Submissions to House of Lords : Immigration Law Practitioners Association

Inquiry into the development of the second generation Schengen Information System (SIS II)

1. This association, which is comprised of immigration practitioners primarily in the UK, shares the view of the Committee of the House of Lords that the development of the SIS II system merits investigation in detail. We are, therefore, both honoured to participate in this inquiry and very interested in the subsequent report.

2. We have had the pleasure of reading the evidence submitted by the Standing Committee of experts in international immigration, refugee and criminal law with which we are in broad agreement. Accordingly, we will not repeat comments and issues which have already been taken up in that memorandum to your Lordship, except and unless our view differs from that the expressed in their memorandum.

Decision Making Process

3. As the original SIS was developed in fairly comprehensive secrecy among the five original Member States of the Schengen Agreement (though subsequent adherent states were involved), the degree of availability of information regarding the development of SIS II is refreshing. None the less, shortcomings are still evident. What is particularly evident in the documents which have been published by the Commission and those available on the Council's website under the transparency arrangements is that SIS II is consistently presented as a technical matter. The language employed is full of technical phrases, concerns about capacity and the like. Indeed, even the need for a new generation SIS was presented on the grounds of enlargement of the EU and the additional demands which ten new participants would make on the system. More important, in our view, than the technical issues of the SIS II, are the new capacities which it appears the SIS II will have and their consistency with fundamental rights of individuals. As many of the newer Member States are still painfully aware, the collection, retention, manipulation and use of data about the individual by the state has been critical to the maintenance of power by totalitarian regimes. One of the first things which occurred in the post 1989 period in Central and Eastern Europe was the massive destruction of files on individuals held by the Securitate and their ilk. It would be unwise to underestimate the importance of the right to privacy to democracy in Europe. While transparency must be the guiding principle in the activities of the state, the right to privacy is paramount for the individual. Coercive practices in some parts of Europe have been built on the inversion of these relationships.

Operational Management

4. Our key concern regarding management of the SIS II system is not so much which institution is responsible but rather what rules apply. It seems to us that it is unclear how the right of privacy of the individual is being protected in the EU at the moment. While the principle is contained in the European Convention on Human Rights (article 8 which prohibits state interference unless justified on limited grounds) and in the EU's own Charter of Fundamental Rights, there is no clarity on how the right is protected. What is clear is that unlike the US system, nowhere in the EU in the protection of his or her privacy (and data) considered a matter exclusively for the individual and for him or her to pursue single-handedly in the civil courts. In all Member States, as far as we are aware, there are institutions established by statute and paid out of public funds, whose job it is to protect the individual's data. While this may be in the form of ombudsmen with direct

responsibility, or of national agencies with indirect access, nonetheless the principle is the same. The state accepts a substantial degree of responsibility to protect the individual against the state in this field.

5. The question which arises in the case of SIS II is how is the individual's data protected when the entity collecting, storing, manipulating and transmitting the data is not the state or a private actor within the state's control, but a supranational actor in whom the state participates. Can the state systems of protection adequately protect the individual or are other entities and systems required? The highly active role which the European Ombudsman has taken to ensure transparency of EU policy making might be an example for the European Data Protection Supervisor as regards the protection of personal data. But the remit of both these EU institutions may be too limited to provide the effective control which fundamental rights norms require.

6. There is also a political question which arises here – if the citizen of the Union (particularly some of the citizens in the newer Member States) is vitally concerned about the collection and use of data on him or her (to the extent of burning the files less than 20 years ago), should national institutions be responsible for protecting the citizen against the supranational authority peeping into his or her life? Or should the EU institutions protect the individual's privacy, including from the national authorities excessive curiosity?

Biometric Data

7. There is much concern at the moment about the collection, retention and use of biometric data. In our view this is fuelled by the presentation of biometric data as a solution to the certainty of identification of individuals. While it is certainly the case that biometric data used in certain controlled situations can give fairly accurate indications of the identity of an individual, the parameters around that identification must be borne in mind. There is nothing automatic about biometrics – an official is required at all times to ensure that the biometric information being fed into the system corresponds to the individual who is feeding it in. Thus the impression of automaticity in the use of biometrics is not entirely accurate. For instance if a numeric photo is held to a camera and the image corresponds to the numeric photo which the computer at the other end of the numeric camera is expecting to receive, there is a full correlation; but this does not say anything about the person holding the numeric photo. The use of biometric data only moves one step on the point of verification that the biometric data actually belongs to the individual presenting it. However, the collection, storage, use and transmission of biometric data on some grounds, of individuals within a community, to the exclusion of other groups, places the monitored group substantially further under the control of the state's coercive forces than others as we explain in the next paragraph.

