Zoltán Dóczi

Law Enforcement Large-Scale IT Systems in EU Internal Security and Migration Policies

Department of International and European Law

Supervisor:

Dr. Erzsébet Sándor Szalayné, JD, PhD, Habil.

habilitated professor

University of Pécs,
Faculty of Law, Doctoral School of Law

Ph.D. dissertation

Zoltán Dóczi

Law Enforcement Large-Scale IT Systems in EU Internal Security and Migration Policies

Gothenburg, 2016

SUMMARY

Borderless Europe raises the problem of increased security deficit. One of its segments may be counterbalanced by the control of immigration flow at the external borders that consists of three endeavours: the common border control policy, the common visa policy and the common asylum policy. The aim of the current research is to understand internal security and migration policies of the European Union through observing eu-LISA, the sole European Agency being a law enforcement large-scale IT system. Observing what kind of social preferences are reflected through the Agency, the EU internal security and migration policies can be more sophisticatedly characterised. The primary question is stretched by analysing all relevant law enforcement large-scale IT systems, i.e. those operating in the area of freedom, security and justice.

For the analysis, a methodological tool is developed proposing the relative measurement of three indicators such as accountability for acts, respect of human rights standards and transparent operation. Indicators are examined through the development process of the units of analysis (institutionalist approach) and through analysing the interactions among them and their environment (functionalist approach).

It is also conjectured in line with the proposed methodological tool that analysing the above three indicators the relationship of the examined law enforcement large-scale IT system with social beneficiality can be determined. Since it is a double conjecture, i.e. indirect inference, it shall be challenged to be proven. Testing this projection capacity, the tool is applied to comparable law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice.

The received results characterise reflected social preferences and social beneficiality if presumptions and limitations are accepted. In this way, the proposed methodological tool may be used for social measurement related to law enforcement large-scale IT systems.

Keywords:

Schengen • large-scale IT systems • law enforcement • eu-LISA • smart borders
information power • security deficit • facilitate travel

ÖSSZEFOGLALÓ

A határok nélküli Európa felveti a biztonsági deficit megnövekedésének problémáját. Ennek egy részét ellensúlyozza a bevándorlás ellenőrzése a külső határoknál, amelynek három fő eleme van: a közös határellenőrzési politika, a közös vízumpolitika és a közös menekültügyi politika. Jelen kutatás célja az Európai Unió belbiztonsági és migrációs szakpolitikáinak megértése az eu-LISA vizsgálatán keresztül, amely az egyetlen európai ügynökség, amely bűnüldözési nagyméretű információs rendszerként működik. Megvizsgálva az Ügynökségen keresztül tükrözött társadalmi preferenciákat az EU belbiztonsági és migrációs szakpolitikája pontosabban leírható. E kérdéskör kiterjed az összes releváns bűnüldözési nagyméretű információs rendszer vizsgálatára, amelyek a szabadság, biztonság és jogérvényesülés térségében működnek.

A kérdés megválaszolására kifejlesztett módszertan három indikátor összevetésén alapul, úgymint az elszámoltathatóság, az emberi jogok tisztelete és az átlátható működés. Ezt a három indikátort vizsgáljuk az elemzési egységek fejlődési folyamatában (institucionalista megközelítés), és az egymásra, illetve környezetükre való hatásuk alapján (funkcionalista megközelítés).

Összhangban a javasolt módszertannal a bűnüldözési nagyméretű információs rendszerek társadalmi hasznossága meghatározható a három indikátor elemzésével. Azonban a rendszerek társadalmi hasznossága közvetetten vezethető csak le a három indikátor alapján. Mindezért a módszer előrejelzési képességének vizsgálata során a módszertant a szabadság, biztonság és jogérvényesülés térségében tervezett, összehasonlítható bűnüldözési nagyméretű információs rendszerekre alkalmazva teszteljük.

Az előfeltevéseket és korlátokat elfogadva az eredmények jellemzik a rendszerek által tükrözött társadalmi preferenciákat és hasznosságot. Így a javasolt módszertan használható a bűnüldözési nagyméretű információs rendszerek társadalmi értékelésére.

