6. SECURITY OF THE INTERSTICE AND INTEROPERABLE DATA SHARING: A FIRST CUT

DEIRDRE CURTIN

Information exchange in the EU constitutes an essential part of various different policies. In many policy fields, information sharing is crucial for decision-making but this does not necessarily include the exchange of personal information. In certain fields, however, information exchange contains vast troves of personal data and therefore affects the rights of individuals. The Area of Freedom, Security and Justice (AFSJ), as it was renamed in the Amsterdam Treaty, has seen significant policy developments since the late 1990s.

There has arguably been no other example of a policy area making its way so quickly and comprehensively to the centre of the Treaties and to the top of the EU's policy-making agenda.[1] In areas related to law enforcement and judicial cooperation, such as the AFSJ, horizontal information sharing (including the exchange of personal data) has become an essential tool in the internal security policy of the EU.[2] It is also an essential tool of external security. This has helped the creation of a common administrative space and

[1] See J. Monar, "Justice and Home Affairs in a Wider Europe: The Dynamics of Inclusion and Exclusion", ESRC 'One Europe or Several?' Programme Working Paper 07/00, Economic and Social Research Council, Swindon, 2000 (http://www.mcrit.com/scenarios/visionsofeurope/documents/one%20Europe%20or%20Several/J%20Monar%20.pdf).

[2] F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonized Data Protection Principles for Information Exchange at EU-level*, Berlin and Heidelberg: Springer Verlag, 2012, p. 1.

effective policy implementation while avoiding the creation of a large, centralised EU government.[3]

Data sharing is the opposite of 'stove piping' and implies that existing data are shared among multiple users for efficiency reasons and the desire to achieve more effective decision-making. It is closely associated with intelligence reform in response to changing and often accentuated security threats or apparent failures of intelligence, regarding collection, sharing or analysis. Interoperability implies not only full availability but also inter-connections between different systems and actors. It refers to the ability of information systems to exchange (personal) data and to enable the sharing of information.[4]

The interoperability-based mechanisms of data exchange in the AFSJ share many of the traits of what is usually termed as Europe's composite administration. Composite administration is a concept that seeks to bring into balance "autonomy, mutual considerateness and the ability to undertake common action".[5]

The term is usually employed to describe the networked character of relations between the various regional, national and supranational levels of administration in the EU. Some versions of the concept of composite administration have convincingly demonstrated that Europe's multilevel administrative system is also increasingly connected to international levels

---

[3] D.-U. Galetta, H. Hofmann and J.-P. Schneider, "Information Exchange in the European Administrative Union: An Introduction", *European Public Law*, Vol. 20, No. 65, 2014, p. 68.

[4] European Commission, High-Level Expert Group on Information Systems and Interoperability, "First Meeting – 20 June 2016, Report", Brussels, 27 June 2016, p. 6 (http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=24078&no=1); European Commission, High-Level Expert Group on Information Systems and Interoperability, "Scoping Paper", Brussels, June 2016 (http://statewatch.org/news/2016/sep/eu-com-hleg-interoperability-info-systems-scoping-paper-6-16.pdf).

[5] E. Schmidt-Aßmann, "Einleitung: Der Europäische Verwaltungsverbund und die Rolle des Europäischen Verwaltungsrechts", in E. Schmidt-Aßmann and B. Schöndorf-Haubold (eds), *Der Europäische Verwaltungsverbund*, Heidelberg: Mohr Siebeck Verlag, 2005, p. 7.

of governance.[6] As the possibilities for transnational security mechanisms have expanded in recent decades, it is unsurprising that composite administration, in interoperable networks, has come to include also cooperation with third states.

The acceleration and intensification of databases at the EU level goes hand in glove with the concern to preserve the states' control over what occurs in their territories while maintaining a European space without internal borders. The EU's powers in security are exercised by a wide array of institutions and a growing number of agencies and administrative bodies. The Hague programme of 2004 placed greater emphasis on the exchange of information between EU agencies and the interoperability of databases,[7] particularly in the context of migration management.[8] Intelligence networks in the AFSJ result from the policy of interoperability. They are composed of quite different types of EU legal entities: independent EU agencies (Europol, Frontex), large police and immigration databases (Schengen and the Visa Information System, VIS). The various nodes are multi-level, multi-actor and can span both the public and private sectors. Ballaschk has helpfully distilled two different levels of networks: vertical (basically the EU agencies and bodies) and horizontal (Prüm Treaty and passenger name records) as well as the 'intermediate' information systems (eu-LISA, Schengen, VIS, Eurodac and Customs).[9]

The question of interoperability has been most sensitive regarding access to the VIS and Eurodac. Both databases were primarily designed as instruments of migration control. Law enforcement agencies at the national and EU levels have attempted to utilise migration control practices to abet counter-terrorism activities. In particular, there is evidence that systems for monitoring and gathering data on migrants have been harnessed as part of

---

[6] A. von Bogdandy and P. Dann, "International Composite Administration: Conceptualizing Multi-Level and Network Aspects in the Exercise of International Public Authority", *German Law Journal*, Vol. 9, 2008, pp. 2013, 2015.

