1216-2574/USD 20.00

ACTA JURIDICA HUNGARICA
54, No 2, pp. 164–183 (2013)
DOI: 10.1556/AJur.54.2013.2.4

ZOLTÁN DÓCZI*

The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice

"The international community must adopt a new strategy to combat terrorism by promoting international cooperation and its own effective use of information power."[1]
(Kohara, Masahiro)

Abstract: The abolishment of the internal border checks and the common procedures at the external borders fosters the decision-making of the European Union to establish large-scale IT systems in the area of freedom, security and justice. The decrease of the security deficit by the control of immigration flow consists of three endeavours: the common border control policy, the common visa policy and the common asylum policy. The aim of this paper is to analyse and evaluate the development of the operational management of large-scale IT systems in the area of freedom, security and justice. The development process of these systems is not more than their integration into the so-called IT Agency. *This new regulatory agency was established in January 2012. It has merged the operational management tasks of the further developed version of SIS (the SIS II), VIS and EURODAC and it is* flexible to add other existing and potential new systems. Hence, the added-value of the IT Agency is to be assessed, since new technologies shall be harnessed to meet the requirements of enhancing security and facilitating travel at the external borders.

Keywords: Schengen, large-scale IT systems, information power, security deficit, facilitate travel

1. Introduction

In the flow of the European integration process, the so-called large-scale IT systems, namely the Schengen Information System (SIS), the Visa Information System (VIS) and the EURODAC were established to support the realisation of Community/Union policies in relation to immigration, visa, asylum and the free movement of persons within the Schengen area. These information systems are highly important for the border security strategy, since among others the systematic data gathering and data exchange of information concerning third country nationals happen through them.

In this paper, the three existing large-scale IT systems are observed. Their operation and difficulties can give a frame of reference to evaluate them. Therefore, their integration process, i.e. the establishment and the functioning of the *Agency for the operational*

* Ph.D. student, Corvinus University of Budapest, Faculty of Social Sciences, Institute for International Studies, H-1093 Budapest, Közraktár u. 4–6.
E-mail: zoltan.doczi@stud.uni-corvinus.hu
Manuscript finalised on 28 October, 2012.

[1] Kohara, M.: International Power and International Security. *Progress in Informatics*, 1 (2005) 1, 39–46.

management of large-scale IT systems in the area of freedom, security and justice[2] (hereinafter: the IT Agency) is highly relevant. Via the assessment, the relevance of the smart borders initiative,[3] i.e. the establishment of new systems is more easily understandable.

Henceforward it is fundamental to consider how the newest segment of the large-scale IT systems' operational management, i.e. their integrated operational management system contributes to the smarter European borders.

The establishment of a new European Agency were proposed by the European Commission for the operational management of the large-scale IT systems in the European Union.[4] It was established in 1 January, 2012.

The current analysis is limited in time. The relevant information sources, legislations, proposals and the academic literature are examined, which were issued before 28 October, 2012.

Firstly, it is worth to consider why the establishment of the IT Agency was legally predetermined to give an over-all picture of the IT Agency with a special focus on its effects concerning the realisation of smarter borers in Europe.

Then it is essential to understand the aims and the basic tasks of the IT Agency in order to evaluate the scope of this European agency taking into account the principle of subsidiarity and proportionality.

The next step of the analysis is the relationship of the IT Agency with other EU agencies. For that a layer model is presented to better highlight the interrelations.

Finally, an assessment is made to define and to detail the added-value of the IT Agency. It is scrutinised in order to be answered how the delineated development process of the large-scale IT systems' operational management contributes to the increase of the efficiency of the information power in order to decrease the security deficit thus contributing to a more secured Europe.

2. Historical Development of the Large-Scale IT Systems in Brief

In the current chapter, the development and the basic tasks of the existing large-scale IT systems is to be concisely highlighted in order to give a background for the evaluation of SIS', VIS' and EURODAC's integration. It is crucial to understand the common grounds and possible connections among them and with the IT Agency. Furthermore, their operational difficulties add another aspect to the birth of the smart borders initiative.[5]

[2] Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, 1–17.

[3] COM(2011) 680 final Communication from the Commission to the European Parliament and the Council Smart borders–options and the way ahead, Brussels, 25.10.2011.

[4] COM(2009) 293 final Proposal for a Regulation of the European Parliament and of the Council e*stablishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, Brussels, 24.6.2009. After the Lisbon Treaty, equivalence with COM(2010) 93 final Amended Proposal a Regulation (EU) No .../... of the European Parliament and of the Council on e*stablishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*, Brussels, 19.3.2010.

[5] COM(2011) 680 final, *op. cit.*

Schengen Information System (SIS)

The Schengen Information System is a large-scale IT system that allows the competent authorities (i.e. national police, customs, and border control authorities when making checks on persons at external borders or within *Schengenland*, and the immigration officers when dealing with third-country nationals, in particular when deciding whether to issue visas or residence permits[6]) to obtain information regarding certain categories of persons, vehicles and objects.

The SIS has become operational with the entry into force of the Schengen Implementing Convention in March 1995. Further rules were laid down by the decisions of the Schengen Executive Committee, such as "the Decision establishing the SIRENE[7] Manual, which governs subsequent exchanges of information following a 'hit' in the SIS."[8] The factual data are stored on the SIS but the SIRENE bureaus make it possible to exchange 'soft' data such as criminal intelligence information.[9] The power of the Executive Committee and its working groups was transferred by the 1997 Amsterdam Treaty to the Council and to its working groups. The SIS consists of two fundamental elements: the central database (called C-SIS) that is located in Strasbourg and the national SIS-bases (called N-SIS) in all of the participating states.

The corresponding authorities can enter certain types of information about or relating to persons. Submitted personal data are certain personal details and an indication of whether he or she is armed or dangerous.[10] "There are six broadly defined reasons for which information can be included on the SIS."[11] These are the so-called types of SIS 'alerts'.[12]

The SIS is communitarised as a Schengen *acquis* with the entry into effect of the 1997 Amsterdam Treaty. In spite of the protocols on the special status of the United Kingdom and Ireland, they also joined the SIS for criminal law and policing purposes;[13] however they do not apply the Schengen *acquis*.

