Statewatch analysis:
The dream of total data collection
- status quo and future plans for EU information systems

The broad use and the extension of EU information systems in the field of policing and especially policing of immigration is a clear indication of the EU growing together - but in a way that is not desirable.

Justice and home affairs policy in the EU is about to make a technological quantum leap: the second generation Schengen Information System (SIS II) was expected to go online in 2007. The new system marks a generational change, not only in terms of the technology it uses but also in terms of the data it contains. Biometrics has now become a central component of EU police data systems and the Commission is already planning "interoperability" with other systems: namely, with the Visa Information System (VIS) which was also expected to go online in 2007, and with Eurodac, the database which has been used since 2003 to collect and compare fingerprints of asylum seekers at the EU level. In November 2005, Europol started its "information system" and thereby finalised - for the time being - its information technological instrument.

Only 25 years ago, it would have been unthinkable that data collection would exceed the national framework. This was not only due to technical but also political barriers. The first attempt to introduce such as system for Interpol failed in 1981 on grounds of sovereignty questions and a lack of trust towards the professional standards of the National Central Bureaux of particularly Third World countries.

In comparison, the SIS, for which the concrete planning began in 1988, could build on a political framework. At first, on that of the Schengen Group and from 1999 onwards, on that of the EU, with the coming into force of the Amsterdam Treaty. In March 1995 it went online, initially only for then seven participating states. Currently, 15 states are connected, namely, the "old" EU Member States excluding the UK and Ireland and including the non-EU states Norway and Iceland.

The first step - the SIS

The fact that the development of EU police data systems started with a system for wanted persons and objects such as the SIS is no coincidence: Wanted persons/objects systems are "hit/no hit" systems which only allow for simple queries. They indicate if data on a relevant person or object exists or not. Data entries in the SIS are (as yet) very small. Next to details on identity, personal data entries merely contain the specification of the alerting authority and the reason for the alert, as well as a possible indication "violent" or "armed". The exchange of background information relating to the alerts - in case of a "hit" - takes place outside of the SIS via the SIRENE national contact points that are located in the national police centres - in Germany, for example, in the Federal Criminal Investigation Bureau (Bundeskriminalamt - BKA).

At the same time, alerts are data which should be broadly available within police organisations so that the basic police forces - i.e. officers controlling at the borders and inland - can take relevant law enforcement measures. Altogether 30.000 terminals were connected to the SIS within the EU in 1995. Today, the number of German terminals connected alone, exceeds this number considerably: the Federal Police (the renamed Border Guard) and customs have around 1.700 stationary and mobile terminals at their disposal at the borders. In addition, SIS data can be accessed to a large extent through the working place computers connected to INPOL (the central police data system in Germany). As a recent parliamentary question by Linkspartei MPs (the Left-Wing Party) revealed, this amounts to "approximately" 10,500 computers located with the Federal Police and customs. There are no figures concerning the regional police forces. (1)

Alerts for objects - such as bank notes (registered notes), arms, vehicles, identity papers and blank documents - massively dominated the SIS from its initiation. Explanatory remarks on alerts for the years 2003 and 2006 (table 1) show that their share in the total figure has increased again. Identity papers show an above-average increase in the database.

At first sight, data entries relating to persons appear not have changed much. The total number of persons seems to have increased only marginally since 2003. What has remained is the disproportionate amount of alerts issued on grounds of Article 96 of Schengen Implementation Agreement (SIA) in respect of third country nationals for the purpose of refusing entry (in 2003 this was 89 per cent, in 2006 it is 85.2 per cent of person records).