Kulcsszavak:

Schengen • nagyméretű információs rendszerek • bűnüldözés • eu-LISA
intelligens határok • információs hatalom • biztonsági deficit • az utazás megkönnyítése

ACKNOWLEDGEMENTS

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this Ph.D. project. I would like to express my special appreciation and thanks to my supervisor Professor Dr. Erzsébet Sándor Szalayné, you have been a tremendous mentor for me. I would like to thank you for encouraging my research and for allowing me to grow as a researcher. Your advice on both research as well as on my career have been priceless.

I was fortunate enough to spend more than 1.5 years as an expert at the Department of European Cooperation of the Ministry of Interior, Hungary. I owe thanks to all my superiors, especially dr. Péter Stauber and Judit Ferkócza for the trust and allowing me to represent Hungary in numerous conferences including the tasks of the European Migration Network that equipped me with valuable experience.

In addition, a thank you to Dr. Tamás Molnár, who introduced me to large-scale IT systems, and whose passion for the topic had lasting effect resulting in two theses with your constructive supervision. I thank the Corvinus University of Budapest and especially Professor Elisabeth Kardos Kaponyi for the inspiring and supporting environment where I could start my research in 2008 as BA student continuing up to 2012 turning to be a Ph.D. student there.

My Ph.D. carrier would have been ended in 2013 without Dr. Ágnes Töttős, a former colleague at the Ministry, who took me under her wings directing me to Pécs and still supporting me in any academic issues. I am grateful for the University of Pécs and specifically to Professor László Kiss admitting me in the Programme and supporting me with merciful and flexible attitude in what the dedicated work of Csilla Dr. Kalmár Nagyné Ottohál shall be emphasised.

I am thankful for the teaching and publications opportunities for Professor Erzsébet N. Rózsa, Professor Laura Gyeney, Dr. Anna Péczeli, Dr. István Gellérthegyi, Dr. Bernadett Judit Lehoczki, Dr. Ágnes Kemenszky and Péter Stepper.

A special thanks to my family, to my partner and to my friends who tolerated the constant lack of time. Words cannot express how grateful I am for your even financial aid and for your couches all across Europe where I could sleep before a conference or a lecture. I am also grateful for Gothenburg including my thinker tree in front of our flat and all acquaintances here for getting me out of the groove and making me start putting down all my thoughts.

Thank you all.

TABLE OF CONTENTS

List of Figure and Table

List of Abbreviations

CEAS	Common European Asylum System
CoE	Council of Europe
ECHR	The Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EU	European Union
eu-LISA	Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EURODAC	European Dactylographic System
Eurosur	European Border Surveillance System
ICCPR	International Covenant on Civil and Political Rights (1966)
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination (1965)
JHA	Justice and Home Affairs
PNR	Passenger Name Record
RTP	Registered Traveller Programme
SBC	Schengen Borders Code
SIS	Schengen Information System
SIS II	Second Generation of the Schengen Information System
UDHR	The Universal Declaration of Human Rights (1948)
UN	United Nations
VIS	Visa Information System

Introduction

The abolishment of the internal border checks makes it easier for people to move around. We can travel freely in the Schengen area, which makes for economic, regional and cultural dynamism within Europe and especially at the border areas. Any foreign visitor can travel to all Schengen States on a single visa, which means, for example, that economic activity related to tourism is promoted. At the same time, the Schengen cooperation aims to protect people and their property, since it fosters the cooperation among police forces, customs authorities and external border control authorities of the Member States in order to decrease the security deficit formed with the abolition of internal borders. The Schengen *acquis* provides systems of communication for police forces, hot pursuit of criminals and the cross-border surveillance of suspects, as well as mutual operational assistance and direct exchanges of information among police authorities. In parallel, strict uniform rules have been adopted to ensure the protection of data and to protect people against any infringement of their fundamental rights. Moreover, mutual assistance in criminal matters lays more emphasis on consequences of law breaching promoting the work of law enforcement agencies with cross-border deterrence.