The original SIS has already been updated to 'SIS 1+' in order to enable linking the Nordic countries to SIS.[14] Thus the Schengen Implementing Convention SIS rules were amended in 2004 and 2005 within the current technical framework. As a result of the amendments, the judicial authorities, the Europol, the Eurojust and with another regulation the vehicle registration authorities got access to SIS data. A further decision conferred power upon the Commission to amend the SIRENE Manual.[15] However, these amendments designed to be more technical.

The data storage capacity of SIS was planned for a limited number of countries (ideally for eighteen according to the average opinion), so due to the eastern enlargement the

[6] Schengen Implementing Convention, OJ L 239, 22.9.2000, Art. 92(1), 42.

[7] It stands for Supplément d'Information Requis à l'Entreé Nationale.

[8] Peers, S.: Key Legislative Developments on Migration in the European Union: SIS II. *European Journal of Migration and Law*, 10 (2008) 1, 79.

[9] Broeders, D.: The New Digital Borders of Europe – EU Database and the Surveillance of Irregular Migrants. *International Sociology*, 22 (2007) 1, 80.

[10] Schengen Implementing Convention, *op. cit.* Art. 94(3), 43.

[11] Peers, S.: *EU Justice and Home Affairs Law*. "Oxford European Community Law Series", 2nd ed., Oxford–New York, 2006, 548.

[12] See: Schengen Implementing Convention. *op. cit.* Art. 95–100, 43–45.

[13] Peers: Key Legislative Developments… *op. cit.* 80.

[14] Cf. the incorporation of the Nordic Passport Union into the Schengen area.

[15] Peers, S.: *EU Justice and Home Affairs Law. op. cit.* 548–549.

Member States decided to develop and to build up the second generation SIS (SIS II) till March 2007. It became clear at the meeting of the Ministers of Justice and Home Affairs in December 20006 that more time is needed for the development of SIS II. Thus they agreed on that the accession of those new Member States from the ten which are ready to join to the Schengen area shall happen with the accession to the SIS 1+, while the SIS II should have been operational in the enlarged *Schengenland* in 2008. This proposal came from Portugal for the development of a 'SIS One4 All'. As I have mentioned, the SIS One 4 All is the extension of the existing SIS 1+, a solution which had previously been understood to be technically impossible.[16]

Once the development phase of SIS II comes to an end, the operational phase starts expectedly in 2013.[17] New functions were added to the second generation SIS compared to the SIS 1+. These include biometric data, new categories of data and the possibility for running searches on the basis of incomplete data.[18] So, the functioning of SIS has been extended to provide for the fight against terrorism[19] and adopted to enable the storage of photographs and fingerprints after 11 September 2001. The addition of biometric information to SIS is one of the key aspects of the overhaul, while biometric data can be used both to confirm someone's identity and to identify somebody.[20] The SIS II has a further novelty concerning to the access of data, i.e. persons listed on the EU terrorist list based on decisions by the Sanctions Committee of the UN Security Council can be included in the SIS.[21]

As a result of legal, political and technical problems, the set out deadlines in the global SIS II timetable[22] cannot be observed. That is why the Commission formulated a proposal for the a Council Regulation amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information

[16] Peers: Key Legislative Developments… *op. cit.* 81–82.

[17] Council Regulation (EU) No 541/2010 of 3 June 2010 amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), OJ L 155, 22.6.2010, Art. 1(6), 22.

[18] *Ibid.*

[19] Cf. Council Regulation (EC) No. 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 162, 30.4.2004, 29–31; and Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 68, 15.3.2005, 44–48.

[20] Baldaccini, A.: Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases. *European Journal of Migration and Law*, 10 (2008) 1, 37–38.

[21] Boeles, P.–Heijer, M.–Lodder, G.–Wouters, K.: *European Migration Law.* Antwerpen–Oxford–Portland, 2009, 423. See also: Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, Art. 26, 15.

[22] 5780/07 Revised Global SIS II schedule in light of the SISone4ALL implementation, Brussels, 29.1.2007.

System (SIS II).[23] A group of experts (i.e. the Global Programme Management Board) has been set up to elaborate the technical specifications for the switch to the operational phase of SIS II which is envisioned to start in 2013.[24]

Visa Information System (VIS)

The so-called Santiago Plan[25] included proposals, *inter alia*, on visa policy and on information exchange and analysis on migration flow. Regarding visa policy, it recommended the annual review of the visa lists, the inclusion of photo and biometric data of visa holders in their visas, the establishment of joint visa offices with a pilot project in Pristina, and the establishment of the Visa Identification System.[26] The Visa Identification System has been renamed to Visa Information System (VIS). The VIS is a system for the exchange of visa data among its Member States. Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)[27] provides the legal basis for the development of the system. The VIS Regulation[28] defines the purpose, the functionalities and the responsibilities concerning the VIS. It sets up the conditions and procedures for the exchange of data among its members on application for short-stay visas and on the related decisions.

The technical set-up of the system is similar to the SIS. The new visa system has a central database (C-VIS), and interface at the national level (N-VIS) and local access points (terminals) for police, immigration authorities and consular posts.[29] The VIS can serve as an instrument to detect and identify those irregular migrants who travelled into the EU legally at any border, and the overstayed.[30] It is not a law enforcement tool. However, it is a law enforcement access. The VIS is for facilitating border and police checks, to combat fraud, to improve consular cooperation and to prevent visa-shopping. The VIS facilitates the application of the Dublin II Regulation[31] fixed in Article 21 and 22 of the VIS

[23] COM(2009) 508 final Proposal for a Council Regulation amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), Brussels, 29.9.2009.

[24] *Ibid.* especially Art. 1(5) and Art. 1(6).

[25] Proposal for a Comprehensive Plan to Combat Illegal Immigration and Trafficking of Human Beings in the European Union, OJ C 142, 14.6.2002, 23–36.

[26] Meloni, A.: *Visa Policy within the European Union Structure*, Berlin, 2006, 178.

[27] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004, 5–7.

[28] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, 60–81. The further legislation of VIS is the Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designed authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.8.2008, 129–136.

[29] Broeders: *op. cit.* 86.

[30] *Ibid.* 85.

[31] Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ L 50, 25.2.2003, 1–10.