Differences to 2003 only appear when considering which states issue alerts: the German contribution to Article 96 data has been disproportionately high since 1995. With almost 270.000 alerts in 2003, Germany then already "owned" more than 23 per cent of all entry bans in the SIS. When questioned by the German civil liberties journal *Bürgerrechte & Polizei/CILIP* about the fact that this figure had fallen by more than 100.000, the Bundeskriminalamt (BKA) replied this was due to the accession of Central and Eastern European states in May 2004. The accession meant that citizens of these states could no longer be entered in the SIS database for the purpose of refusing entry. Italy is now the front-runner with regard to this data category: with 378,381 persons it is responsible for almost half of all Article 96 data.

First and foremost, the SIS therefore remains an electronic instrument for border control and not one of police investigation in the normal sense. Since the SIS came online, alerts issued under Article 95 SIA for arrest and extradition (which requires an international (or EU) arrest warrant) never reached 2 per cent of all data relating to persons. The number of persons entered under Article 98 for judicial purposes (wanted to appear in court as witnesses or accused of petty crime) is now three times higher

than the number of alerts issued for the purpose of arrest. The SIS therefore indicates an altogether low crime rate.

In comparison to 2003, the number of people entered for the purpose of police "observation" ("discreet surveillance") has doubled. This measure is devised, under Article 99 SIA and also in German police law, as a preventative action. This means the persons in question are not accused of a crime, nor are they necessarily under concrete suspicion. A police prognosis that holds that if the person in question will commit a crime in future is enough grounds for inclusion in the database. In case of a police check, the circumstances, identity of fellow passengers etc. are to be reported to the issuing authority. It is not possible to deduce from the statistics the number of "observations" which are possibly entered in the database. When questioned about the increase of Article 99 alerts, the BKA gave the succinct yet circular reply that the increase was because they had used it more often. This "increased use" is presumably a consequence of the "fight against terrorism" which generally starts long before a concrete suspicions exist. According to Article 99 SIA, intelligence services are also entitled to issue surveillance alerts, as far as national law allows them to. With its new Anti-Terrorism Amendment Act, the Bundestag has granted this power to the German intelligence services. (2) The present statistics do not show if other states are currently using Article 99 in this way or not. In 2003, only 5 cases were recorded.

The statistics on "hits" (table 2) do not show all "successful" controls but only the hits that police of Schengen states had inside the EU on the basis of an alert issued by another Schengen state. This means that if officers come across an alert issued by their own state, it is not counted. The statistics do, however, provide a picture of how control strategies connected to the SIS work on the ground.

First of all, it becomes clear that most of the successful checks concern persons from non-EU states. The extremely high "hit" rates in the years 2002 and 2003 are, according to the BKA, explained by the fact "that a Member State practiced a deviating procedure of data collection during this period". Which state exactly this was, the BKA did not want to disclose. Still, when looking only at the validly collected data from the years 2001, 2004 and 2005, the fact remains that around a third of all SIS related arrests are entry refusals. The reasons for this are to be found not only in the high number of data entries in this category but also in the increase of control measures applied against immigrants in the EU.

Second step: the SIS of customs authorities

Similar to the SIS supporting police controls (of persons) at the external borders and in the common "investigation area", a Customs Information System (CIS) intends to facilitate goods control in the internal market. At least this was the argument used during the first negotiations on the legal basis of the CIS. In 1995, justice and home affairs ministers signed the Convention "on the use of information technology for customs purposes". In 1997, a Regulation followed on mutual assistance between administrative authorities.(3) The latter was drafted with view to the application of EU law on customs and agricultural matters. The Convention, however, relates to cooperation in the area of criminal matters relating to customs and therefore to the unlawful import or export of goods (including, for example, illegal drugs and arms). In technical terms, the Convention and Regulation use two different systems, which are connected through a common search engine. Both are located with the Commission, or rather the European Anti-Fraud Office OLAF, and they are accessible from national customs authorities. Because of, amongst other things, the slow ratification process of the Convention, the CIS went live only in March 2003. The current OLAF activity report says that "over 3,000 users located in the main ports, airports, border posts, risk analysis services, investigation and intelligence services" are connected to the CIS through the terminals of the AFIS (Anti-Fraud Information System). It is reported that the CIS handled 16.000 search requests during the activity period (mid-2004 to the end of 2005). But the OLAF team is not content and finds the "initial level of use of the CIS by national authorities has been disappointing". At the end of 2004, only 140 cases were registered in the database, by the end of 2005 it had risen to 537.(4)