In the flow of European integration, three, in the beginning, separated policy areas have been elaborated for handling the challenges of the cross-border security deficit caused by the fall of Schengen internal borders. For managing the common internal security risks of *Schengenland*, slowly approaching policy areas can be observed, namely, common border control policy, common visa policy and common asylum policy.

All policy areas are supported by systems that gather and store systematic data in order to satisfy criminal law claims deriving from the risk of breaching rated *acquis* and even national provisions. Therefore, the aggregated claims of nation states has resulted in large-scale systems filling the perceived the security gap of borderless Europe. Gathering and storing systematic data in mass volume, it is reasonable to encompass the advancement of information technology. The fact, that each policy area created its own large-scale IT system operating in the area of freedom, security and justice is called the exploitation of information power. It means that the European Union (hereinafter: EU) established the legal instruments for large-scale IT systems supporting law enforcement, which are embodied as the Schengen Information System (hereinafter: SIS), the Visa Information System (hereinafter: VIS) and the European Dactylographic System

(hereinafter: EURODAC). On the whole, irregular migrants found in Member States can be registered in the SIS, but irregular migration defies this registration itself. The SIS was further developed establishing the Second Generation of the Schengen Information System (hereinafter: SIS II). Those who enter through asylum procedures are registered in EURODAC and those who enter using a legal channel, i.e. being issued a visa are registered by the VIS.[1]

The consideration of the integration of all these systems into one "European Information System" is not a new desire.[2] The creation of a *Big Brother* Agency, as it was trendy to refer to, opened up the possibility to use information power more concentrated desiring to contribute more effectively to fight against terrorism, organised crime, human trafficking and irregular immigration. The Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, which is the so-called eu-LISA, implements a cohabitation of the existing systems using multilevel governance which is separated on operational level. The Agency is regulated by the so-called eu-LISA Regulation.[3]

The integration of the above existing systems were found not to comprehensively cover all presided security challenges. Moreover, the facilitation of travel is frequently brought into the limelight in connection with competitiveness. Therefore, in line with the Post-Stockholm Programme (however, well before that), the Smart Borders Package[4] was submitted by the European Commission aiming at the establishment of the new systems, i.e. the Registered Traveller Programme (hereinafter: RTP) and the Entry/Exit System (hereinafter: EES). The basic role of the RTP would be to ensure fast and simple border crossings for third country nationals at the external borders. The EES would take the challenge of establishing a more effective monitoring tool for travel flows and for the movements of third country nationals across the external borders.

The proposed systems are interesting in the light of the Member State planned or operated and EU level planned Passenger Name Record (hereinafter: PNR) data exchanges. Patterns for PNRs are important, since they not only have border crossings

[1] For precise description of division of labour among the existing systems, see: Ch. II.2.
[2] Broeders, Dennis, "The New Digital Borders of Europe – EU Database and the Surveillance of Irregular Migrants", *International Sociology*, 22(1), 2007, pp. 71-92.
[3] 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, pp. 1-17.
[4] "Smart Borders Package", *European Commission, DG Home Affairs*, http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm#/c_, [9.3.2013.].

registration, but also criminal intelligence features making them able to be used pre-emptively.

The multitude of existing and planned systems raises the problem of their connectedness with each other and with Justice and Home Affairs Agencies (hereinafter: JHA Agencies).[5] Moreover, it is very topical to understand the underlying social processes catalysing the establishment of such systems. This is the key motive behind the current research, i.e. understanding the emergence of the systems, interpreting them in their environment and defining their relevance in EU internal security and migration policies that together may help comprehend their reflected societal patterns.

[5] The author deliberately uses JHA Agencies aiming at referring to the time of their establishments. As of writing, the Agencies are operating in the area of freedom, security and justice.

I. Hypotheses and Methodology

Eu-LISA is a law enforcement large-scale IT system, since it supports law enforcement agencies with systematic data gathering. It means that the stored information is of assistance to all eu-LISA users in relation to their day-to-day operation. However, it shall be borne in mind that the Agency incorporates the operational management of three separately also exiting law enforcement large-scale IT systems so their functioning and interaction inevitably effect eu-LISA.

