CENTRE FOR EUROPEAN POLICY STUDIES
Thinking CEPS ahead for Europe since 1983

The Other Side of Moon
The Schengen Information System and Human Rights: A Task for National Courts

CEPS Working Document No. 288/April 2008

Evelien Brouwer

Abstract

The recent proposals of the European Commission for a European Border Management Strategy are based on an almost blind faith in the use of large-scale databases, identification measures and biometrics for immigration and border control purposes. It is clear that these measures entail a risk to the protection of not only the right to privacy and the right to data protection, but also to the freedom of movement and the principle of non-discrimination. This paper by Evelien Brouwer, lecturer at the Law School of Utrecht University, considers the human rights implications of the Schengen Information System (SIS). Describing the case of Mr. and Mrs. Moon, who have been reported as "inadmissible" in the SIS for more than ten years, the difficulties for third-country nationals trying to remedy a false or unlawful SIS report are highlighted. The Moon case illustrates that the outcome of national proceedings dealing with an SIS alert can be very different. The author concludes with recommendations to guarantee individuals' rights to effective remedies and to improve the position and powers of national courts.

ISBN-13: 978-92-9079-785-2
Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

THE OTHER SIDE OF MOON

THE SCHENGEN INFORMATION SYSTEM AND HUMAN RIGHTS: A TASK FOR NATIONAL COURTS

EVELIEN BROUWER*

1. Introduction

In January 2008, the Schengen Joint Supervisory Authority (JSA) published its report on the implementation of Article 111 of the Convention Implementing the Schengen Agreement (CISA).[1] Article 111 entails the right of an individual to bring an action with regard to information held about him or her within the Schengen Information System (SIS). In this report, the JSA concludes that the cornerstone in safeguarding data subjects' rights is the enforcement of final court decisions and data protection authorities by the member state issuing the SIS alert. In practice, however, both the access to national courts and data protection authorities, and the enforcement of their decision with regard to SIS alerts is not a matter of course. Even if the SIS is operational for more than ten years, there is a lack of information and clarity with regard to the tasks and powers of national courts and data protection authorities while 'safeguarding data subjects' rights'. Unfortunately, the report of the JSA does not consider this problem.

In this contribution, I will describe the case of Mr. and Mrs. Moon, leaders of the Unification Church recorded by the German authorities in the SIS between 1995 and 2007. This case is one of a number of examples showing the necessity of effective legal remedies for third country nationals who are literally 'stored' in the SIS. An analysis of the different procedures dealing with their case in Germany, France, Belgium and the Netherlands offers valuable insight into significant problems concerning the use of databases such as the SIS for immigration law purposes. In the first place, the Moon case illustrates the human rights implications of an SIS alert; implications that are often ignored or even denied by national authorities issuing the alert or refusing entrance or a visa on the basis of such an SIS alert. Secondly, the judgements illustrate the uncertain or restrained attitude of some national courts when dealing with a foreign decision to report an individual in the SIS. Before going into the different procedures in the abovementioned countries, I will describe the SIS and give an overview of the rights and remedies of the individuals concerned.

---

* Evelien Brouwer is lecturer in constitutional and administrative law at the Law School of Utrecht University, e.brouwer@law.uu.nl. She would like to thank Leonard Besselink and Sergio Carrera for their valuable comments. This paper falls within the scope of the CHALLENGE project – *the Changing Landscape of European Liberty and Security*, funded by the Sixth EU Framework Programme of DG Research, European Commission, see www.libertysecurity.org.

[1] Report of 18 January 2008 on a survey of the implementation of Article 111 of the Schengen Convention, SCHAC 2502/08. Another report of the JSA of 18 January 2008 concerned the use of Article 99 alerts in the SIS, SCHAC 2501/08.

2. The Schengen Information System: Keeping the unwanted out[2]

2.1 Background

At this moment, the Schengen Information System or SIS is one of the most important databases used for immigration and border controls in the EU.[3] The SIS finds its roots in the abovementioned CISA: an intergovernmental treaty signed in 1990 by a small group of EC member states dealing with the abolition of internal border controls. Since the integration of the so-called Schengen acquis in EU law by the Amsterdam Treaty of 1997, the CISA has become binding for the EU member states, including the new EU member states, and on the basis of a special protocol, also for Iceland and Norway. The UK and Ireland are only partially involved in the Schengen acquis. Since its launch in 1995, the majority of personal data held in the SIS concerns third-country nationals to be refused entry on the basis of Article 96 CISA.

Until September 2007, the SIS was in use by the 15 'old' EU member states (except the UK and Ireland) and Norway and Iceland. In this year, the SIS contained approximately 15 million reports on different categories of persons and objects, including stolen vehicles and lost or stolen identity papers, as well as persons wanted for arrest for extradition or for the purposes of discreet surveillance, witnesses or other persons summoned to appear before the judicial authorities. Since 1 September 2007, with the abolition of internal border controls in the enlarged Schengen area in December 2007, nine new EU member states obtained access to the SIS (under the headings of "*SISone4all*").[4] These nine states include the Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia and the Slovak Republic. Statistics of 1 January 2008 show that compared with the data of January 2007, the total number of data stored in the SIS rose by 30% from 17,5 million data to almost 23 million data.[5] The most significant rise is due to the increase of data entered on the basis of Article 100 CISA on stolen or lost ID documents (30%) and vehicles (74%). Surprisingly, the number of data held on third country nationals to be refused entry dropped by 7.4% since 2007 (from 752.338 to 696.419 alerts). One would have expected that with the accession of new member states this number of alerts would also rise considerably. This decrease could mean that some member states still had to withdraw a large number of data on third-country nationals who, with the accession of the new member states in 2004, became EU citizens.

According to Article 96 CISA, the decision to record a third-country national in the SIS can be based firstly on a national decision that this person is considered a threat to public order, public security or national security. Secondly, the decision can be based on an immigration law decision regarding the deportation, refusal of entry or removal of this person. The consequence of such a report in the SIS is that the person will be refused entry to every other Schengen state. On the basis of an SIS alert, a third-country national can also be denied a visa or a residence permit, or even expelled or detained. This refusal of entry or visa is based on the provision in

---

[2] In the words of the House of Lords European Union Committee: "….keeping the unwanted out – for example, undesirable aliens – and preventing the wanted from leaving, chiefly those suspected of criminal offences", 9th Report of session 2006-07, *Schengen Information System II. Report with Evidence*, HL Paper 49, London: The Stationery Office Limited, published 2 March 2007.

[3] For more details on the development and background of SIS, see Evelien Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, series *Immigration and Asylum Law and Policy in Europe* 2008 (dissertation Radboud Universiteit Nijmegen, 2007), ISBN: 978-90-04-16503-8.

[4] Council Decision 2007/471 of 12 June 2007, *OJ* L179/46, 7.7.2007.

[5] Source: SIS Database Statistics dd. 01/01/2007, Council document 6178/07, 13 February 2007 and SIS Database Statistics dd. 01/01/2008, Council doc. 5441/08, 30 January 2008.