Regulation.[32] However, the VIS data substantially contribute to the prevision, detection or investigation of terrorist offences and of other serious criminal offences.

Detailed rules on access for entering, amending, deleting and consulting VIS data as well as on access to biometrics (photographs, fingerprints) for verification at border crossing points, for verification within the territory of the Member States, for identification and as appointed in the previous paragraph for determining responsibility for asylum applications and for examining an asylum application. The VIS shall be connected to the national system of its Member States to enable the competent authorities of the Member States to process data on visa application and on visa issued, refused, annulled, revoked or extended.[33]

The Schengen Borders Code has been harmonised with the VIS by a regulation.[34] As of 2008, the VIS shall have begun operations by December 2010 as planned. In that case the expiry of the derogations in the VIS Regulation and the Schengen Borders Code concerning the use of biometrics in the VIS is at the same time as the entry-exit system could begin operation estimated by the Commission.[35] As Steve Peers recalled "the initial thee-year derogation from the use of fingerprint checks at external borders in the VIS Regulation will overlap with the rolling out of the VIS–so the impact of use of the VIS at external borders will be limited for some time."[36]

The Visa Code[37] has been applied from 5 April 2010. Article 54 harmonises the VIS Regulation with the Visa Code. If the applicant is a person for whom an alert has been issued in the SIS for the purpose of refusing entry, it indicates a ground for the refusal of the visa.[38] Article 54(7) defines the data which the visa authority shall add to the application file if a visa is annulled or revoked. Furthermore, the Visa Code gives some aspects to the monitoring and the evaluation of the VIS and of the Visa Code.[39]

Not only the operation of SIS II delayed–as I mentioned above, but also the operation of VIS. The VIS has been operational since 11 October, 2011. However, the VIS will have been applied step by step, i.e. region by region (regional rollout). The Commission adopted Decision 2010/49/EC[40] which determines the first regions for the rollout. According to the Commission Decision, the VIS shall subsequently be deployed in the Near East, and then in the Gulf region. In November 2011, the VIS started its full operation in North Africa after all Schengen States having visa-issuing consulates in the region informed the Commission that they had taken the necessary technical and legal arrangements for collecting and

[32] Regulation (EC) No 767/2008, *op. cit.*, Art. 21–22, 70–71.

[33] Boeles–Heijer–Lodder–Wouters: *op. cit.* 424.

[34] Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, OJ L 35, 4.2.2009, 56–58.

[35] Peers, S.: Legislative Update: EC Immigration and Asylum Law, 2008: Visa Information System. *European Journal of Migration and Law*, 11(2009) 1, 84.

[36] *Ibid.*

[37] Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), OJ L 243, 15.9.2009, 1–58.

[38] *Ibid.* Art. 54(6)b, 24.

[39] *Ibid.* Art. 57(3), 26.

[40] Commission Decision 2010/49/EC of 30 November 2009 determining the first regions for the start of operations of the Visa Information System (VIS), OJ L 23, 27.1.2010, 62–64.

transmitting the data for all applications in the region to the VIS.[41] The Commission planned to adopt another decision determining a second step of regions for the VIS consular rollout by the end of 2011.[42] This goal was achieved in April 2012.[43]

EURODAC (European Dactylographic System)

EURODAC is a database that stores and compares the fingerprints of asylum applicants and illegal migrants apprehended in connection with the irregular crossing of an external border. It was established to allow Member States to determine the state responsible for examining an asylum application according to the Dublin Convention, and now the Dublin II Regulation. The EURODAC Regulation[44] was adopted in 2000, and the Council adopted the implementing rules[45] in 2002. The system has become operational in 15 January 2003.[46] These regulations highly contribute to the building of the Common European Asylum System.

The EURODAC Regulation consists of the Central Unit managed by the European Commission containing an Automated Fingerprint Identification System (AFIS) which shall receive data and transmit "hit–no hit" replies to the national authorities (to the National Access Point servers) in each Member State. Its activity is monitored by the European Data Protection Supervisor. The national authorities are responsible for the overall quality of data transferred to, recorded or erased from the Central Unit and for the security of the transmission of data among their national authorities and the Central Unit. Several categories are defined for asylum applicants and aliens. The following data is collected for any asylum applicants over 14 years of age: fingerprints; sex of the data subject; Member State of origin, place and date of the application for asylum; reference number used by the Member State of origin; date on which the fingerprints were taken, date on which the data were transmitted to the Central Unit and the operator user ID of the person who transmitted the data.[47]

As it was highlighted by Steve Peers, "the Council's March 2004 conclusions on anti-terrorism and the November 2004 Hague Programme, both of which call for the 'interoperability' among EURODAC, the planned Visa Information System (which will store fingerprints of visa applications), and the second-general Schengen Information

[41] MEMO/11/682 "Frequently Asked Questions: The Visa Information System goes live", *Europa Press Releases RAPID*, Brussels, 11.10.2011.

[42] *Ibid.*

[43] 2012/274/EU: Commission Implementing Decision of 24 April 2012 determining the second set of regions for the start of operations of the Visa Information System (VIS), OJ L 134, 24.5.2012, 20–22.

[44] Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "EURODAC" for the comparison of fingerprints for the effective application of the Dublin Convention (EURODAC Regulation), OJ L 316, 15.12.2000, 1–10.

[45] Council Regulation (EC) No. 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "EURODAC" for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 62, 5.3.2002, 1–5.

[46] Peers, Steve (ed.): EU Immigration and Asylum Law: Text and Commentary. *Immigration and Asylum Law and Policy in Europe*. Vol. XII., Leiden, 2006, 259.

[47] Boeles–Heijer–Lodder–Wouters: *op. cit.* 424–425.

System (which will have the capacity to store fingerprints)."[48] In December 2008, the Commission proposed the first three measures which would constitute the second phase of the Common European Asylum System: amendments to the EURODAC Regulation, the Dublin II Regulation and the Reception Conditions Directive.[49, 50]

The 2010 Belgian Presidency was committed to speedy completion the Common European Asylum System. The Dublin and EURODAC Regulations and the Long Term Residence and Qualification Directives have been prioritised with ensuring coherence in relation to the Reception Conditions and Procedures Directives.[51] Therefore, the legislative package of the Common European Asylum System includes six legislative proposals which EU Member States have committed to adopt by 2012.[52] Therefore, an amended proposal[53] was born aiming at the fostered transmission of fingerprint records and the involvement of Europol and national law enforcement authorities. At the time of writing, the initiative is still in the European decision-making.