The CIS allows for alerts on goods, transport vehicles, companies and persons. As in the first generation SIS personal data entries in the CIS are relatively short. Next to names, date of birth etc., entries can specify "objective and permanent characteristics", a warning note with regard to violent behaviour, carrying of arms or danger of flight, the license plate number of the vehicle as well as the reason for the alert and the proposed action to be taken in case of a "hit". The latter concerns, next to "recording and informing" – eg: arresting or confiscating a person or goods - "secret registration", that is police or customs surveillance. This measure can be applied to persons as well as arms, vehicles and containers. Whilst this alert category plays a quantitatively minor role in the SIS, in takes first place in the CIS.

With a Protocol to the Convention on the use of information technology for customs purposes, the EU complemented the CIS by creating a customs files identification database for grave customs violations (FIDE – Fichier d'identification des dossiers d'enquêtes douanières) which is planned to go live in November 2006.(5) The data entered covers the following categories: the field covered by the investigation file, the file number, the name, nationality and the contact information of the Member State's authority handling the case. With regard to personal data, the 'customs files identification database' can hold the names of persons and companies who are suspected of committing a serious infringement of national laws, or who have been "the subject of a report establishing that such an infringement has taken place" or who have been the subject of an "administrative or legal sanction for such an infringement". Data relating to current investigation files can be stored up to three years. When it has been "established" that an infringement has taken place, data can be stored up to six years and data retention is granted for a period of ten years in case an investigation file has led to a conviction or a fine.

Third step: "Intelligence" with Europol

In July 1995, the justice and home affairs ministers signed the Europol Convention, which extended the remit for the Europol agency to hold personal data. "The Europol Computer Systems" (TECS) were to be comprised of three parts: firstly, an "information system", that is a register on persons and cases relating to the remits of the authority, with national police forces entering and searching data. Data here refers to convicted and suspected persons as well as "persons who there are serious grounds for believing will commit criminal offences for which Europol is competent". The "information system" therefore unites convicts, suspects and not-yet-but-soon-to-be suspects.

The second component intends to represent the actual added value of the Europol agency: "work files for the purposes of analysis", to be held for a limited time period and function as a working instrument for analysis groups. Access to the data held therein was only to be given to the relevant participating national experts and liaison officers. The range of persons to be entered is accordingly broad: next to convicted persons, suspects and the above-named not-yet suspects, these work files also hold details on witnesses, potential witnesses, victims, potential victims, contacts and associates as well as "persons who can provide information on the criminal offences under consideration". In

other words, Article 10(1) of the Convention lays down that anyone who the police officers believe to be of any interest to them at all, can be entered in the files. Finally, the third component is an index system "for the data stored on the files referred to in Article 10(1)".

When Europol, after the ratification of the Convention in 1999, lost its provisional status of a "Europol Drugs Office" and officially started its operations, an "interim system" with work files came into operation. In December 2004, the authority operated 19 of the files, altogether hold the data of 146,143 persons.(6) Around 10,000 people were registered in the work file "Islamic terrorism", 22,500 were registered in a file on Turkish, and around 14,000 in a file on Latin American organisations involved in drugs trade. Data on 3,200 persons were held in a file on the smuggling of Indian citizens. 2,200 persons were registered in a file on the illegal immigration of Iraqi Kurds, which was created whilst the US was still bombing the country. The biggest work file, with tips from financial institutions on financial transactions pointing to money laundering and cross border cash transfers unites information on over 68,870 persons. Considering the open definitions contained in the Convention, this high number of registrations in the work files was to be expected. Whether this mass suspicion, however, will actually lead to concrete investigation results is very questionable.