Article 5 CISA (now Article 5 of the Schengen Borders Code) stating that a person for whom an alert has been issued in the SIS for the purpose of refusing entry, must be refused entry into the Schengen territories.[6] Only on the basis of humanitarian grounds, grounds of national interest or because of international obligations, may national authorities derogate from this duty to refuse entry.

The national criteria for registration into the SIS are very divergent and in many countries SIS alerts can be based on minor offences or even the suspicion of a criminal act. Article 112 CISA obliges national authorities to check every three years whether it is still necessary to maintain an SIS alert. Reports of national data protection authorities and, as we will see below, the case of Mr. and Mrs. Moon show that in practice these time limits can be extended indefinitely.[7]

2.2 SIS II: Individual assessment and proportionality clause

In order to transform the SIS into a system that was technically feasible for a larger group of users, including the new EU member states, the EU legislator prepared the so-called second-generation SIS, or SIS II. This development of the SIS II has been used to introduce new functions of the SIS and in December 2006, the EU Council adopted Regulation 1987/2006 on the establishment of SIS II.[8] SIS II is planned to be operational in 2009 and is to be used by no fewer than 30 states.

Compared to Article 96 CISA, the criteria for inserting third-country nationals to be refused entry into SIS II remain more or less the same. What is new compared to Article 96 CISA is the provision in Article 24 (1), according to which a national decision to issue an alert should be taken "on the basis of an individual assessment". Article 24 states that an SIS II alert shall be based "on a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law taken on the basis of an individual assessment". This new provision makes it clear that national authorities cannot report third-country nationals "automatically" on the basis of another decision that is taken with regard to this person, for example an expulsion decision. For each individual case, the national authorities will have to consider whether the national criteria and the criteria of the Regulation are met and whether the interests at stake merit registration in SIS II.

This individual assessment requirement should be read together with the so-called proportionality clause in Article 21 of the SIS II Regulation. This provision goes further than the clause that was included in Article 94 (1) CISA. According to this latter provision, member states issuing an alert should determine in advance whether the case is "important enough to warrant the entry of the alert in the SIS". The new Article 21 provides: "Before issuing an alert, Member States shall determine whether the case is adequate, relevant and important enough to warrant entry of the alert in SIS II". With the addition of the criteria of 'adequacy' and 'relevance', the new provision makes it clear that the importance of the case or matter for which a person is to be reported is not enough. There should be a direct relationship between the reason for which a person is to be reported in SIS II and the added value or effect the registration will have for the reporting national authorities. Both rules – the individual assessment requirement and the proportionality clause – are important limitations on the power of national administrations to enter information on third-country nationals into SIS II.

---

[6] Schengen Borders Code or Regulation 562/2006, 15 March 2006, *OJ* L105, 13.4.2006.

[7] For a description of the national implementation of SIS in France, Germany and the Netherlands, see Evelien Brouwer's thesis, supra note 4.

[8] *OJ* L381/4, 28.12.2006.

3. Rights and Remedies

3.1 Right of access to information and the right to information

Both the CISA of 1990 and the new Regulation 1987/2006 on SIS II include provisions on the rights of individuals reported in the SIS. According to Article 109 CISA, the right of individuals to demand access to their data is to be asserted in accordance with the national legislation of the state in which they invoke this right. When national law so provides, as is the case in France, the right to access cannot be exercised directly, but must be asserted via the national supervisory authority. There are two restrictions on the right of access with regard to information held in the SIS. Firstly, when the state to which the application for access is made is not the issuing state, the latter state must be given the opportunity to set forth its position, before the requested state can give the individual the requested information. This duty to consult the issuing state often causes considerable delays in the relevant procedures and extends the time the applicant has to wait before he or she is informed. Secondly, according to Article 109 (2), information must be refused when this is "indispensable for the performance of a lawful task in connection with the alert" or "for the protection of the rights and freedoms of other parties". The right to access must in any event be refused during the period of validity of an alert for the purpose of discreet surveillance.

Article 41 of the new Regulation 1987/2006 on SIS II includes a comparable rule as provided in the CISA. As in the Article 109 CISA, the requested state should give the issuing state the opportunity to state its position before communicating the requested data. Also, Article 41 allows national legislatures to give the national data protection authorities a primary role with regard to access rights. Unlike the provision in the CISA, Article 41 includes a time limit of 60 days within which an individual applying for access to his or her data should be informed. And in no more than three months should the individual be informed of the "follow-up" given to the exercise of his rights of correction or deletion.

Article 42 of the Regulation on SIS II gives additional rules on the right of information comparable to the provision in the EC Directive 95/46 on the protection of personal data.[9] Article 42 provides that third-country nationals who are the subject of an alert shall be informed in accordance with Articles 10 and 11 of Directive 95/46. This information must be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert in SIS II. The inclusion of this right is of utmost importance as in many member states using the SIS, persons are not informed about the fact they are being registered into the SIS, and they often find out about their alert when it is too late to start legal proceedings. Article 42 (2) of the SIS II Regulation allows for exceptions to this right of information going further than those provided for in the EC Directive 95/46. Firstly, the information must not be provided where "(i) the personal data have not been obtained from the third-country national in question; and (ii) the provision of the information proves impossible or would involve a disproportionate effort". Secondly, the information must not be provided where the third country national in question already has the information. Thirdly, there is no duty to inform the data subject when national law allows for the right of information to be restricted, in particular in order to safeguard national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences. It is the important but in practice very difficult task of courts and data protection authorities to oversee that these limitations are not being interpreted too widely by the national authorities.

---

[9] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L281, 23.11.1995.

3.2 Right to remedies

As mentioned above, Article 111 CISA includes a crucial provision for the legal protection of individuals registered in the SIS. Article 111 (1) provides for the right of a person, in the territory of each contracting party, to bring before the courts or the authority *competent under national law* an action to correct, delete or obtain information or to obtain compensation in connection with an alert involving him or her. Thus, the individual is not obliged to address the court in the country of his nationality or stay, but may seek access to a competent court or authority of *every* state applying CISA or using SIS. However, the choice of authority that is competent to assess the individual claim and the scope of the available remedies has been left to the scrutiny of each Schengen State.