[48] Peers (ed.): *EU Immigration and Asylum Law. op. cit.* 272.

[49] COM(2008) 815 final Proposal for a Directive of the European Parliament and of the Council laying down minimum standards for the reception of asylum seekers, Brussels, 3.12.2008; cf. COM(2011) 320 final Amended proposal for a Directive of the European Parliament and of the Council laying down standards for the reception of asylum seekers (Recast), Brussels, 1.6.201. COM(2008) 820 final Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person, Brussels, 3.12.2008; cf. COM(2008) 820 final Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (Recast), Brussels, 3.12.2008. COM(2008) 825 final Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], Brussels, 3.12.2008; cf. COM(2010) 555 final Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], Brussels, 11.10.2010.

[50] Peers: *Legislative Update. op. cit.* 71.

[51] 13703/2010 Common European Asylum System–State of Play, Brussels, 27.9.2010.

[52] 15848/10 "Press Release, 3043rd Council meeting, Justice and Home Affairs", *Europa Press Releases RAPID,* Brussels, 8–9.11.2010.

[53] COM(2012) 254 final Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No […/…] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version), Brussels, 30.5.2012.

3. The Incorporation of the Large-Scale IT Systems into a Single European Agency

This section deals with the legislative integration process of the information systems working for the European Union's public safety. In what follows, the connection points of the large-scale IT systems' operational management are highlighted.

The EU Member States want to foster the integration of the information systems for seven years at least. As the Hague Programme states

> "[...] [t]he European Council requests the Council to examine how to maximise the effectiveness and interoperability of EU information systems in tackling illegal immigration and improving border controls as well as the management of these systems on the basis of a communication by the Commission on the interoperability between the Schengen Information System (SIS II), the Visa Information System (VIS) and EURODAC to be released in 2005, taking into account the need to strike the right balance between law enforcement purposes and safeguarding the fundamental rights of individuals. [...]".[54]

The fundamental legislation of SIS II[55] was adopted on 20 December 2006. This is the SIS II Regulation. Worthy of note, the SIS II has more legal instruments.[56] Article 15(1) of the SIS II Regulation states the followings:

> "After a transitional period, a management authority (the 'Management Authority'), funded from the general budget of the European Union, shall be responsible for the operational management of Central SIS II. [...]".

Till the establishment of the Management Authority, during a transitional period, the Central SIS II is managed by the Commission. In the interim transitional period the Commission may delegate its power to two Member States.[57] Thus the

> "CS-SIS, which performs technical supervision and administration functions, shall be located in Strasbourg (France) and a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system, shall be located in Sankt Johann im Pongau (Austria)." [58]

Based on Article 55(1), the SIS II Regulation entered into force on 17 January 2007. A Joint Statement of the Commission, the Council and the European Parliament on Article 15 relating to operational management of SIS II assigns

[54] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, 7.

[55] Regulation (EC) No 1987/2006, *op. cit.*

[56] Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding the access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsibility for issuing vehicle certificates, OJ L 381, 28.12.2006, 1–3; and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation of Schengen Information System, OJ L 205, 7.8.2007, 63–84.

[57] Regulation (EC) No 1987/2006, *op. cit.* Art. 15(4), 11.

[58] *Ibid.* Art. 4(3), 8.

> "[...] the necessary legislative proposal to entrust an Agency with the long-term operational management of the Central SIS II and parts of the Communication Infrastructure. [...]".[59]

It means that these proposals shall be published in 2009. According to the Joint Statement the Agency shall take up fully its activities in 2012.[60]

The same legislative techniques are used in case of the adaptation of legal instrument of the Visa Information System (VIS).[61] The VIS Regulation was adopted on 9 July 2008.[62] After a transitional period the Management Authority shall be founded.[63] During that period the Commission is responsible for the operational management of VIS, which may delegate its power to two Member States.[64] Consequently, the central VIS is located in Strasbourg (France) and the back-up central VIS in Sankt Johann im Pongau (Austria).[65, 66]

A Joint Statement of the European Parliament, the Council and the Commission on Article 26 relating to operational management of VIS[67] was approved. Its requirements, its goals and the planned deadlines are the same as in the Joint Statement relating to the SIS II. According to the Joint Statement, an Agency has been established for the long-term operational management of the VIS. The Statement added that

> "[...] [t]he impact assessment could form part of the impact assessment which the Commission undertook to carry out with regard to the SIS II. [...]".[68]

The third IT system is the EURODAC. Its interoperability shall be ensured in line with the Hague Programme. The Commission issued three proposals,[69] *inter alia*, to promote the harmonisation of the EURODAC with other IT systems.

[59] Statement 235/06 Joint Statements of the long-term management of SIS II and VIS. Joint statement by the Commission, the Council and the European Parliament on Article 15 relating to operational management of SIS II. Source: SEC(2009) 837 Commission Staff Working Document, Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice and Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, Impact Assessment, Brussels, 24.6.2009, Annex 4, 102.

[60] Peers: Key Legislative Developments. *op. cit.* 86–87.

[61] Regulation (EC) No 767/2008, *op. cit.;* and Council Decision 2008/633/JHA, *op. cit.*

[62] Regulation (EC) No 767/2008 *op. cit.*

[63] *Ibid.* Art. 26(1), 72.

[64] *Ibid.* Art. 26(4), 72.

[65] *Ibid.* Art. 27, 73.

[66] Peers: Key Legislative Developments. *op. cit.* 86–87.

[67] Statement 235/06 Joint Statements of the long-term management of SIS II and VIS. Joint statement by the European Parliament, the Council and the Commission on Article 26 relating to operational management of VIS. Source: SEC(2009) 837, *op. cit.* Annex 4, 102.

[68] *Ibid.*

[69] COM(2008) 815 final, *op. cit.;* cf. COM(2011) 320 final, *op. cit.* COM(2008) 820 final, *op. cit.*; cf. COM(2008) 820 final (Recast), *op. cit.* COM(2008) 825 final, *op. cit.*; cf. COM(2010) 555 final, *op. cit.*

One of the proposals[70] would like to implement a new recital as Recital 11 into the Dublin II Regulation[71] in order to tone in with the VIS Regulation although the recitals are not legally binding. But these items of a regulation express the purpose of the legislators and the legal basis. In disputes the recitals can be very important adopting the soft law approach to the specific situation.

