in:ex

Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

D.2.4 Policy Recommendation Report: The Intersection between the Schengen Information System and the EU Rule of Law

Deliverable submitted March 2011 (M36) in fulfillment of requirements of the FP7 Project, Converging and Conflicting Ethical Values in the Internal/External Security Continuum in Europe (INEX)

PRIO	International Peace Research Institute, Oslo	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.inexproject.eu

POLICY RECOMMENDATION REPORT
THE INTERSECTION BETWEEN THE SCHENGEN INFORMATION SYSTEM AND THE EU RULE OF LAW
INEX REPORT / MARCH 2011

JOANNA PARKIN[1]

1. Introduction

This policy recommendation report is based on the case study conducted within Work Package One on the development of the Schengen Information System II (SIS II), set out in the INEX working paper, *The Lifting of the Internal Borders in an Enlarged EU: The Relationship between the Schengen Information System and the Rule of Law*.[2] This report synthesises the key findings from the case study and draws a set of policy recommendations for improving policy strategies in the development of large-scale IT systems in the EU's Area of Freedom Security and Justice (AFSJ).

The Schengen Information System II was selected as subject of analysis for several key reasons: first, the SIS occupies a central role within the EU's ASFJ; it is a key flanking measure underpinning the freedom of movement and forms a cornerstone of EU internal security and migration management strategies. Second, the decision to upgrade the Schengen Information System to accommodate new member states and new functionalities is a tangible example of the growing priority given to security technologies within the EU's internal security strategy. Given that the SIS II is only one of several new large scale EU databases currently in the pipeline, it is pertinent to examine decision-making on SIS II in order to draw wider lessons for the EU's information management strategy. Finally, the development of SIS II was selected for analysis because it has become synonymous with inefficient policymaking: the project is considerably overbudget, several years behind schedule, and the source of serious tensions between member states and the Commission. At the time of writing, more than 5 years after the original deadline for completion of the SIS II project, the second generation of the SIS is still not operational and there is no guarantee that the SIS II will come on stream in the near future, if at all. More worrying still, should the SIS II enter into operation, serious question marks hang over its

[1] Joanna Parkin is a research assistant in the Justice and Home Affairs section of the Centre for European Policy Studies (CEPS). This report was drafted under the supervision of Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs Section of CEPS.

[2] See J. Parkin (2011), *The Lifting of the Internal Borders in an Enlarged EU: The Relationship between the Schengen Information System and the Rule of Law*, INEX Working Paper (D.1.5.), March 2011.

impact on fundamental rights in view of the new functionalities (including storage of biometric data) and extended scope of the upgraded system.

The case study aimed to unravel the underlying causes behind the deficiencies of SIS II, by focusing on the legal and political governance frameworks and decision-making practices during both the design and development phases of the SIS II project. It charted the chronological development of SIS II from the period 2001-2011 and assessed the implications of the patterns of governance and decision-making for the principles of accountability, proportionality and fundamental rights. This report first synthesises the key findings which emerged from the case study. It then elaborates a number of policy recommendations to be drawn from the empirical evidence brought to light by this analysis.

2. Key Findings: decision-making on SIS II and implications for the rule of law

2.1 SIS II shaped by the politics of emergency

Emergency-driven agendas played a considerable role in driving forward negotiations on SIS II that took place largely within Council working groups under the former EU third pillar. Decisions on the scope of SIS II were shaped by a doxa of security based on the construction of new transnational 'threats' to the EU, strengthened following the acts of political violence in New York in 2001 and Madrid in 2004. The politics of emergency surrounding 9/11 provided impetus for, and justified, a policy process on SIS II where there was no clear legal competence. It allowed member states to propose and quickly agree on a number of functionalities for SIS II which, given their implications for fundamental rights and rule of law, would have otherwise provided points of profound controversy.

In addition, political pressures to have SIS II on stream in time to allow for the expansion of Schengen to the 10 enlargement countries that joined the EU in 2004 led to an overambitious timetable. This had the effect of sidelining proper procedures for evidence-based policymaking (such as impact assessments) and excluded opportunities for democratic debate. Pressures surrounding the unrealistic calendar for SIS II meant that the European Commission began developing the technical system without first having the appropriate legislative instruments and legal basis in place, thus sowing the seeds for the technical, political and ethical tensions that followed.

2.2 Fragmented decision-making and struggles between EU and inter-governmental methods of cooperation

The difficulties encountered by SIS II cannot be separated from the fragmented decision-making and struggles between the EU and inter-governmental methods of cooperation that have marked the project from the outset. Despite endowing the European Commission with project management powers in 2001, and even after the expansion of the co-decision procedure in 2005, which strengthened the legislative roles of the Commission and Parliament, member states were not ready to relinquish control of a tool so central to security and migration management. Strategies to retain ownership of the project emerged. These include the proliferation, since 2006, of a complex network of expert working groups which have served as a means for national delegations and experts to steer the direction of the SIS II project in accordance with their aims. The proposal for an 'inter-governmental' alternative to SIS II (named SIS I+RE) put forward by Austria, France and Germany in 2008 can be interpreted as another strategy by member states to retain control of the Schengen Information System and represents a direct political challenge to the European Commission.