[7] Boehm (2012), op. cit., p. 7.

[8] V. Mitsilegas, "The Borders Paradox: The Surveillance of Movement in a Union without Internal Frontiers", in H. Lindahl (ed.), *A Right to Inclusion and Exclusion? Normative Fault Lines of the EU's Area of Freedom, Security and Justice*, Oxford: Hart Publishing, 2009, p. 55.

[9] J. Ballaschk, "Interoperability of Intelligence Networks in the European Union: An analysis of the policy of Interoperability in the EU's Area of Freedom, Security and Justice and its compatibility with the right to data protection", PhD thesis, University of Copenhagen, 2015.

the EU's anti-terrorism strategy. Migration data was long declared essential for law enforcement and counterterrorism purposes and national security agencies were granted access to pre-existing databases as well as to a growing number of new databases and data collection schemes in this area.

6.1 Interoperable EU databases: Security of the interstice

The use of new information and communication technologies in the AFSJ in the form of *information systems* has spiralled in recent decades, as witnessed by the recent creation of a new EU agency specifically to manage these information systems: eu-LISA, the European agency for the operational management of large-scale IT systems in the AFSJ. In its own words, it "strives to support and facilitate European policies in the area of justice, security and freedom. It proactively supports and promotes effective cooperation and information exchange between relevant EU law enforcement bodies by ensuring the uninterrupted operation of large-scale IT systems".[10] These information systems vary greatly in their degree of complexity and formality. In the EU, a layered approach has been followed. New or enhanced EU bodies (or specific databases) intended to promote information sharing among the law enforcement and security agencies of its Member States (through Europol, Eurodac and Schengen) have seen their powers boosted considerably (for example, Europol and Eurojust). More recently, new agencies have been set up (the European Border and Coast Guard) or discussed (an EU intelligence agency).

The EU has actively attempted to facilitate and encourage information sharing among the Member States by developing the principle of availability.[11] According to this principle, information needed for law enforcement purposes by the authorities of one EU Member State should be made available by the authorities of another Member State, subject to certain conditions. The Hague programme of 2004 placed greater emphasis on the

---

[10] See the eu-LISA website, "Mandate and Activities" (http://www.eulisa.europa.eu/AboutUs/MandateAndActivities/Pages/default.asp).

[11] J.D. Occhipinti, "Availability by Stealth? EU Information-sharing in Transatlantic Perspective", in C. Kaunert and S. Léonard (eds), *European Security, Terrorism and Intelligence: Tackling New Security Challenges in Europe*, Basingstoke: Palgrave Macmillan, 2013, pp. 143, 144.

exchange of information between EU agencies and the interoperability of databases,[12] particularly in the context of migration management.[13]

Mitsilegas commented that the emphasis on enabling the flow of data between EU databases or EU agencies and bodies in order to enhance the exchange of personal data is often justified on the basis of the 'war on terror'.[14] As Ballaschk puts it, "[t]he history of the development of a supranational EU justice and home affairs policy is a history of institutional and political interoperability".[15] Interoperability is a more general and less passive term than availability that implies not only full availability but also interconnections between different systems and actors. It refers to the ability of information systems to exchange data and to enable the sharing of information.[16] It fits within an accentuated trend in recent years towards more institutional and organisational interoperability in law enforcement and intelligence in the EU and globally.

In a recent Commission Communication on "Stronger and Smarter Information Systems for Borders and Security", for example, the Commission highlighted the recent terrorist attacks in Paris and Brussels and the need to improve the interoperability of information systems as a long-term objective.[17] To achieve these objectives, the Commission set up a High-Level Expert Group on Information Systems and Interoperability, which has been given the task of assessing different options for achieving interoperability and of identifying any gaps and shortcomings of information systems at the European level.[18] The expert group recently published a report of its first meeting and the challenges that lie ahead, but no mention was made of the legal framework applicable to data protection

---

[12] See European Council, "The Hague Programme: Strengthening freedom, security and justice in the European Union", OJ C 53/1, 3.3.2005; see also Boehm (2012), op. cit., p. 7.

[13] Mitsilegas (2009), op. cit., p. 55.

[14] Ibid. p. 54.

[15] Ballaschk (2015), op. cit., pp. 38-39.

[16] European Commission, High-Level Expert Group on Information Systems and Interoperability, "Scoping Paper" (2016), op. cit.

[17] European Commission, "Stronger and Smarter Information Systems for Borders and Security", COM(2016) 205 final, Brussels, 6.4.2016, p. 2.

[18] Ibid., p. 15.

in information exchanges between EU agencies.[19] The expert group appears to be more centred on enhancing interoperability, further cooperation and the technical requirements.[20]

The Commission nonetheless emphasised the importance of the Charter of Fundamental Rights and in particular the new data-protection reform instruments in addressing current gaps and shortcomings in the EU as regards data management for border control and security. The Commission holds that the principles of the Charter and EU data protection legislation will "guide the Commission" and ensure that the "further development of information systems in these areas will be in line with the highest standards of data protection".[21] For now such words are mere pious aspirations that have no grounding in concrete data protection requirements nor in any readily comprehensible way for data subjects to challenge the exchange of their personal data and the use to which it is subsequently put.

