 EU PNR project mean for the EU as an international actor?

From a conceptual point of view, the main reason is that the EU PNR setting is not a mere technological instrument at the disposal of the EU in the external dimension or just a symbolic element. But, as shown in the preceding pages, its construction and the possible resolution of its related controversies directly affect the making of the EU and of its external dimension. The process of assembling bodies, institutions, materials, regulations, software, operates irrespective of a clear-cut division between human and non-human elements or between an internal and an external space of the EU. Rather, most of the operations aim to stabilize and make sense of these 'external elements' by incorporating them into a sort of 'black-box'. According to Callon and Latour, it is exactly such a capacity of black boxing 'modes of thoughts, habits, forces and objects' that transforms a

[42] Argomaniz, 2009, *supra* n. 5.

micro-actor into a macro-actor.[43] From this perspective, these processes enact the EU as an international, macro, actor, but one that is not essentialist or transcendental by nature, but made, substantiated, by the multiple actions and the folding of a heterogeneous group of actants.

Similarly, the EU PNR setting, even at the stage of a project, discloses a dynamic ontology of the external dimension. Hence, socio-technical assemblages and their controversies call for a different view of decision-making and policy analysis. As discussed above, the study of primary sources shows that even classical institutions already devote time and attention to 'mundane' controversies and technicalities. Indeed, even before a formal agreement on the EU PNR project is formally reached, too many different elements have still to be articulated, too many controversies have already emerged, too many foldings must be completed, too many detours are probably needed. Then, notions such as 'norms' taker', 'norms' provider', 'securitizing', or 'policy tools' risk to fall short not only in accounting for the panoply of actants at stake within every setting but even in questioning the action, the legitimacy, and the power of the most traditional actors. Surely, a policy instruments approach acknowledges the political and symbolical features of technologies,[44] but it still tends to take the black boxing of non-human elements for granted and thus overlook important sites of politics.

Indeed, if a system like the EU PNR is at the same time constituted by, and performative of, the JHA external dimension, then understanding how the sealing of all the elements of the black box is attempted (from a procedural and content point of view) has an important political function. It reopens important spaces for politics, in institutional and non-classical *fora* and in the very functioning of the systems. Thus, it contributes to re-actualizing the possibility of engaging within the projected assemblage to assess and discuss articulations and their potential effects, to slowing down the folding not for the fear of technologies but for the sake of a more aware relation with and through them.

---

43 '[A] difference in relative size is obtained when a micro-actor can, in addition to enlisting bodies, also enlists the greatest number of durable materials', but the necessary enrolment goes a 'little more' beyond 'relationships, alliances and friendships': it also implies the action of putting relations, 'modes of thoughts, habits, forces and objects' into black boxes; cf. M. Callon & B. Latour, 'Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So', in *Advances in Social Theory and Methodology: Toward an Integration of Micro- and Macro-Sociologies*, ed. K.D. Knorr-Cetina & A.V. Cicourel (Boston: Routledge & Kegan Paul, 1981), 284.

44 T. Balzacq, 'The Frontiers of Governance: Understanding the External Dimension of EU Justice and Home Affairs', in *The External Dimension of EU Justice and Home Affairs: Governance, Neighbours, Security*, ed. T. Balzacq (Gordonsville: Palgrave Macmillan, 2009), 15–21.