Article 111 (2) obliges each contracting party to mutually enforce the final decisions of the national courts or authorities concerning SIS. This provision had to be inserted because the use of SIS is based on the principle that only the contracting state issuing the alert can modify, add to, correct or delete the data in SIS (Article 106 CISA). If a national court considers a foreign SIS report unlawful and orders the withdrawal of this alert, the reporting member state is obliged to enforce this decision. In practice, this implication of Article 111 (2) often raises doubts and mistrust by national authorities and the judiciary. Where national authorities do not have any problem recognising and enforcing foreign SIS alerts, they generally find it difficult to accept the binding force of foreign courts' decisions. Based on the principle of sovereignty, it is held that national courts cannot assess the lawfulness of foreign administrative decisions. However, any other interpretation would render meaningless the rule inserted into Article 111 (2). A similar conclusion can be drawn from the judgement of the European Court of Justice (ECJ) in *Van Straaten v. the Netherlands*. In this case, a Dutch lower court was considered competent to assess the lawfulness of an Italian Article 95 alert in the SIS and given a tool to order the Italian authorities to withdraw this alert.[10] Moreover, Regulation 1987/2006 maintained the same rule as in Article 111 CISA, which means that the member states did not want to amend this 'cornerstone' for the protection of individual rights. According to Article 43 (1) of Regulation 1987/2006, every person may bring an action before the courts or the authority competent under the law of any member state to access, correct, delete or obtain information or to obtain compensation in connection with an alert relating to him/her. Article 43 (2) provides that the member states must mutually enforce the final decisions of national courts or authorities as referred to in paragraph 1.

One of the remaining problems is the exact meaning of "final decisions". In the aforementioned report on Article 111 CISA, the JSA fails to offer a clear definition. In my view, "final decisions" should not be interpreted too narrowly. It does not imply that this only covers decisions of the highest (administrative, civil or criminal) courts. The fact that Article 111 CISA and Article 43 of the SIS II Regulation also refers to decisions of national data protection authorities, means that a decision should be considered as final, as long as the decision is executable and none of the parties lodged an appeal against this decision.

4. The Case of Mr. and Mrs. Moon

4.1 Background to the case

Mr. Moon is the founder and leader of the religious organisation the Unification Church. To prevent Mr Moon and his spouse, born respectively in 1920 and 1943, from visiting Germany to

[10] C-150/05. See District Court Den Bosch for the Dutch judgement, 4 April 2007, LJN: BA 2132.

meet its members, the Border Police of Koblenz listed them in the Schengen Information System in 1995 to be refused entry on the basis of Article 96 CISA. This report in the SIS was based on the general concern of the German authorities that the visit of the Moons to Germany would constitute a danger to German youth and would thus pose a threat to public order and security. According to the German government, the activities of the leaders of the Unification Church would pose a threat to "the personal development of young people" and their public performances could lead to "violent reactions" (*heftigen Reaktionen*) in Germany.[11] As citizens of the Republic of Korea with legal residence status in the USA, Mr. and Mrs. Moon do not need a visa to enter the EU. Therefore, they usually asked leave to enter one of the EU member states before travelling to that state. The Moon couple lodged procedures in different member states against their alert in the SIS. As we will see below, only twelve years after their first registration, the German authorities were forced by a decision of the German court to withdraw their alerts. Temporarily, the Moon couple also have been reported in the SIS by the Portuguese and Austrian authorities. And after the withdrawal by the German authorities in 2007, the French authorities even 're-entered' the alerts in the SIS, apparently on behalf of the German authorities. However, at the end of 2007, these French alerts were deleted again.[12]

4.2 Germany: Freedom of religion

In 1998, the German authorities extended the alert on Mr. and Mrs. Moon for another three years. In the same year, the German section of the Unification Church lodged an appeal against the SIS alert before the administrative court. This organisation held that the residence ban applicable to their leader, Mr. Moon, would cause an infringement of their constitutional right of freedom of religion (Article 4 (1), (2) of the German Constitution). By making it impossible for their leader to meet members of his religious organisation, these members would be prevented from exercising their right to freedom of religion.

In July 2001, the Federal Administrative Court reached its first decision in this case.[13] In its judgement, the Court did not deny the existence of a right to freedom of religion of third parties with regard to the SIS alert on their leader. The Federal Court stressed that it was the duty of the state to take into account the interests of the religious movement concerned. According to the Court, a residence ban on a religious leader could be in breach of the constitutional right to freedom of religion of others; "if the visit of the leader, according to the standards of current religious doctrine, would have significant meaning for the common exercise of this religion". The question of whether these standards would give the applicants a subjective right in this case was referred back to the Koblenz Oberverwaltungsgericht. In its judgement of June 2002, the administrative appeal court delivered a much stricter interpretation of the freedom of religion as that formulated by the Federal Court in its judgement July 2001.[14] Among other things, the Koblenz Court held that, according to the theology of the Unification Church, the personal presence of the leader at religious meetings would not be an absolute prerequisite, referring to earlier satellite and internet meetings that were organised by this church. In September 2003, the Federal Administrative Court rejected the appeal against the judgement of the Koblenz Court. Although the Federal Administrative Court confirmed the claim of the applicants that the court of Koblenz had made an overly strict interpretation of the "specific significant meaning of a

[11] These reasons of the German government were cited by the Federal Administrative Court in its judgement BVerwG, 10.07.2001, Az. 1 C 35.00.

[12] Information provided by the Dutch lawyer of Mr. and Mrs. Moon.

[13] BVerwG 10.07.2001, Az. 1 C 35.00, *InfAuslR* 2001, p. 509.

[14] OVG Koblenz 7.6.2002, Az. OVG 12 A 10349/99.

visit of a religious leader", it did not examine the lawfulness of the SIS alert itself.[15] Generally, the Court recognised the relationship between a residence ban and the constitutional rights of others. However, in this case, it held that there were no sufficient grounds to conclude that the refuted decision of the German authorities not to grant entrance to Mr. and Mrs. Moon were in breach of the right of freedom of religion of its members. In its final consideration, the Federal Administrative Court emphasised however that this judgement did not mean that with regard to future visits to be planned by the Moon couple, the Court would rule in the same way.

In November 2006, the Constitutional Court annulled the judgement of the Federal Administrative Court and handed the case back to the Court of Appeal of Koblenz.[16] The Constitutional Court ruled that the constitutional right to freedom of religion included not only the right to expression of that belief but also to enable certain practices of religion of which the content was mainly to be decided by the religious community itself. The question of whether a personal encounter between a religious leader and its members was of specific importance for this religious movement, was not a matter to be decided by the governmental institutions. The Constitutional Court therefore criticised the fact that the Federal Administrative Court made its own assessment of whether a meeting of the members of the Unification Church and their leader was of specific significance for their religious belief. More importantly, the Constitutional Court emphasised that the Federal Administrative Court did not assess whether the alert in the SIS was in accordance with the applicable laws. The Constitutional Court explicitly ruled that the SIS alert which is based on Article 96 (2) CISA, requires the availability of "substantial grounds" (*gewisse Erheblichkeit*) that the presence of the third-country national poses a threat to public policy or security. For this conclusion, the Court referred to the examples listed in Article 96 (2) including the fact that the person has been convicted or that there are serious grounds to believe that he or she will commit serious crimes in future. According to the Constitutional Court, during the procedure before the administrative courts it was not clarified why the visit of Mr. and Mrs Moon implied such risk. Furthermore, the Constitutional Court held that there were no reasons to believe that the SIS alert on Mr. and Mrs. Moon could be justified, especially when taking into account the interests of the applicants (members of the Unification Church).