1. The Research Question

Eu-LISA according to the author's view has a double aim to deal with. On the one hand, internal security of *Schengenland* shall be supported. On the other hand, the Agency has designated role in relation to the management of migration flows.

The aim of the current research is to understand internal security and migration policies of the European Union through observing eu-LISA as the sole European Agency being a law enforcement large-scale IT system. Observing what kind of social preferences are reflected through the Agency, the EU internal security and migration policies can be more sophisticatedly characterised.

It means that the main focus of the research is to define what social preferences are reflected through eu-LISA which is interpreted as a law enforcement large-scale IT system.

2. Observing *Big Brother Features*: A Methodological Tool for Social Measurement of Law Enforcement Large-Scale IT Systems

The aim of the current section is to propose a methodological tool for the observation of information power used in law enforcement large-scale IT systems.

In line with the starting point of the mainstream literature, information power in the current context is the access to information and the control over its distribution.

It is conjectured that information technology used in law enforcement large-scale IT systems may have special, *Big Brother features* which can be characterised by the

position of the systems in social processes. On the basis of the features, indicators can be set in order to qualitatively describe the systems.

2.1.Paradigm Intersections: *Big Brother Features* in Theories

An ideal-typical identification of information power used in law enforcement large-scale IT systems can be defined by defining the position of information power in social processes. The combination of control society paradigm including surveillance society and risk society theories[6] with the theoretical framework of intelligence cycle approach could give an account of the problem.

Demand Side: Why are Law Enforcement Large-Scale IT Systems Needed?

The notion of risk is hidden behind today's processes concerning crime control. It has resulted in the converting relationship between freedom and security which are more likely opposing being hardly complements to each other. Concerning risk society theory, information and knowledge have gained greater role, since they are crucial in how to handle and manage threats.[7] However, the knowledge is reflexive, i.e. there is no such a thing as objective knowledge. Therefore, the cognoscibility of risks is characterised by considerable uncertainty.[8] To sum up, risk society is determined by information which applies to risk.

Even so, risk does not bypass morality; it alters its basis aiming at the utilitarian predictability of social institutions.[9]

In criminal control, risk is recognition of criminal risk, its effective neutralisation and minimisation of damage. However, fear creates market for risk society. Fearing of fear constellates a vicious cycle around risk societies, which results in a need which never can be satisfied for managing fear-constellated risks.

If an over ensured process occurs, not only the rights of criminals are infringed. Technological and scientific developments make intense control possible. The control

[6] Cf. Bárd, Petra and Borbíró, Andrea, "Kontrollálatlan kontrolltársadalom", *Kriminológiai tanulmányok*, 47(1), 2010, pp. 87-112.
[7] Beck, Ulrich, *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Frankfurt am Main, Subrkamp Verlag, 1986, pp. 25-66.
[8] Giddens, Antony, *The Consequences of Modernity*, Stanford, Stanford University Press, 1990, p. 40.
[9] Ericson, Richard V. and Haggerty, Kevin D., *Policing the Risk Society*, New York, Oxford University Press, 2001 (reprint), originally published in 1997, pp. 39-40.

tries to tackle public security problems. However, this solution raises many legal and ethical conflicts as well. These conflicts are natural, as BECK said, about the close interconnectedness of secularisation and risk:

> "When Nietzsche announces: God is dead, then that has the – ironic – consequence that from now on human beings must find (or invent) their own explanations and justifications for the disasters which threaten them."[10]

For the management of risk, control society theory proposes the presence and spread of surveillance techniques. According to the theory, surveillance techniques are merged into a system which is called *surveillant assemblage*.[11] The current control culture expends reframing the scope of democracies. *Surveillant assemblage* is a specific pattern of control society. It is an enormous network which is embodied as joining control culture organising all fields of social life and technology up. The chance of being disappeared has disappeared in this system.[12] On the one hand, more and more moments of one's life are cognoscible, recordable, retrievable, analysable and organisable. On the other hand, increasing number of players can have the chance to get the data into their possession. Therefore, today's postmodern surveillance society is the agglomerate of various tools for surveillance and of multitude of players' different motivation to use them.

Supply Side: What do Law Enforcement Large-Scale IT Systems Offer?