According to the current activity report, the agency operated 18 work files at the end of 2005: three on the drugs trade, three on "crimes against persons", five on financial and property crime, four on "organised crime groups", two on terrorism and one on forgery of money.(7) The agency refuses to disclose the number of registered persons, however, the report notes that the amount of data provided by the Member States has increased during the activity period.

Europol only started operating the information system in October 2005. Initially, only three of the 25 Member States were involved: Sweden, France and Germany. No detailed information on this matter has been published so far.

Fourth step: with Eurodac towards less asylum

In 1991, the "ministers responsible for immigration" announced their intention to create a common information system for the comparison of fingerprints of asylum seekers. One and a half years before, they had signed the Dublin Agreement: consecutive asylum applications in the EC/EU - in official jargon: "abuse of the asylum system" or "asylum shopping" - was thereby supposed to be prevented. The Agreement, which came into force only in 1997 and was replaced by a Regulation in 2002, regulates the procedure by which the state responsible for handling an asylum claim is determined.(8) In the best case scenario, this would be the state which the asylum seeker first entered. In practice, it is the state in which a person first lodges an asylum application. The "not responsible" state can deport the person in question back to the "responsible" state.

The realisation of Eurodac, however, necessitated an additional legal basis because the Dublin Agreement did not foresee an automated data comparison system. In 1998, a final draft of a Eurodac Convention was presented, which was transformed into a Regulation after the coming into force of the Amsterdam Treaty.(9) Like all automated fingerprint identification systems (AFIS), Eurodac registers "no personal details such as name, but relies on a biometric comparison, which represents the most secure and precise identification method".(10) However, this reassurance offered in the press release of the European Commission, which operates the system, has little to do with data protection. The dactyloscopic data (dactyloscopy = fingerprint identification) are entered together with a reference number and can therefore always be allocated to personal data contained in an asylum application.

Fingerprints of all asylum seekers from the age of 14 onwards are registered in the Eurodac database and compared with already existing data. The fingerprints of those who are apprehended crossing borders illegally or residing without a residency permit within the EU are only compared but not retained. In cases of "apprehension" the comparison is aimed at establishing whether a “sans-papiers” has already applied for asylum in another Member State (and therefore can be deported back to that state).

On 15 January 2003, Eurodac went online. The result of the first two years is evaluated by the Commission and by the Member States as a success. During the first year (15.1.03-15.1.04), Member States transferred 246,902 data entries of asylum seekers to the Commission's Eurodac central unit. Seven per cent of the newly registered persons had already lodged an asylum application in another Member State. In addition, 7,857 people were "apprehended" at the border and 16,814 inside the EU. Because Eurodac started as an empty database, this was a significant result - so the Commission celebrated itself in its annual report. During the second activity year (the whole of 2004), the central unit received 232,205 data entries and achieved 13 per cent duplicate or multiple applications. Despite the increase in persons "apprehended" (16,183 at the border, 39,550 inland), the Commission still complained that Member States were neglecting their tasks in this area.(11)

The German Federal Office for Migration and Refugees (BAMF) also compliments its own achievements. Because of Eurodac, the number of requests for "responsible" states to take back asylum seekers had increased and secondly, the "evidence" had improved: the alerts issued by Germany had increased from 1,249 in 2003 to 6,939 in 2004. Since July 2004, the percentage of applications related to Eurodac "hits" reached over 50% and an "increasing tendency" can be detected.(12)

The fact that Eurodac is working is also known by refugee organisations. They report that refugees who already applied for asylum in another Member State were now being deported back to Member State that do not or only minimally guarantee support for traumatised persons.(13) Furthermore, the risk of chain deportations back to the torturing state is growing. In many cases, the Dublin's "one chance only" rule means practically "no chance at all".