Finally, in its judgement of 19 April 2007, the Administrative Court of Appeal ruled that the German SIS alert on Mr. and Mrs. Moon was unlawful.[17] According to the Court, the German government did not produce convincing arguments to justify the refusal of entry of Mr. and Mrs. Moon. Considering the importance and special weight of the constitutional rights of the members of the Unification Church, the Court of Appeal found that this right could not be limited on the basis of "vague assumptions of fear" (*vage geltend gemachten Befürchtungen*). The German authorities did not lodge an appeal against this decision. Finally, in 2007, after 12 years of litigation, the alerts on Mr. and Mrs. Moon were deleted by the German authorities from the SIS.

The conclusion of the German Constitutional Court on the need of an individual assessment has been repeated in another case, in a decision of the Administrative Court of Munich.[18] The Munich Court rejected the automatic reporting of third-country nationals in the SIS after their expulsion or deportation. The Court ruled that the German authorities should make an individual assessment of the interests and rights of the person at stake. In this case, they should

---

[15] BVerwG 4.9.2003, Az. 1 B 288.02, *InfAuslR* 2004, p. 38.

[16] BVerfG 9.11.2006, BvR 1908/03, § 3.

[17] OVG Koblenz, 19.04.2007, Az. A 11437/06.

[18] VG München 19.12.2006, M 21 k 05.2136, reported in *ANA-ZAR* 1/2008, p. 4.

have taken into account that issuing an alert on the applicant in SIS would prevent his lawful residence in Spain.

4.3 France: Right of access to information

Faced with their refusal of entry by the French authorities, Mr. and Mrs. Moon also started judicial proceedings in France. With regard to their request to be allowed entry and stay for several days, their claim was rejected by the French courts. Even if in previous judgements, the French highest administrative court, the Conseil d'État, established a critical review of the reasons for foreign reports in the SIS, in the case of Mr. and Mrs. Moon it was reluctant to assess the lawfulness of the German alert.[19] The Conseil d'État argued that, based on the information submitted by the German government with regard to the reasons for its report in SIS, the French authorities were justified in deciding, without making a "manifest error of appreciation", that the German SIS report was not based on any legal or factual error. Therefore, the application to annul the refusal of rectification made by the French Data Protection Authority, Commission Nationale Informatique et Libertés or CNIL, was rejected. The French lawyer of Mr. and Mrs. Moon started proceedings before the European Court of Human Rights in Strasbourg, claiming that the alert infringed the applicants' right of freedom of religion as protected under Article 9 ECHR. However, after the deletion of their alerts in the SIS in 2007, they withdrew their claim.

Although the Moon couple did not succeed in their personal claim before the French court, their proceedings resulted in general discussions and even changes in French law with regard to the right of (indirect) access to information. Mr. Moon applied for access to the information entered in the NSIS on behalf of the German authorities. With regard to the right of access to the data held in the NSIS, Article 6 of the French NSIS decree of 6 May 1995 stipulated that the right to access is to be exercised in conformity with Article 39 of the LIFL.[20] On the basis of this latter provision, the right of access had to be asserted through the CNIL.[21] Before 2002, based on a theory of "indivisibility of data files", it was generally accepted that if a public file contains information that should be kept secret in the interests of national security, a person should be denied direct access to the whole file. Considering the partial use of the NSIS for national and public security purposes, and based on the 'indivisibility rule', both the government and the CNIL argued that there was only a right of indirect access with regard to data held in the SIS. In practice, the application of the right to indirect access to SIS resulted in long delays before the applicant was informed. And generally, if the information was to be refused, as in the underlying Moon case, the applicant would not be given any reasons for this refusal. The CNIL only informs the applicant that he or she is not to be given access to his or her data. In its decision of 6 November 2002, the Conseil d'État departed from its earlier jurisprudence on the indivisibility theory. The Conseil d'État concluded that with regard to information held in the SIS on the basis of Article 96 CISA, applicants had a right of direct access.[22] The Conseil d'État explicitly distinguished between, on the one hand, information held in the NSIS, communication

---

[19] CE 2 June 2003, no. 219588, see *Hak Ja Han M (Mrs. Moon)*. For earlier judgements in which the Conseil d'État was more critical: CE 9 June 1999, no. 190384; CE 9 July 2001, no. 209037; CE 11 July 2001, no. 206644; CE 15 March 2002, no., 221818; CE 13 December 2002, no. 224877.

[20] Law no. 78-17 of 6 January 1978 "relative à l'informatique, aux fichiers et aux libertés".

[21] Decree no. 95-577.

[22] CE 6 November 2002, *Sun Myung X (Moon)*, no. 194295-219587. Most of the jurisprudence of the Conseil d'État and other French courts can be downloaded from http://www.legifrance.gouv.fr, or, partially, via: http://www.conseil-etat.fr/ce/home/index.shtml. This judgement has been commented upon by R. Errera in *Public Law*, 2003, p. 187.

of which would affect the interests of national security, defence or public order and, on the other hand, information that would not affect these interests if communicated. With regard to the second category, the highest administrative court decided that the responsible authorities, or the CNIL with the consent of these authorities, would have to communicate these data to the person concerned.

In order to implement the consequences of this judgement, the French legislature amended Article 39 LIFL in 2003.[23] Based on this amendment, information can be communicated directly by the CNIL to the person concerned, if the CNIL concludes that the communication of the personal data to the data subject does not interfere with the interests of national security, defence or public order. Unfortunately, in 2005, the extended power of the CNIL to communicate 'insensitive' information directly to the person concerned was restricted again. Based on a decree from 2005, this information may not be communicated by the CNIL if this is prohibited by the authority responsible for the data processing.[24] This means that it is no longer the CNIL deciding whether the information can be directly communicated or not.

4.4 Belgium: Freedom of religion revisited

As in the German procedures, freedom of religion played a central role in the decision of the Belgian court dealing with the SIS alerts on Mr. and Mrs. Moon. Also in this case, it was the Belgian section of the Unification Church applying against the refusal of the Belgian authorities to allow the Moon couple access for four days in order to be able to participate in a conference held in Belgium. In a judgement of 6 December 2006, the Belgian Administrative Court of Appeal (Brussels) explicitly ruled that the Belgian religious organisation, which was a member of the Unification Church, was admissible in its appeal against the refusal of entry of their leader, Mr. Moon.[25] The Belgian Court held that the organisation had a valid interest with regard to the admission of their leader to their country and with regard to a meeting between Moon and his disciples, including the members of the Belgian section of the Unification Church. According to the court, even if the Belgian organisation was not the addressee of the refuted decision (refusal of entrance to Mr. Moon), this decision infringed the rights as protected in Article 9 and 11 ECHR of the members of this organisation. The right to freedom of religion implies the right to manifest this right collectively, in public and with those who are supporters of this religion. The Belgian Court made explicit that even a religious movement qualified as a sect falls under the protection of Article 9. Furthermore, the Belgian Court concluded that the Belgian government did not submit any interest of public security or other pressing grounds. The Court emphasised that the Belgian authorities refused entry without knowing the reasons for the alert and without considering whether these reasons were in accordance with the criteria of Article 96 CISA. In its conclusion, establishing that the decision was insufficiently motivated and in breach of the limitation grounds of Article 9 ECHR, the court ordered the Belgian state to give Mr. Moon leave to enter Belgian territory for five days.