Another proposal[72] suggests replacing Article 4 of Council Regulation (EC) No 2725/2000[73] with the followings:

> "1. After a transitional period, a Management Authority, funded from the general budget of the European Union, shall be responsible for the operational management of EURODAC. [...]
> 4. During a transitional period before the Management Authority takes up its responsibilities, the Commission shall be responsible for the operational management of EURODAC.
> [...]
> 7. The Management Authority referred to in this Regulation shall be the Management Authority competent for SIS II and VIS."

Pursuant to the three cited proposals concerning EURODAC and to the above-mentioned Joint Statement, a European Agency shall have been established for the long-term operational management of SIS II, VIS and also EURODAC until 2012. Therefore, the foundation of the IT Agency was legally foreordained, which could have signed the perception of some security deficit in *Schengenland*.

4. Mechanisms of the IT Agency

The current chapter is about the presentation of the aims, tasks and operation of the newest EU Agency. Firstly, the general aims are detailed. Then the problem of the territorial scope of the IT Agency, the so-called *la géométrie variable* (variable geometry) is raised. Then the governance structure of the Agency is briefly summed up.

By the creation of the IT Agency, the establishment of a new regulatory agency was found to be the best alternative. On the one hand, according to this option, the IT Agency is responsible for the long-term operation management of SIS II, VIS and EURODAC, and the IT Agency shall organise trainings related to the use of SIS II, VIS and EURODAC.[74] On the other hand, the Agency shall develop and manage other IT systems.[75]

One of the basic aims of all the options presented in the impact assessment[76] is to foster the interoperability among the large-scale IT systems. This endeavour creates synergies and thus reduces costs; consequently, it contributes to their cost-effective

[70] COM(2008) 820 final, *op. cit.*, Recital 28; cf. COM(2008) 820 final (Recast), *op. cit*. Recital 28.

[71] Council Regulation (EC) No 343/2003, *op. cit.*

[72] COM(2008) 825 final, *op. cit*.

[73] Council Regulation (EC) No 2725/2000, *op. cit*.

[74] Regulation (EU) No 1077/2011, *op. cit.*, Art. 3–5, 6.

[75] *Ibid.* Art. 6, 7.

[76] SEC(2009) 837, *op. cit.*

operation. Moreover, the structural arrangement of the IT Agency respects the principle of subsidiarity, since, evidently, the above presented aims cannot be achieved by the Member States individually. Furthermore, concentrating on the proportionality principle, the competences of the IT Agency are kept to the minimum, since it manages only the central parts of SIS II, the central parts of VIS and the national interfaces, the central part of EURODAC and certain aspects of the communication infrastructure, without having responsibility for the data entered in the systems.

As the European Data Protection Supervisor (hereinafter EDPS) highlighted in his opinion,[77] during the legislative and public debate "concerns have been voiced about the possible creation of a 'big brother agency'."[78] These feelings are in relation to the possibility of function creep and the issue of interoperability. The EDPS also stated that "the risk of mistakes or wrong use of personal data may increase when more large-scale IT systems are entrusted to the same operational manager."[79]

According to the above referred impact assessment, the IT Agency should have been a first pillar agency with accompanying acts covering third pillar legal issues. Since the proposals were submitted, the 2010 Lisbon Treaty has become operational. The EDPS advised that Article 87(2)(a) TFEU could be the sole basis for the proposed measures. Taking Article 87(2)(a) TFEU as the legal basis, the Commission was be able to merge to two previous proposals.[80] The only disputable point of the EDPS's approach is that the cited article concerns to the police cooperation. The SIS II is more related to the police cooperation. But the VIS and the EURODAC system are clearly connected to the common visa and the asylum policy.

The IT Agency is responsible for the protection of personal data.[81] In that way, the application of the 2010 Lisbon Treaty is more preferred, since the personal data protection "stems from a fundamental right acknowledged by Article 16 TFEU and Article 8 of the Charter of Fundamental Rights, which became binding on 1 December 2009."[82]

On 19 March 2010 the European Commission merged the two previous proposals into one united proposal pursuant to Article 293(2) of the TFEU.[83] The amended proposal is the equivalent of the two previous proposals. Besides the clarification of the legal basis of the

[77] 5039/10 Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of EU Treaty, Brussels, 7.1.2010.

[78] *Ibid.* Point 24.

[79] *Ibid.* Point 25.

[80] COM(2009) 293 final, *op. cit.*; and COM(2009) 294 final Proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of the EU Treaty, Brussels, 24.6.2009.

[81] 5039/10 Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and on the proposal for a Council Decision conferring upon the Agency established by Regulation XX tasks regarding the operational management of SIS II and VIS in application of Title VI of EU Treaty, Brussels, 7.1.2010, Points 15–17.

[82] *Ibid.* Point 15.

[83] COM(2010) 93 final, *op. cit.*

Agency, there is not any significant amendment. The united proposal suggested the Title V of TFEU as the legal basis of the IT Agency. Article 87(2)(a) remained as one of its legal basis. Finally, the accepted Regulation[84] (hereinafter: IT Agency Regulation) refers to the articles of Title V of TFEU as the legal basis of the IT Agency.

The Regulation of the IT Agency properly guarantees the involvement of public interest, the data protection and the security rules on the protection of classified information and non-classified sensitive information; and regulates the access to documents.[85] On the one hand, after the entry into force of the 2010 Lisbon Treaty, the fundamental rights and freedoms shall be more carefully respected by the European institutions. On the other hand, the appropriate accountability of the European Agencies is ensured by the European Parliament and the European Data Protection Supervisor. Furthermore, the European Court of Justice[86] and the General Court have full jurisdiction over the activities of the IT Agency.