Although 12 years passed since the ministers' first declaration of intent for the creation of Eurodac, it is a fact that the EU's repressive asylum policy has led to the first modern biometric database. From the start, the police had a vested interest in using such a database beyond the area of asylum.

Fifth step: Biometric control thanks to SIS II and VIS

At the end of the 1980s, when the plans for the existing SIS were first drafted, the Schengen group comprised five states. The system was therefore initially only created for connecting eight states. When in 1998, the Nordic states were connected, the SIS had to be updated to an “SIS plus”. Already by December 1996, the Schengen Executive Committee had toyed with idea of a second generation SIS (SIS II). The planning for such a system started in 2000 but gained an additional impetus after 11 September 2001. The SIS II, which is to go online in 2007, not only offers new technological functions, but it will also fundamentally change the police practice based on the system. Some changes relating to the existing SIS will already come into force in October and November this year.(14) On 31 May 2005, the Commission presented two draft Regulations on aspects of the system relating to the EU's first pillar (external borders, visa policy, etc.) as well as one draft Council Decision for the third pillar (police matters in the strict sense of the word).(15)

In June 2006, the Council finished its internal debate.(16)

The regulations, however, will have to be adopted by the European Parliament. The co-decision procedure in principle would have given a significant power to the parliament, to introduce not only better data protection, but also a different policy regarding the rights of non-EU-citizens – mainly affected by the existing SIS. The EP, however, accepted from the start the calendar set up by the Council and the Commission. According to that, the SIS II was supposed to be ready in March 2007 and should go online in October of the same year. This would have also been the date for the full integration of the ten states who had entered the EU in 2004, into the group of Schengen users, including the lifting of controls on persons at the borders to and between these new member states. The latter was the official reason, why the EP once again agreed into a secret trialogue procedure without any chance for a public dabete, which led to a false "compromise" with the Council in September 2006 and the adoption of the whole SIS II-package at first reading at 25 October 2006.

This is even more annoying as the time table presented by the Council and the Commission has proved unrealistic – a fact which was evident at least since the summer of 2006. It suffered from technical and organizational problems. In 2005, the Commission even had to stop the whole process of the construction of the SIS II due to a decision of the European Court of first instance in a legal row with one of the companies which did not succeed in the submission process.

In summer 2006, the Council began to work on a second plan. The Portuguese Ministry of the Interior presented a feasibility study for a "SISone4all", a once again updated version of the existing SIS, which will include also the access by the ten new member states. According to the new time table, the "SISone4all" shall be ready for the loading of data in June 2007. After another evaluation, internal border controls at land and sea borders of the ten new member states shall take place in January 2008 and at the airport at the end of March.

Thus, the SIS II is now calculated to go online in 2009, three years after its legal fundaments have been adopted in a needless and undemocratic fast track procedure. The results of that procedure are as follows:

- The alert categories will be differentiated and extended: alerts for arrest (up to now Article 95 SIA) will now relate to the European Arrest Warrant. Entry bans (up to now Article 96 SIA) will be separated into "restrictive measures" on grounds of danger for "public security" or "internal security" (e.g. entry bans issued after a conviction has been made) and "purely" aliens law related removal orders (e.g. from rejected asylum seekers). Alerts can also be issued on "vehicles, boats, aircrafts and containers" for the purpose of "discreet surveillance". For the purposes of seizure or use as evidence in criminal proceedings (formerly Article 100 SIA), alerts can be issued on trailers and caravans, driving licenses and visas, vehicle registration certificates and vehicle number plates as well as banknotes, securities and means of payment. A new alert category on "violent offenders" as it has been discussed for a while is as yet not included.

- The data retention period will be extended: up to now, data related to discreet surveillance had a "conservation period" of one year, all other data could be kept for three years. In the SIS II, after one year in the case of alerts for discreet surveillance and after three years for all other alerts on persons, there will be an examination, to see if the data still are needed. If the respective member state thinks that this is the case, the storage period is prolongated for the same time. The introduction of an obligatory examination is the only point where the EP got a slight success. The original proposal of the commission wanted a conservation period of five years for data on discreet surveillance and ten years for the rest of alerts on persons. The extension of storage periods will necessarily lead to a massive increase of data contained in the SIS.