The decision of the Belgian Administrative Court is important for two reasons. Firstly, because of the conclusion that national authorities making a decision on the basis of a foreign SIS alert have a duty to investigate the reasons for this alert. Secondly, the Court confirmed the duty of national authorities to assess the proportionality of the reasons for refusing Mr. and Mrs. Moon entry considering the infringement of human rights caused by the refusal of entrance.

---

[23] Law no. 2003-239 of 18 March 2003.

[24] Decree no 2005-1309, *JO* 22 October 2005.

[25] 2006-12-07, Cour d'Appel de Bruxelles, 2006/KR/223.

4.5 The Netherlands: Principle of mutual cooperation v. human rights obligations

Before 2005, in spite of the German alert in the SIS, the Dutch authorities granted the Moons temporary access for short visits several times. These visits were allowed under certain conditions, such as promises from Mr. and Mrs. Moon that they would not seek public attention or have contact with the press during their visit to the Netherlands. These visits took place in 1997, 1999 and 2000. In 2005, however, the Dutch Minister for Immigration refused the applicants permission to enter the Netherlands for a short visit. This refusal resulted in several proceedings before the Dutch courts. These proceedings dealt, among other things, with the question of why the Dutch government refused to apply the provision of Article 5 (2) CISA making it possible to grant a third-country national access to its territory on humanitarian grounds, despite an alert by another Schengen State. As we will see below, during the Dutch procedures, the Moons invoked their freedom of religion, but without success.

Three judgements from 2005 and 2006 deserve attention at this point. In 2005, Mr. and Mrs. Moon began proceedings against the refusal of entry by the Minister of Immigration. In order to make it possible to visit the Netherlands for three days in November 2005, they applied for an interim measure to the District Court of Amsterdam. This interim measure was granted on 21 October 2005.[26] The Court ordered the Dutch authorities to treat the Moon couple as third-country nationals not to be refused entry on the basis of Article 5 CISA, for three days in the period around 3 November 2005. In order to reach this decision, the Court rejected the formal viewpoint of the Minister, according to which the applicants had no right of appeal since there was no administrative decision. The Minister argued that Article 5 (2) CISA could not be invoked because it was not directly applicable. The Amsterdam Court rejected this argument referring to the meaning of Article 111 CISA. Even if the lawfulness of the German alert could not be discussed during this procedure, the Court held that this foreign alert affected Mr. Moon and Mrs. Moon "within the Dutch legal framework" following the intention of the Dutch authorities to deny the applicants right of entry. The Court ruled that the Dutch government attached legal consequences to the German alert and therefore the applicants should have the right of appeal against the decision of the Minister, which made it clear that they would be refused entry. In a letter of 18 May 2005, which was cited during this procedure, the Minister of Immigration stressed the increasing importance of "respecting the SIS alerts of other Schengen partners", especially considering the fact "that Europe was getting stronger", but also because of "the changed situation with regard to security in the world". The Court, however, rejected these grounds as unfounded. In its conclusion, it referred to the decisions of the Dutch government before 2005 by which the Moons were granted access and to the earlier statement by the German authorities that they would not object to such a temporary admission.

The Minister of Immigration appealed against this interim measure. During the same appeal procedure, the applicants asked the Court to impose a penalty of € 1 million per day in the event of non-compliance by the Dutch authorities. Both appeals were rejected by the Court on 1 November 2005.[27] During this procedure, the Dutch government submitted further information on the 'lawfulness' of the German alert. Firstly, it was stated that, apart from Germany, the French and the Portuguese authorities had also reported the Moons as unwanted in the SIS. Secondly, it was held that in several judgements the German courts concluded that the alert in question was lawful. Thirdly, the Minister of Immigration produced a memo dated 27 October 2005 at a meeting between the IND (Immigration and Naturalisation service) officers and a

[26] District Court of Amsterdam, 21 October 2005, *Jurisprudentie Vreemdelingenrecht* 2006/69, annotation B. Olivier.

[27] District Court of Amsterdam, 1 November 2005, AWB 05/48355, AWB 05/48358.

German liaison officer. During this meeting, the latter officer submitted the German objections to a visit to the Netherlands by Mr. and Mrs. Moon. This new information did not convince the Dutch court. With regard to the alerts of the two other Schengen States, the Court found that these were not substantiated during the proceedings. With regard to the more recent decisions of the German court, the Dutch Court stressed that these judgements were applicable to the German situation and could not "have any meaning for the (Dutch) dispute at issue". Finally, the memo of October 2005 was also considered irrelevant, since it provided no new facts or circumstances that should have led to the withdrawal of the interim measure.

In a decision of 23 June 2006, the same District Court was asked to consider a renewed application from Mr. and Mrs. Moon for admission into the Netherlands, this time only for 24 hours.[28] This application was declared inadmissible by the Minister of Immigration, after which the applicants again lodged an appeal for a temporary provision. In these judgements, the District Court of Amsterdam refused to consider the application for a provisional measure, but decided immediately on the merits of the case. This judgement is important because the District Court of Amsterdam rejected the formal reasoning of the Minister of Immigration, according to which a request to review an earlier decision refusing the Moon couple leave to enter would be inadmissible. The Minister had claimed that there was no formal decision by the border guards against which Mr. and Mrs. Moon could lodge an appeal. According to the Minister, the question of whether or not Mr. and Mrs. Moon should be granted access was a decision to be taken by the Dutch border police. Since the applicants had not yet travelled to the Netherlands and had not submitted their request at the border to the appointed officers, the Minister held that they had not been formally refused entry. The Court dismissed the Minister's grounds by stating that the applicants cannot be asked to travel to the Dutch border first in order to appeal against the decision to refuse them entry even if, based on earlier letters from this Minister, they knew their (short) stay would be refused anyway. Mr. and Mrs. Moon, as South Korean nationals, were not obliged to hold a visa in order to enter the Netherlands. Therefore, their only way of knowing whether they would be allowed entry, was to ask for this before starting their journey. The Court stated that it is the responsibility of the Minister of Immigration to decide whether or not to refuse entry to the Netherlands. Since the request by the applicants of 2 June 2006 was to be considered a request for an administrative decision, the Minister acted unlawfully when she rejected this request as inadmissible. The Court ordered the Dutch government to reach a new decision within six days of the date of publication of this judgement, so as to allow the applicants to make their travel arrangements. In this judgement, the Court did not deal with the substantial grounds on which the Moons were registered in the SIS.

