statewatch

Analysis

Counter-terrorism and the inflation of EU databases

Heiner Busch (@Busch_Heiner) and Matthias Monroy (@matthimon)

Translation by Viktoria Langer

May 2017

The topic of counter-terrorism in Europe remains closely linked to the development and expansion of police (and secret service) databases. This was the case in the 1970s, after 11 September 2001 and has also been the case since 2014, when the EU Member States started working on their action plans against 'foreign terrorist fighters'.

The first effect of this debate has been a quantitative one: the amount of data in the relevant databases has increased explosively since 2015. This can be seen by looking in particular at available data on the Europol databases, like 'Focal Points' (formerly: Analytical Work Files) of the Europol analysis system. Since 2015 they have become one of the central instruments of the European Counter Terrorism Centre (ECTC) which was established in January 2016.

'Hydra', the 'Focal Point' concerning Islamist terrorism was installed shortly after 9/11. In December 2003 9,888 individuals had been registered, a figure that seemed quite high at the time – but not compared with today's figures. [1] In September 2016 'Hydra' contained 686,000 data sets (2015: 620,000) of which 67,760 were about individuals (2015: 64,000) and 11,600 about organisations (2015: 11,000).

In April 2014 an additional 'Focal Point', named ‘Travellers’, was introduced, which is exclusively dealing with “foreign terrorist fighters” (FTF). One year later 'Travellers' included 3,600 individuals, including contact details and accompanying persons. In April 2016 the total number increased by a factor of six. Of the 21,700 individuals registered at the time, 5,353 were “verified” FTFs. In September 2016, of 33,911 registered individuals, 5,877 had been verified as FTFs.

Since 2010 Europol and the USA have operated the Terrorist Finance Tracking Programme (TFTP), which evaluates transfers made via the Belgian financial service provider SWIFT. Until mid-April 2016 more than 22,000 intelligence leads had been arisen out of that programme, of which 15,572 since the start of 2015. 5,416 (25%) were related to FTFs.

In contrast to Europol’s analytical system, the Europol Information System (EIS, the registration system of the police agency) can be fed and queried directly from the police headquarters and other authorities of EU Member States. Here, more than 384,804 'objects'

[1] Bürgerrechte & Polizei CILIP 77 (1/2004), p. 92

(106,493 individuals) were registered at the start of October 2016, 50% more than the year before. The increase is partly due to the growing number of parties participating in the EIS. In 2015 13 Member States were connected; in 2016 19 Member States. Some of the EU States, like the UK, also let their national secret services participate in the system. 16 Member States currently use automatic data uploaders for input. The number of third parties involved has also increased (in 2015 there were four, in 2016 there were eight). Interpol, the FBI and the US Department of Homeland Security are some of them.

Europol has reported further growth in the number of “objects” linked to terrorism in the EIS. According to the Slovak Presidency of the Council of the EU’s schedule for the improvement of information exchange and information management, in the third quarter of 2016 alone these grew another 20% to 13,645. [2] The EIS includes 7,166 data sets about individuals linked to terrorism, of which 6,506 are marked as FTFs or their supporters, or are assumed to be so. For May 2016 the CTC stated a figure of 4,129. [3] The increase in terrorism linked data can also be seen in the Schengen Information System (SIS) – in the alerts for “discreet checks or specific checks” following Article 36 of the SIS Decision. According to this, suspect persons are not supposed to be arrested. However, information about accompanying persons, vehicles etc. are recorded to provide insight into movements and to keep tabs on the contacts of the observed person.

At the end of September 2016 the number of such checks by the police authorities (following Article 36(2)) was 78,015 (2015: 61,575, 2014: 44,669). The number of alerts of the national secret services based on Article 36(3) was 9,516 (2015: 7,945, 2014: 1,859). “Hits” on such alerts and additional information are supposed to be sent directly to the alerting authorities and not as usual to national SIRENE offices (which deal with the exchange of supplementary information regarding alerts in the SIS). This option was only introduced in February 2015.