8. For instance, if the EURODAC data base were made available to law enforcement agencies in the Member States, asylum seekers who committed crimes would be discovered almost to a man. Thus the clear up rate of offences committed by asylum seekers would, statistically speaking, be excellent but would indicate a highly level of criminality among asylum seekers than among the domestic population. This impression would, of course probably be wrong, as the statistics would be based on the access to finger print data on all asylum seekers and the sparse fingerprint data available on nationals of the state. But the public imagination could easily be manipulated against asylum seekers on the erroneous conclusion that they are more prone to criminality than the domestic population.

9. DNA data presents even further problems. We understand that this type of biometric data can provide information on sex and race. Such data is inherently dangerous as the European experience in 19940 – 45 has shown.

Interlinking Alerts

10. The problem here is one of the transfer of data. Even where an authority has justified the collection and storage, for a limited time, of personal data, it cannot be presumed that the transmission of that data to another authority, even within the state, is justified. The principle of privacy in European human rights law mitigates against any such assumption. Transmission of data is among the most sensitive of issues regarding the right of the individual to privacy. While the individual may agree to the collection and retention of his or her data for one purpose, he or she may be vehemently opposed to its transmission to another authority – for instance information provided to state health services being transmitted to government agencies engaged in insurance or taxation. Alerts are only another way of speaking of personal data about individuals. While the legitimate interest of the state of to find persons suspected of criminal offences may justify the release of data, it is inconsistent with the right of the individual for this to happen on the basis of automaticity.

Criteria for Listing Persons to be refused entry on the SIS

11. One of the key legitimacy issues of the SIS has been that the vast majority of the data on individuals held on the system is data about third country nationals to be refused admission to the EU. Thus the SIS has become a glorified immigration data base rather than a tool in law enforcement in criminal matters (outside immigration offences). While the grounds for inserting law enforcement data on the SIS has been fairly well defined, the criteria for the inclusion of data concerning third country nationals has been woefully vague. A number of cases have come before the national courts of the EU on this question and the solutions have been diverse. What is particularly interesting is that the EU (whether in the form of the Commission, or the Council of Member States) has not taken this occasion to clarify and simply the rules on whose data should be included and whose removed. We understand that even two years on from the last enlargement of the EU some 'old' Member States are still trying to clear out their alerts on nationals of 'new' Member States - which alerts are not justified on the grounds of public policy, security or health as required by EU law. The decision by the European Court of Justice in the Commission's action against Spain for including data in the SIS on family members of Union citizens is particular instructive of how the issue of the inclusion of data on the SIS might be tackled. The Court held that while data on third country national family members of Union citizens could be held on the SIS, the reason for their inclusion must comply with EU law. Specifically they need to be a serious risk to public policy, security or health as interpreted by the Court in previous rulings. One might consider this ruling to be a type of ' taming' of the SIS in that the lawfulness of the inclusion of data will be controlled by the rules of EU law not the vague rules which are contained in article 96 CISA. Whether this optimistic reading of the ruling will prevail is still to be seen.

Use of Data

12. As we have set out above, one of the most important and legitimate concerns of the individual as regards the collection and retention of his or her data is whether it remains within the control and exclusive use of the agency which has collected it, or whether it acquires a life of its own, passing willy-nilly through different databases and different agencies around the EU or indeed the world.

The current controversy over the agreement between the Belgian operators of the SWIFT banking transfer system with the CIA exemplifies exactly this problem. Individuals transferring funds around Europe through the SWIFT system were happy to provide their data to their banks but are aghast at the prospect that that data was subsequently passed on to the CIA without their knowledge or consent. The European understanding of the right of privacy mitigates against any further transmission of data unless under very specific and precisely argued rules.

Adequacy of Data Protection

13. There has been a tendency over the past few years on the part of some state authorities to seek to interpret the fundamental right of privacy as consistent with rather relaxed practices of data exchanges and use among state institutions. This period appears to be coming to an end. The German Constitutional Court has had the occasion to consider and reject the manipulation of data for the purposes of racial profiling. The European Court of Human Rights has recently handed down a judgment reinforcing the right of the individual to protection of his or her data from interference by state authorities. The EC Data Protection Directive provides fairly clear rules (though insufficient, it would seem from the judgment of the European Court of Justice in the PNR case) to protect individual data. The EU's second and third pillars lack data protection measures and the framework decision proposed by the Commission for data protection in the third pillar is weaker as regards the protection of the individual than that already adopted in the first pillar. The collapsing of the pillar as proposed by the draft constitutional treaty would have resolved this issue, bringing a consolidated regime into existence with the data protection directive applying across the board (or almost and subject to its weakness as identified in the PNR judgment). The Commission has recently proposed the use of article 42 TEU to bring the third pillar into the first, which presumably would have the effect of bringing third pillar activities under the control of the data protection directive. This would be most welcome. The strengthening of the data protection directive would also be valuable bearing in mind the recent judgments in Karlsruhe and Strasbourg.

Finally, the UK's position: anomalous as it is, there is little which can be added other than to note that where a state does not participate in a treaty because it is unwilling to accept the freedom required by it, it cannot reasonably expect to enjoy the coercive benefits of the treaty.

13 July 12006