As the legal basis of the IT Agency was merged under Title V of the 2010 Lisbon Treaty, the IT Agency is affected by *la géométrie variable* arising from the protocols on the positions of the United Kingdom, Ireland and Denmark, since these protocols are included in the 2010 Lisbon Treaty with some minor amendments. The IT Agency Regulation constitutes the development of the Schengen *acquis* and builds on the provisions of EURODAC related measures. Hence *la géométrie variable* of the IT Agency is highlighted taking the changed legislative framework and the *non-Schengen* EU Member States not obtaining opt-out on the Schengen *acquis* into account.

In accordance with the Protocol on the Position of Denmark, Denmark decided to implement the SIS II and the VIS Regulation. By virtue of the same protocol, she does not take part in the adaptation of the EURODAC Regulation. However, Denmark applies the current EURODAC Regulation, following an international agreement.[87]

On the one hand, the United Kingdom and Ireland do not take part in the provisions of Schengen *acquis* in accordance with the protocol on their special status. On the other hand, concerning their request to take part in some provisions of the Schengen *acquis*, they are involved in the provisions relating to SIS II. But these countries are not taking part in the adoption of the provisions of Schengen *acquis* and are not bound by them or subject to their application insofar as they related to VIS.[88] The United Kingdom and Ireland are bounded by the EURODAC Regulation following their notice of their wish to take part in the adaptation and application of that Regulation based on their protocol attached to the Treaties.

On the basis of Recital 33 of the IT Agency Regulation, the United Kingdom notified the Council about her intention to take part in the adaptation of the regulation based on her

[84] Regulation (EU) No 1077/2011, *op. cit.*

[85] Regulation (EU) No 1077/2011, *op. cit.*, Art. 21, 28, 29 and 26, 13–14.

[86] *Ibid.* Art. 24, 13.

[87] Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 66, 8.3.2006, 38–43.

[88] Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis*, OJ L 131, 1.6.2000, 43–47; and Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis*, OJ L 64, 7.3.2002, 20–23.

Protocol annexed to the treaties. It means that the United Kingdom is be bound by the regulation and she is the subject to its application. But this fact does not affect the application of the VIS Regulation concerning the United Kingdom. Having regard to Recital 34, Ireland does not take part in the IT Agency Regulation.

Concerning the association of Norway and Iceland with the implementation, application and development of the Schengen *acquis*,[89] these countries are associates in SIS II and VIS. Furthermore, they are also associates with the EURODAC related measures.[90] The same legalisation technique was used concerning the association of Switzerland.[91]

Liechtenstein joined the agreements between the EU and Switzerland on the basis of protocols attached to the original agreements.[92] The Principality has been fully involved in large-scale IT systems as associate in the SIS II, VIS and EURODAC based on the protocols which are enclosed to the agreements concerning the association of Switzerland referred in the previous paragraph.[93]

Base on the accession treaties, Bulgaria, Cyprus and Romania are (and Croatia will be) the signatories of the Schengen Agreement, and the Schengen *acquis* is binding them, but they still do not implement these rules. On the one hand, there is the Cyprus dispute. On the

[89] Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen *acquis*, OJ L 176, 10.7.1999, 36–49.

[90] Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway, OJ L 93, 3.4.2001, 40–47.

[91] Cf. Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, OJ L 53, 27.2.2008, 52–79; and Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, OJ L 53, 27.2.2008, 5–17.

[92] Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, OJ L 160, 18.6.2011, 21–32; and Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, OJ L 160, 18.6.2011, 39–49.

[93] See also: Council Decision 2008/261/EC of 28 February 2008 on the signature, on behalf of the European Community, and on the provisional application of certain provisions of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, OJ L 83, 26.3.2008, 3–4; and Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Community, and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland, OJ L 161, 24.6.2009, 8–12.

other hand, the accession of Bulgaria and Romania is politically not supported in the Council. It means that these countries still do not participate in the SIS II and VIS. But they are participating in the EURODAC.

I did not mention the remaining twenty-one EU and Schengen Member Countries. Of course, they apply the Schengen rules, the SIS II, VIS and EURODAC Regulation.

In terms of the governance structure, the IT Agency facilitates the appropriate representation of users in the decision-making structures. The Agency is a Union body and has legal personality.[94] The administrative and management structure of it comprise a Management Board, an Executive Director and Advisory Groups.

The Management Board compose of one representative of each Member State, two representatives of the Commission and the representatives of the countries associated with the implementation, application and development of the Schengen *acquis* and the EURODAC related measures (hereinafter, associates). The terms of office of the Management Board's members are four years, which may be once renewed.[95] The Chairperson and its alternate are elected by the Management Board among its members for a two-year term, which may be once renewed. But the Chairperson may only be appointed from among those members who are appointed by Member States that participate fully in the adoption or application of the legal instruments governing all the systems managed by the Agency.[96] Each member of the board has one vote in the Management Board, i.e. not only the Member States but also the associates have one vote.[97] Voting right is guaranteed for a Member State if she is bound under Union law by any legislative instrument governing the development, establishment, operation and use of a large-scale IT system managed by the IT Agency.[98] Generally, the decisions shall be taken by a majority of its members with a right to vote.[99]

The Executive Director of the Agency shall be appointed for a period of five years by the Management Board among the suitable candidates identified in an open competition organised by the Commission. The Management Board shall take the decision by a two-thirds majority of all members with a right to vote. The European Parliament shall adopt an opinion setting out its view of the selected candidate. The term of office of the Executive Director could be extended once for up to three years. The Executive Director shall be accountable to the Management Board for his/her activities.[100] The Agency shall be managed and represented by its Executive Director who is independent in the performance of his/her duties. The Executive Director, *inter alia*, shall assume full responsibility for the tasks entrusted to the Agency. The European Parliament or the Council may invite the Executive Director of the Agency to report on the implementation of his/her tasks. The Executive Director shall ensure the Agency's day-to-day administration; prepare and implement the procedures, decisions, strategies, programmes and activities adopted by the Management Board.[101]

[94] Regulation (EU) No 1077/2011, *op. cit.*, Art. 10(1), 7.
[95] *Ibid.* Art. 13, 9.
[96] *Ibid.* Art. 14, 10.
[97] Cf. *Ibid.* Art. 16, 10 and Art. 37, 17.
[98] *Ibid.* Art. 16(3), 10.
[99] *Ibid.* Art. 16(1), 10.
[100] *Ibid.* Art. 18, 11–12.
[101] *Ibid.* Art. 17, 10–11.