The Schengen states used the instrument for discreet surveillance or specific checks very differently. On 1 December 2015 44.34% of all Article 36 alerts came from authorities in France, 14.6% from the UK, 12.01% from Spain, 10.09% from Italy and 4.63% from Germany. [4]

How many of these alerts actually had a link to terrorism remains unclear; a common definition has not yet been found. However, the Council Working Party on Schengen Matters agreed on the introduction of a new reference (“activity linked to terrorism”) for security agencies’ alerts. According to Federal Ministry for the Interior, German alerts are marked with this reference when concrete evidence for the preparation of a serious act of violent subversion (§§129a, 129b Penal Code) can be presented. [5]

'Unnoticed in the Schengen area'

Along with the amount of collected and processed data, the purpose and the use of databases in the area of the former 'third pillar' of the EU (justice and home affairs) is also expanding. The Commission's April 2016 announcement concerning ‘Stronger and Smart Information Systems for Borders and Security’ and the Council's ‘roadmap to enhance information exchange and information management' [6] anticipate further growth in European databases. These innovations are being justified by the terror attacks of 2015 and the migration crisis, the 'irregular border crossings' of refugees. Terrorists – the Commission claims – may get into the EU via illegal migration routes and then remain in the Schengen area unnoticed. Therefore,

[2] Council document 13283/16 (14.10.16)
[3] Council document 9795/16 (07.6.2015)
[4] BT-Drs. 18/7291 (18.01.2016)
[5] BT-Drs. 18/9762 (26.09.2016)
[6] COM(2016) 205 (06.04.2016), Council document 8437/1/16 (20.05.2016)

border management, prosecution and migration management are dynamically linked to each other.

The consequences of this argumentation become evident when we take a look at the databases which currently managed by the European Agency for Operational Management of Large-Scale IT Systems (eu-LISA): the Visa Information System (VIS), the fingerprint system Eurodac and SIS II. The links between migration and border management on the one hand and policing purposes on the other are being pushed further and further.

SIS II, which includes alerts for wanted individuals and objects, discreet checks and entry bans and which is used mainly during police controls at the borders and within the EU, and by consulates for the issuing of visas, shows that this tendency is not new. Europol already has access to specific data in the SIS (alerts for arrest on the basis of European Arrest Warrants or for extradition, for targeted/discreet checks, property tracing), but is only allowed to make single enquiries. Three new proposals for Regulations governing the SIS presented by the Commission in December [7] would give Europol the power to search all data and copy whole datasets out of the system to compare them with its own (so called batch processing). Furthermore, Frontex and its officials will be allowed to use SIS II.

Data categories will also be extended: entry bans for deported third-country members have to be entered in the system even if the deportation took place on the basis of the German law concerning foreigners. The same applies to expulsion orders. Data linked to terrorism is to be included in the SIS on a compulsory basis as well. [8] In these cases an investigation inquiry could be made, permitting the collection of further information from other Schengen states.

SIS II already includes biometric data: facial images and fingerprints. However, they can only be used to verify the identity of a person when an alphanumeric search (name, surname, date of birth etc.) produces a hit. Henceforward, a search to identify individuals with fingerprints and palmprints is going to be allowed. This is why the SIS II includes an Automatic Fingerprint Identification System (AFIS). The dactyloscopic (fingerprint) data would be saved in a separate database. Like the SIS, the AFIS is set up as a centralized system. The implementation is scheduled for 2017 and the access to the data by national SIS offices could be possible from 2018 onwards. Non-allocated dactyloscopic data are to be entered as well, for example fingerprints found at crime scenes. This makes possible a new alert category of “unknown wanted individuals”. The proposed Regulations also include the storage of DNA data, to be used when the identification via fingerprints and facial images is not possible.

The current version of the Eurodac Regulation was decided in June 2013 and has only been active since July 2015, but it is going to be completely renewed. [9] The first European database for biometric data, which was introduced in 2003, currently includes 4.9 million entries and was supposed to identify multiple and follow-up applications by asylum seekers via the comparison of fingerprints. The Commission's proposal does not only include the lowering of the registration age limit from 14 to six years. In the future data on 'illegal residencies' and “third-country nationals” encountered during illegal border crossings (also in the hinterlands, outside the external borders) are supposed to be saved for five years. On top of fingerprints, facial images will also be collected. From 2020 onwards a new search option on the basis of facial images will be ready to use.

[7] COM(2016) 881, 882 and 883 (21.12.2016)

[8] The link to terrorism is defined according to art. 1-4 of the guideline for counter-terrorism of 2002 (Abl. EU L 164 (22.6.2002)).