- Alerts can be linked. Although the SIS will remain a hit/no-hit system, it will have an, albeit limited, possibility to carry out investigative actions through the linking of data.

- More authorities will be able to access SIS data, even if it is specified which data certain authorities can access. These are Europol, Eurojust and the national public prosecutors, or rather, prosecutor's offices (alerts on persons wanted for arrest), surveillance and judicial procedure (witnesses and accused), immigration authorities (alerts for the purpose of refusing entry), Vehicle Licensing Agencies (alerts on vehicles).

- Alerts relating to persons will contain biometric data in future, namely, pictures and fingerprints. This will particularly apply to non-EU citizens, because asylum seekers and, with the creation of the Visa Information System (VIS), also visa applicants are subjected to fingerprinting and photographing.

The already dominant function of the SIS as a control instrument of citizens from non-EU states receives even more importance with the parallel creation of the VIS. Both systems will be run on the same technical platform. Further, the "wanted persons/objects system" SIS II can be accessed by consulates issuing visas as well as by immigration authorities, whilst the police on the other hand will get access to the VIS. The VIS will be linked to 27 Member States and, currently, three associated states. This implies at least 12.000 VIS users and 3,500 consulates connected worldwide.(17) The feasibility study of the Commission reckoned with 20 million visa applications annually. With a retention period of five years, this implies a volume of 100 million data entries.

The VIS is to contain on the one hand alphanumerical data: the personal identification data (names, date of birth etc.) of visa applicants, type and number of travel document, if applicable, details on the invitee or inviting company, details on earlier applications, including their positive or negative results, extension of stay etc. and the reasons for the same as well as the "status" of the processing of the claim by consulates and national "visa authorities" and, finally, the number of the visa sticker to be applied in the passport. Next to this, the entry will contain biometric data (digitalized photos and fingerprints).

The collection of data will be carried out by the relevant consulates, who will also have the remit to run common visa authorities or to outsource parts of the issuing process of visa it to private companies.(18) The VIS is an instrument that serves the EU's restrictive visa politics, created with the intention to stop "visa shopping" and "abuse" of the system. Access, however, is also granted to immigration authorities, "for the purpose of identifying third country nationals staying illegally in the territory in order to enforce a return decision or removal order" and the asylum authorities for the purpose of identification and the determination of the Member State responsible for examining an asylum application.

The VIS is also to serve police functions. This means first, it can be used for controls at the external borders and inland. VIS and SIS II will therefore lead to a fundamental increase in repression and restrictions for non-EU citizens. Up to now, "third country nationals" had to undergo at least a check of the passport and visa as well as a search request on them in the SIS. Now the controlling officers will run an additional search request in the VIS on visa related data. Following the wishes of the Council and the Commission, this data will not be searched on the name, but the fingerprints should be the decisive search criterion. The Commission justifies this in its Communication "on improved effectiveness, enhanced interoperability and synergies among European databases" with the argument that an alphanumerical search with data as large as contained the VIS database would result in "long 'hit' lists", which must then be "verified through a labour-intensive process that is sometimes impossible to perform in a border-control environment". The use of biometric searches would allow for "unprecedented accuracy", says the Communication.(19)

The European Parliament (EP), which agreed in principle to the collection of biometric data for the SIS II as well as for the VIS, now practices damage control with regard to the use of such data, based on the critical statements of data protection officers. According to the EP, police should request VIS data via the number of the visa and only use fingerprints as search criteria if a request through the number is not possible or when they have doubts as to the authenticity of identity papers.(21) This doubt, however, has been the basis of border police practice for years now. The proposed regulation is therefore nothing but a fallback position and it is moreover questionable if the EP will be able to maintain this position in the face of the existing time pressure.