The intention of centralisation of information in law enforcement large-scale IT systems, i.e. of the increase of information power, has a clear connotation related to intelligence studies. The intelligence process can explain significant connections. Applying it in this context, the increase of information power is not more than the processing and exploitation phase of the intelligence cycle.[13] LOWENTHAL analysing CIA materials pointed out that there are only two reference points to give feedback to the processing and exploitation phase of the intelligence cycle: the consumption phase and the analysis and production phase.

---

[10] Beck, Ulrich, "Living in the world risk society – A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics", *Economy and Society*, 35(3), 2006, p. 333.
[11] Haggerty, K. D. and Ericson, R. V.: "The Surveillant Assemblage", *British Journal of Sociology*, 51(4), 2000, pp. 605–622.
[12] *Ibid*, p. 619.
[13] Cf. Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, 2nd ed., Washington, CQ Press, 2003, pp. 41-53.

It is highly true that in democracies constitutional guarantees do not allow the abuse of power or ill-treatment. However, the realist idea of the *raison d'État* and the legally 'special' status of intelligence shall be taken into account. The more the stored amount of files and the access points, the easier it is to create high quality intelligence reports.

As it has been referred to in the demand part, information power is socially embedded. Decision makers and analysts of law enforcement large-scale IT systems, i.e. intelligence users and its makers are in interaction. In this way, law enforcement large-scale IT systems offer reports along orientations which can be focused onto the product (report quality) or onto the market (report outcome). Production orientation means the observation of the threat and its objective handling. Market orientation depends on what kind of report outcome is perceived to be desirable for the decision makers.

***

Intelligence always has been a grey byway in democratic systems. Decision makers are interested in a deeper cooperation to increase the efficiency and the amount of the stored data and of the access quality. Conversely, even decision makers shall harmonise their endeavours with the checks and balances of the rule of law. This double requirement defines the perceptions of the political players and of the state administration, which builds up the *surveillant assemblage* nature of law enforcement large-scale IT systems. It resulted in a more enhanced use of information technology counselling their *Big Brother features.*

2.2.Social Measurement of Law Enforcement Large-Scale IT Systems

Developing indicators, dependent and independent variables shall be set. Concerning the social measurement of law enforcement large-scale IT systems, the *Big Brother features* set out above can be used as dependent variables. For the point of reference in relation to their measurement, the application of democratic theory is proposed, which serves as starting point for defining the independent variables.

The Aristotelian roots of democratic theory address polity focusing on the way to achieve good, just and stable polity. Interpreting law enforcement large-scale IT systems as social institutions hedging socially constructed threats, their institutional arrangements

shall be reflected onto polity criteria set by democratic theory. All social institutions can be interpreted in their environment. Consequently, the institutional arrangements of law enforcement large-scale IT systems shall be measured by 'how good, how just and how stable' they are in their environment. In this context, they can be used as independent variables.

Therefore, it is to be proposed to use accountability for measuring 'good', application of human rights standards for measuring 'just' and transparency for measuring 'stable' as indicators for social measurement of law enforcement large-scale IT systems. This is also conjectured by PAPAGIANNI in migration policy context saying that policy making process in migration could lead to serious concerns, in particular, regarding transparency, accountability and human rights.[14]

Evaluating the optimality of an observed law enforcement large-scale IT system following the measurement along the three indicators, it is important that the indicators shall balance each other. The reason for it derives from the starting point. In democratic theories, the *Dahlian 'polyarchy',* i.e. the pluralist interplay of groups is viewed as democracy. HUNTINGTON worried about a 'democratic distemper' in which citizens demand more than the system can deliver. So transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement.

***

Society's acceptance of new technologies in law enforcement has three levels such as the technology and research, the technology and privacy, and the technology and society.[15] Concerns with a new technology will decrease if that technology is fully integrated and accepted in the society. Social measurement of law enforcement large-scale IT systems may be of assistance in relation to the evaluation of their level of acceptance.