In March 2007, the District Court of Amsterdam rejected the appeal of Mr. and Mrs. Moon against a renewed negative decision of the Minister of Immigration. In this case, the applicants referred to their rights of freedom of religion and freedom of speech as protected in Articles 9 and 10 ECHR.[29] They also claimed that the decision of the Minister was insufficiently motivated. Based on rather formal grounds, the Amsterdam Court this time rejected these claims and held that the Minister had rightly put more weight on the 'Schengen obligations' than on the individual claims of the applicants. According to the court, the Dutch authorities were not obliged to specify the reasons for this refusal, even if in previous years Mr. and Mrs. Moon had been granted access to the Netherlands. Unfortunately, their appeal against this latter judgement was discontinued when it became clear that the German authorities had withdrawn the alerts on

[28] District Court of Amsterdam, 23 June 2006, AWB 06/27382, AWB, 06/27348.

[29] District Court, 23 March 2007, *Jurisprudentie Vreemdelingenrecht* 2007/245, annotation E.R. Brouwer.

Mr. and Mrs. Moon. Considering there was no further interest in this appeal, the court considered the case closed.

5. Conclusions

5.1 Human rights and the SIS

The case of Mr. and Mrs. Moon is just one of many, many cases of third-country nationals confronted with the consequences of being registered in the SIS for the purpose of refusal of entry. Many of these procedures are being dealt with by administrative courts dealing with the negative decision of immigration authorities on the basis of an SIS alert.[30] In this context, it is surprising, not to say worrying, that the national data protection authorities only reported a small number of cases to the Joint Supervisory Authority for the aforementioned inquiry on the implementation of Article 111.[31] This seems to imply that the supervisory authorities are not sufficiently informed about the problems of dealing with the SIS or with the procedures lodged by individuals in order to enforce their rights.

The case of Mr. and Mrs. Moon illustrates that a decision by which a person is refused entry, denied a visa or detained or expelled on the basis of a SIS alert may have human rights implications. It also illustrates that an SIS alert may infringe not only the human rights of the person who is registered in the SIS, but also of the persons who are residing in the country of destination and who have an interest to meet the reported person. This case concerned the right of freedom of religion, but case-law of the European Court of Human Rights (ECtHR) established that other human rights might be at stake as well when dealing with decisions of refusal of entry, expulsion or detention. These rights include the right of protection from torture or inhuman treatment (Article 3 ECHR), the right to liberty (Article 5 (4)), the right to family life (Article 8), the prohibition of discrimination (Article 14), freedom of speech (Article 10).[32]

The inclusion of the right to data protection as a fundamental right in Article 8 of the EU Charter of 2000 confirms that data protection is not merely a code of conduct, but an individual right to be considered independently of the right to private life as laid down in Article 7 of the EU Charter. Already in 2003, the Commission made clear that the incorporation of the right to data protection in the EU Charter gives added emphasis to the fundamental rights dimension of EC Directive 95/46 on data protection.[33] With the adoption of the Lisbon Treaty in December 2007, the EU member states confirmed the legally binding nature of the Charter of Fundamental Rights.[34] This means that when developing and implementing measures in the field of data processing, both EU institutions and member states should give due consideration to the impact

---

[30] An overview of case law in France, Germany and the Netherlands is given in Evelien Brouwer, *Digital Borders and Real Rights,* supra note 4.

[31] SCHAC 2502/08, p. 12 and p. 18.

[32] For judgements dealing with immigration law decisions in which the ECtHR found a violation of these rights see: *Čonka v. Belgium*, 5 February 2002, no. 51564/99, *Sen v. the Netherlands*, 21 December 2001, no. 31465/96, *Moustaquim v. Belgium*, 18 February 1991, no. 12313/86; *Maslov v. Austria* 22 maart 2007, no.1638/03, *Timishev v. Russia*, 13 December 2005, no. 55762/00, *Piermont v. France*, 27 April 1995, no. 15773-74/89.

[33] European Commission, first report on the implementation of the Data Protection Directive of 15 May 2003.

[34] See the Declaration concerning the Charter of Fundamental Rights of the European Union annexed to the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, *OJ* C306, 17.12.2007.

of those measures for the fundamental right to data protection. It is not unlikely that this right will play a more important role in future in procedures dealing with databases such as the SIS, but also the Visa Information System and Eurodac.[35] In this context, the extended registration and use of fingerprint data and other biometrics in the EU raise particular concerns. An important warning has been given by the Advocate General Trstenjak in his opinion to the case of *United Kingdom and Ireland against the Council dealing with the Regulation 2252/2004 on security features and biometrics in passports*. In a conclusion that was of no particular relevance to the issue raised in this case (whether the UK and Ireland could participate in this Regulation), Trstenjak explicitly referred to the problems that might arise from "the perspective of the fundamental right to protection of personal data when implementing this Regulation on biometric passports".[36]

Of course, human rights aside, other rights as protected in European law must be respected when using databases such as the SIS. Since the Amsterdam Treaty, different instruments have been adopted on the basis of Title IV of the EC Treaty. These instruments protect the rights of asylum seekers, long-term resident third-country nationals and third-country nationals who have the right to family reunification. More generally, in EU law, certain categories of 'privileged' third-country nationals gained extra protection, such as the family members of EU citizens, Turkish migrant workers or persons deriving rights from special agreements between the EU and third countries. There is an important tension between the rights of these persons and the possibility of being reported in the SIS for the refusal of entry. This tension became clear in the judgement of the ECJ in the case of the *Commission v. Spain*.[37] Here, the ECJ left no doubt about the fact that an automatic refusal of entry or a visa to a third-country national who is married to an EU citizen, solely on the basis of a SIS alert, violates the principle of free movement that is central to the communitarian system. By taking this negative decision without verifying whether the person concerned poses a genuine and sufficiently serious threat to the fundamental interest of society, the national authorities infringed the rights as laid down in Directive 2004/38.[38]

5.2 Tasks and responsibilities of national courts: Some proposals

What the case of Mr. and Mrs. Moon establishes is that the outcome of proceedings dealing with an SIS alert can be very different, depending on the country in which the appeal is lodged or the court considering the appeal. Where the German and Belgian courts showed an active and principled approach towards the lawfulness and proportionality of an SIS alert, the courts in France and the Netherlands refrained from a substantive assessment of the case. However, in these latter countries the national courts dealing with the Moon case also issued important decisions and rejected the formal approach of the national authorities limiting the rights of the complainants. In France, the Conseil d'État broadened the right to direct access to one's information. In the Dutch case, the courts rejected the formal reasoning of the Dutch administration on the basis of which the applicants could not start legal proceedings against an SIS alert, nor against the advance communication of the Immigration Office that the Moons would be refused entry when arriving at the Dutch borders.

---

[35] See the proposal for a Regulation concerning the Visa Information System (2004/0287 COD) and the Eurodac Regulation 2725/2000, 11 December 2000 (*OJ* L316, 15.12.2000).

[36] Opinion AG Trstenjak, 10 July 2007 in the case C-137/07, UK and Ireland v. Council, para. 126.

[37] Case C-503/03, *Commission v. Spain*, Judgement of the Court (Grand Chamber) of 31 January 2006.

[38] Adopted on 29 April 2004, *OJ* L 229/35, 29.06.2004.