Repeated interventions from the Council and the member states have not only contributed to complicate the development process of what was already a highly complex technical project, but have undermined the project management capabilities of the Commission and called into question the Commission's perceived capability to develop large scale IT systems. Consequently, responsibility to develop large scale IT system (currently an exclusive Commission competence) may, in future, be transferred to the proposed IT Agency responsible for the operational management of large scale IT systems. This move could be interpreted as a step back in Europeanisation, (and a return to the inter-governmental origins of Schengen) given that the agency's management board would be comprised primarily of member states.

2.3 Weak rule of law, transparency and democratic accountability

Eliciting parallels with decision-making under the Schengen regime, an absence of rule of law, transparency and democratic accountability has characterised the design and development of SIS II. Several years before formal legislative proposals were presented by the Commission in 2006, new features and functionalities for the SIS II were being discussed and agreed by national experts (police, interior ministry representatives and experts of security technologies) in closed door Council working groups within the former third pillar framework. The adoption of the Regulation and Decision on SIS II in 2006 provided the first opportunity for democratic

debate, particularly as the legislative package on SIS II was subject to the co-decision procedure. However by this time the technical specifications for the new system had already been agreed in a series of non-binding Council and Commission documents and work on the development of the system was underway by external contractors. This limited the scope for democratic debate on the added value, necessity, scope and features of the SIS II.

The ability of the European Parliament to play its full role as co-legislator was further constrained: political urgency surrounding the adoption of the SIS II Regulation and Decision was used to fast track the adoption of the SIS II legislative package by the European Parliament, through the use of an informal trialogue procedure which further limited the possibility for democratic debate and scrutiny of the legislative proposals.

Since the adoption of the legal basis in 2006, a lack of transparency and accountability continues to characterise decision-making procedures surrounding the technical and political development of SIS II. The network of committees, groups, boards and task forces working on SIS II, some without a formal mandate and several with restricted participation, enable a small group of national experts to play a strong role in steering the direction of the project to the extent that who is really deciding on the direction of SIS II is obscured.

2.4 Marginalisation of proportionality and fundamental rights considerations

Against the background of this emergency led, fragmented and expert driven decision-making, questions regarding proportionality and fundamental ethical concerns have been marginalised. In violation of the EU's proportionality rule for policymaking, no assessment has been made of the necessity, added value and effects of the new system.

Fundamental rights implications of SIS II did not feature during the decision-making process, and were only introduced with the involvement of the European Parliament in 2006, although as seen above, the capability of the Parliament to play its full role as co-legislator was contrained. Consequently, and despite the Parliament's crucial input, the SIS II will only partially overcome the serious fundamental rights deficiencies of the current Schengen Information System. Meanwhile, the new functionalities of SIS II, such as biometrics, the interlinkage of alerts and the possibility for the system to be interoperable with other large scale EU databases, opens a series of important new ethical questions which have yet to be fully answered by the EU.

3. Policy recommendations

In view of the evidence brought to light by this paper, the following policy recommendations can be drawn:

a) SIS II has been shaped by the politics of emergency. Henceforward, steps should be taken to ensure that an ***evidence-based approach prevails over incident driven policy-making***. This implies a genuine assessment of whether new tools for information exchange will increase internal security in the EU, based on full consideration of the principles of necessity, efficiency, proportionality and fundamental rights. Advancing the EU strategy on information management should begin with an *independent* inventory of current policies, tools and institutional structures involved in data exchange in the field of security at EU level, building on the Commission's preliminary mapping exercise undertaken in 2010.[3] Such an inventory could feed into the forthcoming communication on the European Information Exchange Model scheduled for 2012 which should be used as an opportunity for a genuine re-assessment of the value and appropriateness of current instruments, and not an opportunity to propose new and unnecessary measures.[4]

b) The SIS II has not yet proved to be proportionate, safe and reliable. ***No new database should be set up*** until SIS II is found to have met these criteria. Both DG Justice, Citizenship and Fundamental Rights of the European Commission and the Fundamental rights Agency (FRA) should be engaged to conduct a fundamental rights proof-reading of SIS II, taking into account the risks implied by its potential inter-operability with other large scale databases. This assessment should include a comparison of the impact of the current SIS on fundamental rights and the extent to which SIS II will replicate/overcome these deficiencies. Should the SIS II fail its second milestone test, neither the SIS 1+RE, nor any other alternative to SIS II should be developed until a

[3] Commission Communication on an Overview of information management in the area of freedom, security and justice, COM(2010)385, Brussels, 20.7.2010.