[14] Papagianni, Georgia (ed.), *Institutional and Policy Dynamics of EU Migration Law*, "Immigration and Asylum Law and Policy in Europe", vol. X., Leiden, Martinus Nijhoff Publications, 2006, p. 320.
[15] Pattavina, April (ed.), *Information Technology and the Criminal Justice System*, University of Massachusetts at Lowell, Sage Publications, 2005, pp. 261-271.

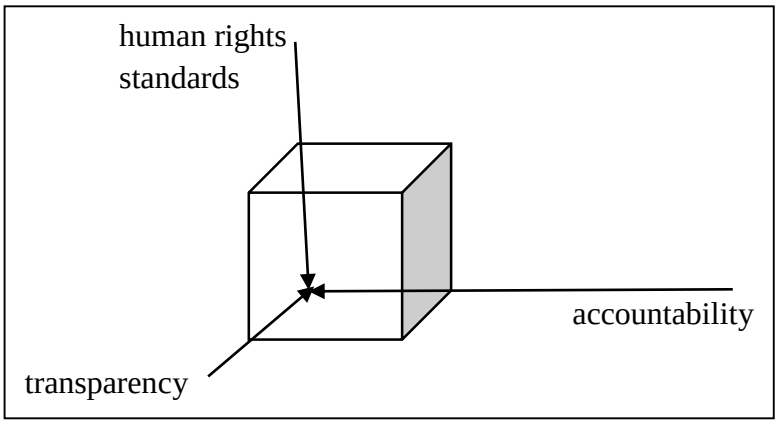
2.3.A Proposed Methodological Tool for the Measurement of Law Enforcement Large-Scale IT Systems

As a synthesis of the above presented results, the following method is proposed to examine law enforcement large-scale IT systems. According to risk society theory, as a presumption, it is to be established that the more a law enforcement large-scale IT system possibly could supply the more the demand there is for the system.

Based on the theories above, these systems are available i.e. rational to set up if the established three indicators intersect. Social beneficiality depends on accountability, human rights standards and transparency features of the observed law enforcement large-scale IT system.

Thus, it can be inferred that law enforcement large-scale IT systems work socially beneficial if they are accountable for their acts, respect human rights standards, and are transparent. Moreover, these systems work optimally if demand (i.e. why law enforcement large-scale IT systems are needed) and supply (i.e. what law enforcement large-scale IT systems offer) intersect. Whereas the position of optimum is determined by social preferences.

Figure 1. Socially Beneficial Law Enforcement Large-Scale IT Systems



It follows that the examination of the three independent variables (i.e. accountability, human rights standards and transparency) indicate the social preferences reflected through the observed law enforcement large-scale IT system assuming that the system operates in the optimum.

3. Research Outline

Below the scope and the envisioned content of current research is outlined giving special attention to structuring research design around hypotheses and relevant conjectured relationships.

As follows from the research question, the core hypothesis is formulated such as

H1 ***What kind of social preferences of EU internal security and migration policies are observed through law enforcement large-scale IT systems operating in the area of freedom, security and justice?***

It calls for the exact specifications of expressions used.

"EU internal security and migration policies": It defines the scope of research. The author underlines that EU home affairs policies (or policy) are deliberately not referred to. Using secure and facilitate dichotomy for interpreting information power channelized through and concentrated in law enforcement large-scale IT systems operating in the area of freedom, security and justice, the borderline policy areas in relation to EU home affairs policies may distort results.

"law enforcement large-scale IT system": It is a system supporting law enforcement agencies with systematic data gathering in mass volume through which the below special features can be established.

(1) Gathering and storing systematic data in mass volume, it is reasonable to encompass the advancement of information technology, which opens up the possibility to use information power.

(2) In line with the starting point of the mainstream literature, information power in the current context is the access to information and the control over its distribution.

"law enforcement large-scale IT systems operating in the area of freedom, security and justice": It defines the unit of analysis. It can be argued that area of

freedom, security and justice is a notion strongly associated with EU home affairs policy. However, solely the effects of the systems on EU internal security and migration policies are observed. Eu-LISA is a law enforcement large-scale IT system operating in the area of freedom, security and justice storing information in mass volume that are of assistance to all eu-LISA user law enforcement agents. Nevertheless, it shall be borne in mind that the Agency incorporates the operational management of three separately also exiting law enforcement large-scale IT systems so that their functioning and interaction inevitably effect eu-LISA. It means the functioning of SIS, VIS and EURODAC shall be examined as well in the mentioned context.