[9] Current version Abl. L 180 (29.06.2013); COM(2016) 272 final (04.05.2016), Council document 14710/16 (28.11.2016)

The changes to the Regulation in 2013 gave Member States' police forces and Europol access to Eurodac but only in individual cases and under the condition that searches in the AFIS of the respective state and the fingerprint files of other Member States – via the Prüm network – failed to return results. Now the demands of prosecution authorities and especially of Europol are going to be taken into account. [10] According to the German government, future data inserted in the system should be immediately sent to the police and secret services of the Member States, who should then compare them with their own databases. [11]

This consultation process already exists today with the VIS: the consulates submit visa applications of people coming from 'risk states' to the responsible authorities of other Member States where they are reviewed. The VIS is also going to be extended to include technologies for facial screening following the Roadmap for the Improvement of Information Exchange and Information Management. Image data are already included, but there is so far no option for browsing it. The legal framework needs to be changed, so that biometric data can be used not only for verification, but also for identification during the search for wanted individuals. In April 2016 plans were released for the expansion of the decentralized Prüm process, so that it too will include facial images. [12] Europol and those Member States that are not currently included in this data exchange process have been asked to check the legal and strategic possibilities. A proposal for the implementation of a centralised or decentralised Prüm process for facial screening could be presented this year.

Finally, the European Criminal Records Information System (ECRIS) will be bolstered with a new target group. In the future the ECRIS will include convictions of third-country nationals if they reside in the EU and fingerprints will become compulsory data. The German central office of the ECRIS network is the Federal Ministry for Justice. The Federal Ministry for the Interior and Justice has already examined the necessary infrastructures for a fingerprint function. Originally, the dactyloscopic data of the ECRIS were supposed to stay decentralised within the Member States, but now EU interior ministers have decided on a centralized storage on EU level. [13] A final decision will be made in June. Furthermore, there is an ongoing debate about a European Police Records Index System (EPRIS). This project was included at the last minute in the final version of the Stockholm programme in 2010, which set out EU justice and home affairs policy from 2010 to 2015. Whether EPRIS will be established at all and if so, when, and whether it will be designed as a centralised database or rather as a cross-linking of national systems, remains unclear.

Controls beforehand and in real time

Since 2004 airlines have had to submit Advanced Passenger Information (API) to the border agencies of EU Member States, which includes personal (biographical) details and information about identity documents. Normally, this information is deleted after it has been compared with the respective database. [14] In April 2016 the European Council and the European Parliament decided on rules for the use of Passenger Name Record (PNR) data – resistance on the part of the Parliament broke down after the attack in Paris in November 2015. [15] The PNR Directive forces airlines and travel agencies to submit up to 60 individual pieces of data about the passenger – from flight and seat number to food preferences, up to credit card information or IP addresses – to the respective national PNR central department (Passenger

[10] Council document 13283/16 (14.10.16)
[11] BT-Drs. 18/9762 (26.9.2016)
[12] Council document 6078/2/16 (19.04.2016)
[13] COM(2016) 7 (19.01.2016)
[14] RL 2004/82/EG, Abl. EU L 261 (06.08.2004)
[15] Abl. EU L 119 (04.05.2016)

Information Unit) with every booking. These data can then be saved in full for six months, and after that in “depersonalised” form for a further five years.

The PIUs are to compare the data not only with the relevant national and European databases. They will also identify “suspicious and unusual travel patterns” and create risk profiles. Criteria for these new indicators will be defined by Europol. Shortly after the decision on the PNR Directive and “due to the current security situation” all EU Member States also announced their intention to apply these instructions not only on flights to and from the EU, but also on flights within the EU. [16] The Belgian government wants to take this a step further and has called for the inclusion of cross border trains, ferries and buses. [17]

In April 2016 the European Commission also presented a new proposal for an Entry/Exit System (EES). [18] This aims for the registration of all entries and exits of all third-country nationals – whether they require visas or not – at the external border. The French government proposed extending the system to EU citizens and other people enjoying the right of free movement. [19] At border crossings the biometric data – facial picture and fingerprints – included in the travel documents would be read and saved for five years, together with biographic information. Following recent plans the system is supposed to be ready for operation in 2020. The EES was requested initially as a border police system against so called 'overstayers', however, it increasingly appears that it will be a tool for counter-terrorism and crime control. The police agency Europol will have access to it and some Member States, including Germany, have requested access for secret services.