The SIS II Advisory Group, the VIS Advisory Group, the EURODAC Advisory Group and any other Advisory Group related to a large-scale IT system when so provided in the relevant legislative instrument governing the developed, establishment, operation and use of that large-scale IT system shall provide the Management Board with the expertise related to the respective IT systems and, in particular, in the context of the preparation of the annual work programme and the annual activity report. For the membership and chairmanship of the Advisory Groups, the methods of the Management Board are applied *mutatis mutandis*. However, the terms of appointments are three years, which may be once renewed. And the Commission has one representative in each Advisory Groups. Furthermore Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS Advisory Group.[102] According to an amended proposal, Europol may appoint a representative to the EURODAC Advisory Group as well.[103] However, this proposal is not approved at the time of writing.

So, the Member States and the Schengen associated countries play an important role in controlling the systems as they are presented in the Management Board. The board and the Executive Director together carry out the day-to-day management of the IT Agency. It is necessary to establish the Advisory Groups to support the Management Board on system-specific issues in order to address issues arising from the different constituencies of the three current systems. The Commission is represented in the Management Board and in the Advisory Groups. Its influence on the budget and on the work programme would allow aligning of the operational management of large-scale IT systems with wider policy objectives. Furthermore, the democratic-control characteristic of the European Parliament is "ensured by the institutional mechanisms put in place to meet financial and management reporting obligations to which European agencies are subject".[104]

However, the complex and non-transparent structure of rules and procedures to accommodate *la géométrie variable* could involve governance risks as delays, inconsistent decision-making and reduced supervision.[105]

5. The Place of the IT Agency in the Complexity of the other "JHA Agencies"

In this phase of the analysis, it is worth to concentrate on the legal instruments of the SIS II and VIS and the existing and proposed legal instruments of EURODAC in order to identify the EU level agencies which have access to and/or influence on the large-scale IT systems. Hence is to define the status of these organisations in the everyday work of the IT Agency. For that a layer model is presented to highlight the interrelations.

The first layer is the *Agency level*. It means the incorporation of other agencies interests into the Management Board and into the Advisory Groups of the IT Agency. Europol and Eurojust have access to SIS II data based on the Article 41 and Article 42 of Council Decision 2007/533/JHA.[106] Europol also has access to VIS data in accordance with Council Decision 2008/633/JHA.[107]

[102] *Ibid.* Art. 19, 12.
[103] COM(2012) 254 final, *op. cit.*, 60.
[104] SEC(2009) 837, *op. cit.*, 23.
[105] *Ibid.* 100.
[106] Council Decision 2007/533/JHA, *op. cit.*, 77.
[107] Council Decision 2008/633/JHA, *op. cit.*

The IT Agency Regulation gives a legal solution for the involvement of the intentions of the Europol and Eurojust in the work of the IT Agency related to the SIS II and VIS. Article 15(4) grants observer status to Europol and Eurojust at the meetings of the Management Board of the Agency, when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Moreover, Europol can be an observer on the meetings of the board, when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, is on the agenda.

Furthermore, the Europol and the Eurojust may each appoint a representative to the SIS II Advisory Group. The same rules would be applicable for the Europol in connection with the VIS Advisory Group.[108]

Article 19(1)d takes further developments into account, since it says that any other Advisory Group can be set up, which relates to a large-scale IT system when in the relevant legislative instrument governing the development, establishment, operation and use of that large-scale IT system is so provided.

An amended proposal of the Commission wants to give the same powers to the Europol in relation to EURODAC as to SIS II and VIS, i.e. observer status in the Management Board (if a EURODAC related issue is concerned) and representation in the EURODAC Advisory Group.[109] At the time of writing, the proposal has not been approved yet.

The second layer is the *management level*. It encompasses the agency level and the "cross large-scale IT Agency relations". All these relations are regulated in separate legislative acts. It has been explicitly stated in Article 1(4) of the IT Agency Regulation, too.

As of now, only one "inter large-scale IT Agency act" is in force. The VIS have been harmonised with the Schengen Borders Code by a regulation.[110] The Visa Code[111] shall be applied from 5 April 2010. Article 54 harmonises the VIS Regulation with the Visa Code. It means that if the visa applicant is a person for whom an alert has been issued in the SIS for the purpose of refusing entry, it indicates a ground for the refusal of the visa.[112]

Article 6 of the IT Agency Regulation gives the possibility for the Agency to be entrusted with the preparation, development and operation of other large-scale IT systems. Therefore, it is worth to consider the "cross large-scale IT Agency relations" and the agency level together as another layer, called the management level.

The third layer is the *cooperation level*. As I have mentioned above, Europol and Eurojust are involved in the work of the IT agency on the agency level. To stretch the horizon, it is important to consider the cooperation of these JHA agencies with the other JHA agencies–such as CEPOL and FRONTEX. That is to be called as the cooperation level.

The Europol and the Eurojust are connected to other JHA agencies via formal cooperation agreements. The main focus of these innominated acts is to strengthen the operative cooperation among EU crime-fighting agencies. The JHA agencies have

[108] Regulation (EU) No 1077/2011, *op. cit.*, Art. 19(3), 12.
[109] COM(2012) 254 final, *op. cit.*, 59–60.
[110] Regulation (EC) No 81/2009, *op. cit.*
[111] Regulation (EC) No 810/2009, *op. cit.*
[112] *Ibid.* Art. 54(6)b, 24.

established an extended cooperation framework based on bilateral cooperation and information exchange. Moreover, a multilateral cooperation is planned among them.[113]

Only between Eurojust and FRONTEX, there is not a formal working agreement.[114] However, it is planned and fostered by the Commission, too. Between Europol and FRONTEX and between Europol and Eurojust exists operational cooperation, i.e. regular exchange of information in the framework of their operation. Europol and FRONTEX exchange strategic information mainly related to illegal immigration and cross-border crimes.[115] The Memorandum of Understanding on a Table of Equivalence allows the Eurojust and the Europol to exchange information up to and including the level of "restricted".[116]

These interrelations could have complementary influence on the operational practice of the IT Agency, since Eurojust, Europol and FRONTEX shall work together for the Standing Committee on operational cooperation on internal security.[117] Furthermore, the Standing Committee shall help to ensure consistency of their actions.[118]

6. Evaluation – The "Utility" of the IT Agency

Hence the added-value of the IT Agency is summed up like a SWOT analysis in order to define how the delineated development process of the large-scale IT systems' operational management contributes to the increase of the efficiency of the information power in order to decrease the security deficit thus contributing to a more secured Europe.