To answer the preliminary research question set out by H1, the proposed methodological tool is tested using institutionalist and functionalist approach. The proposed three indicators such as accountability for acts, respect of human rights standards and transparent operation are examined through the development process of units of analysis (institutionalist approach) and through analysing the interactions among them and their environment (functionalist approach).

For demonstration, context shall be broken down as follows.

H1a Was the development process of the observed law enforcement large-scale IT systems operating in the area of freedom, security and justice inherent?

Findings of institutionalist analysis map underlying social processes since the formation of such systems.

H1b How are the existing specific law enforcement large-scale IT systems operating in the area of freedom, security and justice designed and how do they operate?

It gives functionalist exploration of SIS, VIS and EURODAC aiming at supporting the above indicators.

H1c (How) has the integrated operational management of existing specific law enforcement large-scale IT systems operating in the area of freedom, security and justice changed their functioning?

Combining institutionalist description of eu-LISA with analysing interactions among the Agency, the systems and their environment (functionalist mindset) finetune

the preliminary results and face theory (i.e. legal provisions and legislative purpose) with reality.

According to the proposed methodological tool, it is conjectured that H1a-c results reflected through the three proposed indicators can answer H1 primary research question. Namely, having H1a-c results elaborated in terms of accountability for acts, respect of human rights standards and transparent operation can characterise social preferences of EU internal security and migration policies in the current theoretical framework.

It is also conjectured in line with the proposed methodological tool that analysing the above three indicators the relationship of the examined law enforcement large-scale IT system with social beneficiality can be determined. Since it is a double conjecture, i.e. indirect inference, it shall be challenged to be proven.

To challenge H1 results that are reflected through social preferences, the following is proposed.

H1/sideH1 Observing law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice, the projection capacity of the proposed methodological tool can be tested.

"law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice": The same is valid as above for not planned ones. Eu-LISA is capable of incorporating the operational management of further law enforcement large-scale IT systems regardless of current arrangements.[16] It means that the planned functioning of RTP, EES as well as the patterns of PNRs shall be examined.

"projection capacity": It is the capacity of the above established indicators (accountability for acts, respect of human rights standards and transparent operation) if being projected to determine social beneficiality of the observed system.

"tested": It means the comparison of social preferences reflected through planned and the existing law enforcement large-scale IT systems operating in the area of freedom, security and justice.

[16] See: Ch. II.3.3.

H1/sideH1a Are existing and planned law enforcement large-scale IT systems operating in the area of freedom, security and justice comparable?

Deriving from the characteristics of the existing ones, the mentioned systems are comparable if they are tackling the same challenges of the area of freedom, security and justice. In the current context, it means balancing security needs of *Schengenland* and facilitating people movement within, to and outwards the area by using information power. To handle the dichotomy, an analogy is needed as benchmark. For the purpose, EU return and readmission policy is adequate, since it handles security perspective as long as dealing with competing provisions of right to leave and of obligation to (re)admit to facilitate (mainly forced) migration flows.

If comparability is proved, social preferences reflected through planned and existing systems are also comparable. In this way, indirect interference of indicators' projection capacity is challenged, since today's social preferences are reflected in nowadays decided plans. It means that if the same social preference patterns come out of the analyses of existing and planned systems, the social beneficiality of the existing law enforcement large-scale IT systems can be determined on the basis of and by accepting the presumptions of the proposed methodological tool.

As far as limitations of the scope concerned, the research solely focuses on international migration, i.e. cross-international-border movement of persons, and related law enforcement large-scale IT systems. Therefore, for example, by referring to EU law enforcement large-scale IT systems, Customs Information System (CIS) or European Criminal Records Information System (ECRIS) are out of the scope.