The use of SIS I and SIS II (but also Eurodac and VIS) is based on the principle that authorities should respect and enforce the alerts entered by the authorities of other member states on the basis of the principle of 'mutual trust'. Where national authorities have no problem recognising and enforcing foreign SIS reports, they generally find it difficult to accept the binding force of decisions by foreign courts or data protection authorities. Based on the principle of sovereignty, it is held that national courts cannot assess the lawfulness of foreign administrative decisions. Iit should be clear, however, that the system as described above can only work if the principle of mutual trust between Schengen states is complemented by an active implementation of the principle of mutual enforcement of national courts' decisions dealing with SIS alerts. This principle follows from Article 111 (2) CISA and Article 43 (2) of the SIS II Regulation. Both courts and national authorities should be aware of the tasks and responsibilities required in order to enforce this principle. The enforcement of foreign judgements itself is to be based on mutual trust, and, hence, the lack of such enforcement should be considered as a lack of mutual trust.

Publication of national criteria to issue alerts

To raise awareness of this, different measures are possible. One of these is to find a mechanism in which national courts and authorities could improve their knowledge of the use of the SIS, but especially the criteria on the basis of which national administrations may issue an alert. For this aim, Peers suggested the introduction of a duty for member states to publish their national criteria for issuing alerts in the EU's Official Journal, or to submit their national criteria biannually to the European Commission.[39] This proposal could assist national courts assessing the lawfulness of the national criteria on which the SIS alert is based. However, a problem might occur where at the national level these criteria are often amended and therefore the information submitted could be out of date before it is published in the Official Journal. In future, it is necessary that the Commission use its power of Article 24 (5) of the SIS II Regulation "to achieve a higher level of harmonisation of the criteria for entering the alerts".

Cooperation and exchange of information between national courts

Another measure to assist courts when dealing with SIS alerts, is a system of a "preliminary transnational question" (*question préjudicielle transnationale*) proposed by Gautier.[40] According to this proposal, national courts could submit questions to courts in other member states on the meaning and content of their national law. In my view, this system of preliminary requests by national courts could be complemented by the establishment of one specialised coordination point within the court system in each member state. These coordination points would ensure that each request from a foreign court dealing with an SIS alert is dealt with in a timely and efficient manner. This procedure could be accompanied by appropriate time limits, ensuring a swift response by the authorities involved. Of course, the setting up of a European coordination network of national courts will meet with practical and organisational problems. The organisation of the SIRENE network for a coordinated use of SIS, however, shows that member states have been able to solve these problems for the executive powers. Within this network, national SIRENE bureaux serve as contact points for national authorities when dealing with an SIS alert and the issue of residence permits and visas. These bureaux operate 24 hours a

---

[39] Steve Peers, "Key Legislative Developments on Migration in the European Union: SIS II", *European Journal of Migration and Law*, 2008/1.

[40] M. Gautier, "Le dépassement du caractère national de la juridiction administrative française: le contentieux Schengen", *Droit Administratif*, May 2005, pp. 7 ff.

day, seven days a week and must respond within 12 hours of submission of the request.[41] It is unclear why a parallel mechanism could not be established for the judiciary.

Preliminary proceedings to ECJ

National courts dealing with SIS alerts on third-country nationals should be more aware of their right or even duty to lodge a preliminary reference to the Court of Justice in Luxembourg. Based on the principle of effective remedies, courts have a duty to ensure full application and uniform interpretation of Community law and to eliminate the unlawful consequences of a breach of Community law either directly or by ensuring effective compensation for the damage resulting from it.[42] The system of preliminary references guarantees a clear and coherent interpretation of Community law. On the one hand, the use of preliminary proceedings with regard to questions related to SIS requires the ECJ to analyse the legal problems under Community law submitted by national courts and to provide a generally applicable interpretation. On the other hand, it places an obligation on national courts to ensure that when an issue of Community law needs to be clarified, the issue is to be forwarded to the ECJ.

Considering the case of Mr. and Mrs. Moon, it could have been useful if the ECJ had been asked to give more clarity about, for example, the duty of national authorities (and courts) to make a full assessment of the interests at stake (including human rights), even if the underlying procedure concerns a foreign SIS alert. Also, the ECJ could have been asked for an interpretation of the criteria in Article 96 CISA (and in future Article 24 of the SIS II Regulation) or the scope of the individual right of access to information (Articles 109 CISA and 41-42 SIS II Regulation).

Active use of power to impose penalties

Article 49 of the SIS II Regulation obliges member states to ensure that any misuse of data entered into the SIS II or any exchange of supplementary information contrary to this Regulation is subject to "effective, proportionate and dissuasive penalties" in accordance with national law. To ensure that the rights of individuals are respected with regard to the storage and use of data held in the SIS, this new provision should be complemented with strict rules on the liability of the data holder or data user. This allows national courts or data protection authorities to impose sanctions when necessary. The Eurodac Regulation and the proposed VIS Regulation also include provisions on the duty of member states to impose penalties for the misuse of data.[43] These provisions will give individuals, and national courts, an important practical tool to remedy wrongful use of the information stored in these databases.

Evaluation of current rules and the need for more information

Article 43 (3) of the SIS II Regulation stipulates that the rules on remedies will have to be evaluated by the Commission by 17 January 2009. This evaluation should be used to strengthen the legal position of third-country nationals in the SIS II. Only by evaluating the current

---

[41] See the Sirene manual, revised version, *OJ* L 317/41, 16.11.2006, para. 1.4.5.

[42] John Temple Lang, "The Principle of Effective Protection of Community Law Rights", in David O'Keeffe, *Judicial Review in European Union Law*, The Hague: Kluwer Law International, 2000, pp. 136-138 and p. 235. See also Chapter 10 of Evelien Brouwer, *Digital Borders and Real Rights* (supra note 4).

[43] Article 25 Eurodac Regulation and Article 33 of the proposed VIS Regulation (version of 26 September 2007, PE-CONS 3630/07).

problems and legal obstacles national courts are confronted with, is it possible to develop an effective mechanism in order to safeguard an individual's rights in the Schengen area. For this purpose, national courts and data protection authorities should be actively involved by submitting information and case-law to the Commission to achieve more information on the current implementation of Article 111 CISA (and in future, Article 43 of the SIS II Regulation). To this end, lawyers, judges, officers and experts could be asked to forward the case-law they are acquainted with in a more systematic fashion.

5.3 Final remark

The recent proposals of the European Commission for a *European Border Management Strategy* are based on an almost blind faith in the use of large-scale databases, identification measures, and biometrics.[44] The Commission's "Border Package" of February 2008, includes the proposal of an entry/exit system, allowing the electronic recording of the dates of entry and exit of third country nationals into and out of the Schengen area. This entry/exit system would enable national authorities to identify overstayers and "take the appropriate measures".[45] Another proposal of the Commission includes the introduction of automated gates for "bona fide or registered travellers" enabling "the automated verification of travellers' identity without the intervention of border guards". A machine will read the biometric data contained in the travel documents or stored in a system or database and compare them against the biometrics of the traveller, "accelerating border checks by creating automated separate lanes replacing the traditional control booths". Persons will be granted "Registered Traveller" status after appropriate screening on the basis of common vetting criteria, including a reliable travel history (no previous overstays; data to this effect can be retrieved from the entry/exit system), proof of sufficient means of subsistence, and holding a biometric passport.