In the case of the SIS II, The EP had already drawn back. The original commission proposal on the SIS II did not contain such a practice of biometric controls. In its revision of the Commission proposal, the Council states that "as soon as technically possible, fingerprints can also be used to identify third country nationals on the basis of their biometric identifier".(20) The EP accepted this version – in clear terms, this compromise means, that biometric controls on the basis of fingerprints are only to be used, when they are technically possible!

Border control, however, is not the only policing purpose the two new systems will serve. Access will also be given to the internal security authorities, which means to political police forces and internal intelligence agencies. For the SIS II this was included in the commission`s orginal proposals for the articles 17 of the regulation and 37 of the council decision. The Council for the moment withdraw these provisions in its negotiations with the EP on the adopted SIS II package. The Council, however, already, announced the need for additional legislation on this subject.

The model for this is the Commission's proposal for a Council decision on the access of Europol and the "national authorities responsible for internal security" to the VIS, presented in November 2005. According to this, the agencies shall access the VIS via central access points located in each member state and at The Hague for Europol. (22) Access, says the proposal, is necessary for the purpose of the "prevention, detection or investigation of terrorist offences or other serious criminal offences" and in each individual case, a written or electronic request must be submitted to the central access point, justified on "factual indications". Further, access requests must relate to a "specific event determined by date and place, or to an imminent danger associated with crime, or to a specific person in respect of whom there are serious grounds for believing that he or she will commit terrorist offences or serious criminal offences or that he or she has a relevant connection with such a person" (Article 5). In May 2006, the Police Working Group of the Council at least showed awareness of the fact that this definition of internal security authorities could also encompass intelligence agencies. This awareness, however, had disappeared by the time it published its preliminary consultation report from the beginning of August 2006.(23) Every Member States is to decide which authorities should be authorised to access the VIS and moreover, they should have "fast and practical", that is direct access to VIS data. The Council is not interested in requests and justifications.

The Commission is hardly going to oppose these demands. In its Communication on the efficiency and interoperability of EU data systems, it advocates that authorities responsible for combating crime and terrorism get access not only to the VIS but to all data held in the SIS II (that is not only to judicial or police alerts relating to arrest and surveillance) and Eurodac. It also calls for a European criminal Automated Fingerprints Identification System (AFIS). Moreover, the Commission proposes the creation of an "entry-exit system", to "ensure that people arriving and departing are examined and to gather information on their immigration and residence status". Whereas Germany, when introducing the new passports resisted the construction of a central biometric passport register, the commission now calls for the creation of a European passport register to improve the identification of EU citizens as well. This will be the last step towards the implementation of biometric control. What will soon be reality for third country citizens, is already becoming a tangible reality for EU citizens as well.

Heiner Busch
(Statewatch bulletin, vol 16 no 5/6: an updated article that first appeared in Bürgerrechte & Polizei/CILIP 84 (2/2006)

Footnotes

1 German Parliament publication, BT-Drs. 16/1044, 24.3.2006.

2 Documented on www.cilip.de/terror/gesetze.htm. cf. comment on this law in Bürgerrechte & Polizei/CILIP 85 (3/2006)

3 Convention on the use of information technology for customs purposes (OJ C 316 of 27.11.1995) and Council Regulation on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters (OJ L 82 of 22.3.1997).

4 EU Commission, OLAF: Sixth Activity Report for the period 1 July 2004 to 31 December 2005, Brussels 2006, p 57.

5 Council Act of 8 May 2003 drawing up a Protocol amending, as regards the creation of a customs files identification database, the Convention on the use of information technology for customs purposes (OJ C 139, 13.6.2003).

6 Reaction to the reply of the German government to the question by the PDS MP Petra Pau during parliamentary question time on 24.9.2003. See Bürgerrechte & Polizei/CILIP 77 (1/2004), pp 90-92.