Closing the gaps

Besides the PNR Directive and the planed EES the EU considers its databases insufficient. A further proposal aims to establish an EU wide Travel Information and Authorisation System (ETIAS) which will complement existing systems for advance information on intended border crossings. Information about people requiring visas are recorded prior to entry via the VIS, and the PNR systems allows a prior check of travellers. However, according to the Commission, a gap occurs in cases of third-country nationals exempted from the visa requirement, when entering the Schengen area via land borders. [20] The role models for the ETIAS proposal [21] are systems for entry permission in the USA, Canada and Australia. Every border crossing needs to be announced in advance: travellers will have to give personal details and information about their intended stay via an internet form. [22] This includes the purpose of the journey and a travel plan. Furthermore, there is a discussion on the obligation of giving details about modes of transport. These details would be compared with national and international information systems through a prior check by the responsible border agencies. For this purpose Europol is also supposed to create an ETIAS watchlist.

As with PNR data, the ETIAS is supposed to serve the risk assessment of travellers, especially concerning irregular migration and security. Migration risks will be identified through the ETIAS and EES by using statistical data about certain countries and groups of origin. The Member States are supposed to create indicators for the identification of security risks. This would enable a quicker check-in for travellers with permission through automatic control systems at border crossings. Therefore, ETIAS is described as a tool of travel facilitation. However, registration does not guarantee permission to enter.

[16] Council document 7829/16 (18.04.2016)
[17] www.cilip.de (04.01.2017)
[18] COM(2016) 194 final (06.04.2016)
[19] http://database.statewatch.org/article.asp?aid=35512
[20] COM(2016) 205 (06.04.2016)
[21] Council document 14084/16 (16.11.2016)
[22] https://etias.com

Interoperability

All existing and planned information systems are supposed to be fused together in an EU-wide integrated biometric identity management system for travel, migration and security. According to the Commission, where necessary and possible, systems have to be interconnected and interoperable. Provision is made for the installation of a joint data store managed by eu-LISA for all biometric databases (SIS II, Eurodac, VIS, ECRIS and EES). The Commission calls this particular project the most ambitious long-term concept to ensure interoperability, and the plan goes back to a paper of the German Federal Minister of the Interior, Thomas de Maizière.

This paper, which was recently submitted to the Commission, calls for the linkage of European data sets. The paper explained that "data protection is all well and good, but in times of crises security has priority." The Minister also called for further search options in connected databases. According to the German proposal biometric data and key data would be collected again and software would then prove if the fingerprints are already registered in a different database. If this is the case, the best and broadest data set will be used automatically. The ideal case would be to register ten fingerprints for every person.

Furthermore, the Commission announced the development of a standardised 'Single Search Interface', which would give law enforcement officers and other officials access to multiple databases with one click. Authorities of six Member States, including the BKA, are working together with Europol on the technical implementation. The aim is the installation of a standardised data format (Universal Message Format) and the automation of data exchange processes. Further steps towards EU-wide integrated biometric identity management are being discussed by a Commission-convened High-Level Expert Group on Information Systems and Interoperability, who published their proposals for travel, migration and security in December. [23] Their final report was published in May. [24]

The mixture of counter-terrorism, border control and migration control is an invitation to realise the police's wish list. The control and registration is still directed to non-EU citizens. However, it does not have to stay this way, as can be seen from the terms of references for the 'new systems' subgroup of the aforementioned High-Level Expert Group. Here, the discussion leads to remaining information gaps after the expansion introduced by the ETIAS: holders of long-term residence permits and, finally, EU citizens. The question is: should movements of EU citizens be registered when crossing the external borders or are the systematic controls included in the Schengen Border Code enough? [25] The answer will probably be towards an expansion.

Originally published in Bürgerrechte & Polizei (CILIP) no. 112: Alles Anti-Terror?

Statewatch does not have a corporate view, nor does it seek to create one, the views expressed are those of the author. Statewatch is not responsible for the content of external websites and inclusion of a link does not constitute an endorsement.

[23] http://www.statewatch.org/news/2016/dec/eu-com-hlg-interoperability-report.pdf
[24] http://statewatch.org/news/2017/may/eu-com-hleg-info-systems-interoperability-final-report-5-17.pdf
[25] Ares (2016) 5744990 (04.10.2016); http://www.statewatch.org/news/2016/nov/eu-com-etias.pdf

Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

Statewatch is the research and education arm of a UK registered charity and is funded by grant-making trusts and donations from individuals.

Web: www.statewatch.org | Email: office@statewatch.org

Post: c/o MayDay Rooms, 88 Fleet Street, London, EC4Y 1DH

Charity number: 1154784 | Company number: 08480724
Registered office: 2-6 Cannon Street, London, EC4M 6YH