It is clear that these measures entail a risk to the protection of human rights such as the right to privacy and the right to data protection, but also to the freedom of movement of persons and the principle of non-discrimination.[46] Furthermore, there are serious doubts about the necessity, efficiency, and proportionality of these measures.[47] The current use of the SIS for immigration law purposes has already established that it is extremely difficult for individuals and their lawyers to remedy a false or unlawful SIS report. The Commission's proposals for further "automated decision making at the borders" will undoubtedly increase the problems of individuals seeking legal redress against negative decisions. Considering the case of Mr. and Mrs. Moon, whose alert was finally deleted after 12 years of proceedings, one must be aware that they were privileged by the support of the international network of the Unification Church and a team of experienced lawyers. In the European Union, however, the enjoyment of one's fundamental rights and liberties should not be dependent on one's network or financial status.

---

[44] See the Commission's Communication on *Examining the creation of a European Border Surveillance System (EUROSUR)* and the Communication on *Preparing the next steps in border management in the European Union* COM (2008) 68 resp. COM (2008) 69, 13.2.2008.

[45] COM (2008) 69, pp. 5-6.

[46] See on the relation between the use of biometrics and these rights, E. Brouwer: "The use of biometrics in EU data bases and identity documents. Keeping track of foreigners' movements and rights", in Juliet Lodge (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers, 2007.

[47] See the conclusions in the Impact Assessment Report annexed to the Border Package. See also Elspeth Guild, Sergio Carrera and Florian Geyer, *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No. 154, CEPS, Brussels, March 2008 (http://shop.ceps.eu/BookDetail.php?item_id=1622).

References

Commission's Communication on *Examining the creation of a European Border Surveillance System (EUROSUR)* and the Communication on *Preparing the next steps in border management in the European Union* COM (2008) 68 resp. COM (2008) 69, 13.2.2008. Council Decision 2007/471 of 12 June 2007, *OJ* L179/46, 7.7.2007.

Council document 5441/08, 30 January 2008 SIS Database Statistics dd. 01/01/2008.

Council document 6178/07, 13 February 2007 SIS Database Statistics dd. 01/01/2007.

Declaration concerning the Charter of Fundamental Rights of the European Union annexed to the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, *OJ* C306, 17.12.2007.

Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L281, 23.11.1995.

Elspeth Guild, Sergio Carrera and Florian Geyer (2008), *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No. 154, CEPS, Brussels, March (http://shop.ceps.eu/BookDetail.php?item_id=1622).

European Commission, first report on the implementation of the Data Protection Directive of 15 May 2003.

Evelien Brouwer (2007), "The use of biometrics in EU data bases and identity documents. Keeping track of foreigners' movements and rights", in Juliet Lodge (ed.), *Are you who you say you are? The EU and Biometric Borders*, Nijmegen: Wolf Legal Publishers.

Evelien Brouwer (2008), *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, series *Immigration and Asylum Law and Policy in Europe* (dissertation Radboud Universiteit Nijmegen, 2007), ISBN: 978-90-04-16503-8.

House of Lords European Union Committee, 9th Report of session 2006-07, *Schengen Information System II. Report with Evidence*, HL Paper 49, London: The Stationery Office Limited, published 2 March 2007.

John Temple Lang (2000), "The Principle of Effective Protection of Community Law Rights", in David O'Keeffe, *Judicial Review in European Union Law*, The Hague: Kluwer Law International.

Joint Supervisory Authority, Report of 18 January 2008 concerned the use of Article 99 alerts in the SIS, SCHAC 2501/08.

Joint Supervisory Authority, Report of 18 January 2008 on a survey of the implementation of Article 111 of the Schengen Convention, SCHAC 2502/08.

M. Gautier (2005), "Le dépassement du caractère national de la juridiction administrative française: le contentieux Schengen", *Droit Administratif*, May, pp. 7 ff.

Schengen Borders Code or Regulation 562/2006, 15 March 2006, *OJ* L105, 13.4.2006.

Steve Peers (2008), "Key Legislative Developments on Migration in the European Union: SIS II", *European Journal of Migration and Law*, No. 1.

About CEPS

Founded in Brussels in 1983, the Centre for European Policy Studies (CEPS) is among the most experienced and authoritative think tanks operating in the European Union today. CEPS serves as a leading forum for debate on EU affairs, but its most distinguishing feature lies in its strong in-house research capacity, complemented by an extensive network of partner institutes throughout the world.

Goals

- To carry out state-of-the-art policy research leading to solutions to the challenges facing Europe today.
- To achieve high standards of academic excellence and maintain unqualified independence.
- To provide a forum for discussion among all stakeholders in the European policy process.
- To build collaborative networks of researchers, policy-makers and business representatives across the whole of Europe.
- To disseminate our findings and views through a regular flow of publications and public events.

Assets

- Complete independence to set its own research priorities and freedom from any outside influence.
- Formation of nine different research networks, comprising research institutes from throughout Europe and beyond, to complement and consolidate CEPS research expertise and to greatly extend its outreach.
- An extensive membership base of some 120 Corporate Members and 130 Institutional Members, which provide expertise and practical experience and act as a sounding board for the utility and feasability of CEPS policy proposals.

Programme Structure

CEPS carries out its research via its own in-house research programmes and through collaborative research networks involving the active participation of other highly reputable institutes and specialists.

Research Programmes

Economic & Social Welfare Policies
Energy, Climate Change & Sustainable Development
EU Neighbourhood, Foreign & Security Policy
Financial Markets & Taxation
Justice & Home Affairs
Politics & European Institutions
Regulatory Affairs
Trade, Development & Agricultural Policy

Research Networks/Joint Initiatives

Changing Landscape of Security & Liberty (CHALLENGE)
European Capital Markets Institute (ECMI)
European Climate Platform (ECP)
European Credit Research Institute (ECRI)
European Network of Agricultural & Rural Policy Research Institutes (ENARPRI)
European Network for Better Regulation (ENBR)
European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)
European Security Forum (ESF)

CEPS also organises a variety of activities and special events, involving its members and other stakeholders in the European policy debate, national and EU-level policy-makers, academics, corporate executives, NGOs and the media. CEPS' funding is obtained from a variety of sources, including membership fees, project research, foundation grants, conferences fees, publication sales and an annual grant from the European Commission.

E-mail: info@ceps.be
Website: http://www.ceps.be
Bookshop: http://shop.ceps.be

CENTRE FOR EUROPEAN POLICY STUDIES

Place du Congrès 1 • B-1000 Brussels
Tel: 32(0)2.229.39.11 • Fax: 32(0)2.219.41.51