7 www.europol.eu.int/publications/ar2005/EuropolAnnualReport2005.pdf.

8 Convention: OJ C 254, 19.8.1997, Dublin II Regulation: OJ L 50, 25.2.2003.

9 Council Regulation of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (OJ L 316, 15.12.2000).

10 Press release of the European Commission, 14.1.2003, IP/03/37.

11 See the Commission's annual reports SEC (2004) 557, 5.5.2004 and SEC (2005) 839, 20.6.2005.

12 BAMF: Statistik Migration und Asyl, www.bamf.de/cln_043/nn_564242/DE/DasBAMF/Statistik/statistik_node.html_nnn=true.

13 See, for example, Langthaler, H. (Asylkoordination Österreich): Schub und Recht, in: Solidarité sans frontières 2005, Bulletin 3, p 4.

14 Council document 11336/06, 20.7.2006 and 11337/06, 17.7.2006.

15 Com (2005) 230, 236 and 237 final, all from 31.5.2005.

16 Council document 5709/6/06, 6.6.2006.

17 Com (2003) 771 final, 11.12.2003.

18 See the proposal from the Commission on amending the Common Consular Instructions: Com (2006) 269 final, 31.5.2006.

19 Com (2005) 597 final, 24.11.2005; see the approving statement by France and Spain, Council document 9680/06, 22.5.2006.

20 Council document 5709/6/05, 6.6.2006 - new Article 14c.

21 Compare the synopsis of the versions from Commission, Council and EP, Council document 11632/06, 13.7.2006.

22 Com (2005) 600 final, 24.11.2005.

23 Council document 9199/06, 11.5.2006 and 11405/06, 3.8.2006.

Tables 1 and 2 on following page

Table 1: Persons and stolen/missing objects in the SIS

Article/Reason		SIS total 2006	German data 2006	SIS total 2003	German data 2003
95	Arrest	15,460	4,400	13,826	4,155
96	Entry ban	751,954	162,294	775,868	269,359
97	Missing	39,011	2,377	33,581	2,246
98	Wanted in court	45,189	1,414	34,379	2,752
99	Surveillance	31,013	1,104	16,378	544
	Missing persons	882,627	171,590	874,032	279,056
100	Bank notes	252,442	141,808	380,710	208,500
100	Blank documents	403,900	184,266	265,929	141,514
100	Firearms	297,021	103,225	301,348	143,966
100	Identity documents	11,353,906	1,789,271	7,687,008	1,514,427
99/100	Vehicles	1,472,531	131,947	1,106,626	150,217
	Missing objects	13,779,800	2,350,477	9,741,511	2,158,624

Source: BT-Drs. 16/1044, 24.3.2006; BT-Prot. 15/62. 24.9.2003

Table 2: "Hit" statistics

Article/Reason	2001	2002	2003	2004	2005
95-arrest	1,398	1,486	1,497	1,873	1,935
96-entry ban	15,971	25,537	23,328	12,707	11,594
97-missing persons	1,020	1,028	999	1,115	1,258
98-wanted to appear in court	1,896	2,169	2,091	2,535	3,582
99-persons under surveillance	1,138	1,156	1,253	1,579	2,236
Persons total	**21,423**	**31,373**	**29,170**	**19,809**	**20,605**
99-Vehicles under surveillance	136	168	202	318	328
100-vehicles	7,996	7,755	7,057	6,871	5,827
100-Firearms	143	133	137	158	141
100-Blank documents	1,853	1,928	1,653	1,564	1,565
100-Identity papers	2,853	3,616	3,279	3,022	3,193
100-bank notes	2.863	6	7	7	4
Objects total	**13,991**	**13,606**	**12,317**	**11,980**	**11,058**
"Hits" total	**35,414**	**44,877**	**41,485**	**31,749**	**31,663**

Source: BT-Drs. 16/1044, 24.3.2006