[4] The Stockholm Programme calls on the European Commission to: "assess the need for developing a European Information Exchange Model based on the evaluation of the current instruments… These assessments will determine whether these instruments function as originally intended and meet the goals of the Information Management Strategy". See Council of the European Union, The Stockholm Programme – An open and secure Europe serving and protecting the citizens, 17024/09, Brussels, 2 December, 2009.

thorough assessment has been made of the ethical, efficacy and financial implications and a clear allocation of responsibility for the development of the alternative system has been defined in advance. If the decision is taken to delegate to member states the development of an alternative scenario for a transitional period, it must justify how the financial and legal accountability of those member states will be ensured.

c) An unrealistic timetable exerted artificial pressures on the decision-making process on SIS II. ***Overambitious political timetables should be avoided***, particularly in matters concerning the AFSJ and in areas as sensitive as security policy. They can weaken budgetary oversight, allowing financial expenditures to escalate. Moreover, by sidelining proper democratic and judicial scrutiny of new security technology measures, they risk undermining fundamental rights and the rule of law, and lead to more insecurity for the individual. [5]

d) Decisions on SIS II have largely been taken behind closed doors, in expert working groups and (until recently) with limited involvement of the European Parliament. The ***democratic accountability*** of policy-making relating to the development of large-scale EU databases must be ensured by ***allowing the European Parliament to play its full role*** in the policy process. Parliament should be fully informed of discussions and developments and given sufficient time to scrutinise proposals for future EU large-scale IT systems. The use of informal trialogue procedures should not be used to fast-track legislative proposals. Where trialogue procedures undermine transparency and remove the opportunity for open and plural debate, they are counterproductive. Likewise, the Parliament does not need to rely on the speed by which it passes legislation to prove itself as a responsible co-legislator (despite pressures to the contrary). Efficiency is measured not through speed but the extent to which the Parliament exercises democratic scrutiny of the legislative process, in fulfillment of its role as guardian of liberties and democracy in the EU. It is worth recalling that in the case of SIS II, it was the European Parliament that brought forward questions of fundamental rights and budgetary oversight. Given the central role of the Parliament in holding policymakers accountable to citizens (and taxpayers), the LIBE committee could take steps to strengthen its scrutiny of large-scale IT systems. This may require upgrading the current informal

[5] See also the policy recommendations stemming from F. Geyer's analysis of databases in the AFSJ: Geyer, F. (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS Challenge Research Paper No. 9, May 2008.

Privacy Platform into a formal Working Group or establishing a new working group looking more specifically at issues related to the EU information management strategy, including but not limited to privacy aspects. This working group would contribute to discussions surrounding the European Information Exchange Model and the desirable way forward for large scale EU IT systems by considering the real necessity of these instruments for internal security, as well as their impact on fundamental rights and budgets.

e) Expertise has been privileged in decision-making on SIS II, to the exclusion of other voices. In developing future large scale IT systems, the ***role of experts should be re-assessed and counter-balanced*** by allowing a plurality of actors and perspectives to provide input to the policy process. A close and formalised partnership should be ensured with the FRA, the EDPS and the Article 29 Data Protection Working Party in the phases preceding the formal adoption of proposals and when monitoring their implementation to assess the ethical impacts, added value and practical effectiveness of large-scale EU IT systems. This should be complemented with open consultation mechanisms with other key stakeholders, such as practitioners and civil society organisations.

f) The SIS II experience has led directly to the decision to create an ***agency for the operational management of large-scale IT systems*** in the AFSJ. Appropriate safeguards must be included in the legislation establishing the agency in order to avoid the risk of function creep and prevent infringements of the principle of purpose limitation. Legislation must be clear about the competences and clearly define and limit the scope of activities of the agency. The agency should operate in a transparent manner subject to democratic oversight by the European Parliament. The Parliament should therefore participate in the selection procedure for the agency's Executive Director and receive regular reports from the agency's management board.

g) The ethical dimension has not been part of the policy process of SIS II. Respect for ***fundamental rights and data protection*** must move to the centre of future policy strategies for developing large-scale IT systems in the AFSJ. The impact of new databases or any evolution in the use of current security technology on the individual

should be carefully and independently assessed and properly considered by the relevant Commission services before any new initiative is presented. This should be complemented with the application by DG Justice, Citizenship and Fundamental Rights, of the Commission's new methodology for evaluating EU policy compliance with the Charter of Fundamental Rights.[6] Further, "data protection by design", allowing for automated solutions to data protection requirements such as automatic deletion of data at the end of the permitted period, should be made an obligatory feature in the implementation of new and existing databases. Individuals must be adequately protected against the consequences of data inaccuracies or of negligent data exchange and must be properly informed of their rights.[7]

[6] See Commission Communication on a Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573, Brussels, 19.10.2010.

[7] See also the final policy recommendations of the Challenge Project: Bigo, D., S. Carrera and E. Guild (2009), *The CHALLENGE Project: Final Policy Recommendations on the Changing Landscape of European Liberty and Security*, CHALLENGE Research Paper No. 6, September 2009.