The added-value of the IT Agency is observed in terms of the following criteria: human rights, accountability and transparency. The analysis is the synthesis of the chapter's results and of the prior impact assessment.[119]

The centralisation of large-scale IT systems is the strength of the IT Agency, since it insures interoperability among the incorporated systems. It contains two further segments: the institutionalisation and the long-term cost-effective operation. The institutionalisation of the operational management creates clear ground for the accountability. The accountability of the IT Agencies is ensured by EU institutions. Furthermore, the IT Agency provides a visible and dedicated structure which is also more visible and approachable for the civil society. The long-term cost-efficiency is guaranteed by the fostered interoperability and by the preparation, development and operational management tasks related to other IT large-scale systems, which might be delegated to the IT Agency. The expenditures and the running costs are managed together. Many of the tasks related to the running of the systems, procurement and project management are overlapped for all of the systems managed by the Agency; meanwhile less staff shall be employed. Furthermore, the co-location of network

[113] 5816/10 Interim report on cooperation between JHA Agencies, Brussels, 29.1.2010; and 5676/11 Draft Scorecard – Implementation of the JHA Agencies report, Brussels, 25.1.2011.

[114] *Ibid.*

[115] 5816/10 Interim report on cooperation, *op. cit.*, 5. Cf. 5676/11 Draft Scorecard, *op. cit.*

[116] *Ibid.* 6. Cf. 5676/11 Draft Scorecard, *op. cit.*

[117] Council Decision 2010/131/EU of 25 February 2010 on setting up the Standing Committee on operational cooperation on internal security, OJ L 52, 3.3.2010, Art. 5(1), 50.

[118] *Ibid.* Art. 5(2), 50.

[119] SEC(2009) 837, *op. cit.*

installations also indicates synergies in installations, operational management and monitoring.

Conversely, the accommodation of *la géométrie variable* could be a weakness in the future operation of the IT Agency, since the IT Agency has to handle a complex matrix of legal environment where too many parties are involved on different legal bases and where not all parties use or participate in all segments of the IT Agency's work.

Furthermore, the IT Agency is not cost-efficient in short-term. The costs and time of setting up the Agency and the (hypothetical) transition to new location result in the loss off key staff, training costs and could result in delays in planning and deployment; which means discontinuity. In short-term, there would be also high overheads which would eventually decrease. These overheads could be the insufficient critical mass of operational activity to justify setting up dedicated governance and management structures which result in extra labour costs and redundancy at administrative level; since the long start-up time for the establishment of the IT Agency's organisation, due to legislative procedures and discussion about location, governance structure, employment of stuff could result in delays, staff turnover and probably additional maintenance costs to keep old hardware running. However, these significant start-up costs would be compensated by the achievement of a higher potential for exploiting operational synergies. The operational management of these systems would be more cost-effective in the long run.

The Agency could prepare, develop and manage other large-scale IT systems, too. It is a great achievement, a valuable opportunity concerning the operational management of large-scale IT systems, since the IT Agency creates a cost-effective institutional framework for the future development of new large-scale IT systems, for the integration of the other existing ones and for the further development of the SIS II, VIS and EURODAC.

Concerns which have been voiced about the possible creation of a 'big brother agency' are in relation to the possibility of function creep and the issue of interoperability. Function creep by the IT Agency can be avoided if the scope of (possible) activates of the IT Agency are limited and clearly defined in the founding legal instrument. The application of ordinary legislative procedure decreased the risk of this factor. The IT Agency Regulation is clear and enumerates well-defined tasks. However, the possibility of function creep is a clear threat.

Reflecting the concerns of *human rights*, the importance of the Charter of Fundamental Rights of the European Union has to be underlined. Furthermore, the EU law contains proper principles against ill-treatment. *Accountability* of the European Agencies is ensured by the European Parliament and the European Data Protection Supervisor. Moreover, the European Court of Justice and the General Court have full jurisdiction over the activities of the IT Agency. The EU also has applied several acts to ensure data protection of individuals.[120] Furthermore, the IT Agency is responsible for the protection of personal data.[121]

[120] E.g. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–39; and Regulation No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, 1–22.

[121] Regulation (EU) No 1077/2011, *op. cit.* Art. 28, 14.

Concerning *transparency*, the main problem is the above presented *la géométrie variable* related to the IT Agency. Delays in setting annual budget and work programme due to multi-level governance could lead to delays and inconsistent decision-making. The questions of different levels of countries' participation and new users in the SIS II, VIS and EURODAC could be addressed by putting in place differentiated procedures in the Management Board. The complex and non-transparent structure of rules and procedures are needed to accommodate *la géométrie variable*. It reduces the level of supervision giving more places to the risk of function creep.

Based on the above examined criteria and aspects, the establishment of the IT Agency has more advantages than negative impacts in the long run. The highlighted strengths and the opportunities constitute the added-value of the Agency, which are the followings: interoperability; the preparation, management and development of other IT systems; long-term cost-efficiency; centralisation and institutionalisation of the operational management of the large-scale IT systems; visibility and approachability for the civil society. These enumerated attributions have a clear connotation to the increase of efficiency of the information power, in particular to the issue of the interoperability, of the preparation, management and development of other IT systems, and of the centralisation and institutionalisation of the large-scale IT systems' operational management. It means that the establishment of the IT Agency and the development of the large-scale IT systems in the area of freedom, security and justice contribute to the decrease of the security deficit accordingly the examined aspects, criteria and processes, and regarding the presuppositions.

***

In a perfect world, immigration control would be a neutral policy facilitating the entry of those who have right to enter or reside, and preventing entry and ensuring removal of those without right to stay. In fact, there is a thin line between raising barriers and providing safeguards. The double requirement of enhancing security and facilitating travel has to be borne in mind at the time of evaluating all planned, for example, the smart borders initiative,[122] or existing Schengen *acquis.*

[122] COM(2011) 680 final, *op. cit.*