6.2 In search of transparency and accountability: Pie in the sky?

The visible part of the EU pushes for "a strong Europe in a world of uncertainties".[22] One of the key challenges facing Europe is "to ensure the security of our citizens confronted with growing external and internal threats". In the EU, the 'dignified' institutions (the European Council, Council of the EU, European Parliament and national parliaments) will all have a visible role to play should a European defence union of sorts come to pass with military headquarters and joint defence forces.

Yet the focus of this chapter is on concealed security governance. In a policy area like the AFSJ, the need for a careful balance between EU-wide security interests and the demands of national sovereignty, might recommend not giving public opinion the impression that the EU is extensively involved in security matters. The area of security and law enforcement is where information gathering, mining and interoperable

---

[19] European Commission, High-Level Expert Group on Information Systems and Interoperability, "First Meeting – 20 June 2016, Report" (2016), op. cit.

[20] See for example the High-Level Expert Group on Information Systems and Interoperability, "Scoping Paper" (2016), op. cit.

[21] European Commission, COM(2016) 205 final (2016), op. cit., p. 5.

[22] This is the core joint ambition of the French and German foreign ministries for the post-Brexit EU, in a joint paper with this title by Jean-Marc Ayrault and Frank-Walter Steinmeier of September 2016.

sharing is very largely invisible but at the same time subject to accelerated and intensified cooperation. It makes use of vast networks of 'data cops' to do its 'efficient' work. The problem is, how do we make the invisible transparent? And how do we make informal, unseen and multijurisdictional arrangements accountable?

A network that straddles multiple organisations and jurisdictions gives rise to specific problems that are not the same as those for formal institutions. The boundaries of networks are inevitably amorphous with fluctuating membership and relationships, and they will generally not have their own formal powers or even necessarily formal routines. In one specific respect security networks are like an organisation: "its members are all members of organizations, and the behaviour of network members is conditioned by the patterns of behaviour common to their organizations".[23] Informal expectations are powerful within the network. In the words of Glennon, "members are thus counted on, for example, to exhibit loyalty to existing decisions, avoid publicly embarrassing other members of the network, and demonstrate fidelity to commonly shared values and assumptions".[24]

What can, if anything, be done to improve visibility and accountability? There are different layers to consider in thinking further about possible directions for improvements. One approach is to tone up the 'dignatarian' muscles, for example by deleting or amending the national security exception (Art. 4(1) TEU), or by narrowing the scope of or limiting formal secrecy requirements in security (adopting an EU secrets law as earlier proposed).[25] But such stopgap measures are unlikely to be widely adopted or fruitful even if they were more likely to happen in practice.

Another approach in thinking further about ways of challenging the lack of transparency and accountability is through the principle of legality and the rule of law. As Kaarlo Tuori points out, one of the normative problems of the EU's "security constitution" is that AFSJ provisions treat individuals as "passive recipients of collective security goods rather than active citizens or bearers of rights" who "enter the focus of security measures

---

[23] M.J. Glennon, *National Security and Double Government*, Oxford: Oxford University Press, 2015, pp. 86-87.

[24] Ibid., p. 87.

[25] For example, in my inaugural address at the University of Amsterdam in 2011: "Top Secret Europe" (Inaugural Lecture 415, University of Amsterdam, 2011).

primarily as security risks whose characteristics, propensities and actions must be surveyed and recorded". In this sense, Tuori concludes, the EU's security constitution treats individuals as objects of surveillance, as replaceable members of a group rather than citizens, and therefore risks leading to their "de-individualization".[26] In this light, the need to ensure that fundamental rights are observed becomes even more pressing.

What can the affected individuals do themselves? Despite the fact that it is their personal data that is concerned, there is very little that affected individuals can do. They will very rarely know that information about them is entered into a database or of any causal link with any subsequent action or decision in their regard. There is hardly access to justice in the sense of an ability to bring a case. Of course, law enforcement is always a special case to some extent when it comes to data gathering and data sharing. The need for confidentiality, even of secrecy, is clear certainly when it comes to ongoing or planned prosecutions. Still, when not only national cops, but also national border guards and intelligence officers access personal data that was entered for a concise and different purpose we need to recall the "forgotten purpose" of purpose limitation.[27] The reason this matters is that data cops "do not regulate truck widths or set train schedules. They have the capability of radically and permanently altering the political and legal contours of our society."[28]

---

[26] K. Tuori, *European Constitutionalism*, Cambridge, MA: Cambridge University Press, 2015, p. 317.

[27] E. Brouwer, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", in L.F.M. Besselink, F. Pennings and S. Prechal (eds), *The Eclipse of the Legality Principle in the European Union*, Alphen aan de Rijn: Kluwer Law International, 2011.

[28] M.J. Glennon, "Investigating Intelligence Activities: The Process of Getting Information for Congress", in T.M. Franck (ed.), *The Tethered Presidency: Congressional Restraints on Executive Power*, New York, NY: New York University Press, 1981, p. 52.