The research is also limited in time. Relevant information sources, legislations, proposals as well as academic literature are examined that were issued before 31 January, 2016. EU documents such as founding treaties, communitarised international treaties, regulations, directives, council decisions, commission documents, EU policy documents and other preparatory documents are used as primary sources. Due to the nature of this topic high on the political agenda, predominately the primary sources are examined at the first instance. Furthermore, the academic literature related to the topic is worked up. After repeated systematic searches for relevant sources of academic literature, any fully relevant Hungarian work has not been detected. Mainly Anglo-Saxon and European literature was found and researched. In particular, concerning journals and periodicals,

the *European Journal of Migration and Law* contains several relevant sources. Primary and secondary sources are synthesised in order to give the most suitable interpretation of the above detailed problem. Moreover, working experience and previous scientific activities were of assistance to the current research, too.

II. Existing Law Enforcement Large-Scale IT Systems in EU Internal Security and Migration Policies

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

Examining their roots as well as their relations to EU treaties could support the current analysis with findings on characterising social preferences and motives behind them. Such examination is inevitable, since the integration of the systems into eu-LISA poses the question of approached treaty arrangement. For an effective governance of agencies, common denominators of agents' legal basis are needed to be established otherwise the new governing structure turns out to be an ivory tower of red tape and of inconsistent decisions.

Mapping underlying social preferences of EU internal security and migration policies related through law enforcement large-scale IT systems, functioning and institutional arrangements of the systems are outlined. It is conjectured that the establishment of the systems was part of an inherent development process. Analysing the process, firstly, the relationship of the systems with EU treaties is observed to understand their today's multi-level governance more deeply. Then the exploration of the systems including eu-LISA follows in order to interpret the interactions among them and their environment.

Evaluation of findings is sorted by the indicators of accountability for acts, respect of human rights standards and transparent operation set out in the above methodology. According to presumptions, reflected social preferences of EU internal security and migration policies become distinct via such analysis.

1. Incorporation Process of Law Enforcement Large-Scale IT Systems into the European Treaty Regime

In the section, core legislative milestones concerning large-scale IT systems operating in the European Union are observed. These legislations such as Community and intergovernmental legal acts have created fundamental legal basis for the systems. It means that the development process and the current place of existing law enforcement large-scale IT systems in EU law are to be defined.

The incorporation process of large-scale IT systems into the European Treaty regime can be divided into three phases. The first attempts of the legal core regulations had an "outsider *laissez passer*" feature, since they were a special mixture of intergovernmental and Community acts. In the second phase, the intergovernmental legislations were communitarised. However, the three-pillar Europe could not incorporate the legal grounds of EU large-scale IT systems in a unified manner. Therefore, a complexity of rules of procedures was born in order to handle the cross-pillar nature of the common border control, visa and asylum policy. Only the Lisbon Treaty made it possible to handle the matrix of law enforcement large-scale IT systems as one, unified management system for the external borders, which is considered as the third stage in the incorporation process. Hereinafter, the three phases are detailed.[17]

1.1. The Beginnings: Mixing the Treaty Regimes

The establishment of large-scale IT systems within the framework of the European integration may be considered as a spill-over process. For the implementation of the single market, Member States approved the Single European Act[18] (hereinafter: SEA). Article 13 of SEA modified the EEC Treaty. The EEC Treaty was amended with Article 8a, requiring the Community

> "to adopt measures with the aim of progressively establishing the internal market over a period ending on 31 December 1992".

[17] In his paper, De Capitani excellently interprets Schengen system after Lisbon elaborating on its incorporation process. See: De Capitani, Emilio, "The Schengen system after Lisbon: from cooperation to integration", *ERA Forum*, 15(1), 2014, pp. 101-118.
[18] OJ L 169, 29.6.1987.

That means the abolishment of the fiscal, physical and technical barriers along the borders of members of the EEC. The 1992 Maastricht Treaty (the Treaty on European Union, hereinafter: TEU) transformed these rights to the level of single citizens. The four basic freedoms have already become a reality in the European Union.

However, the Schengen integration stated before TEU or SEA. The Benelux Economic Union, the Federal Republic of Germany and the French Republic signed first the Schengen Agreement[19] (hereinafter: the Agreement) in 1985 and then the Convention implementing the Schengen Agreement[20] (hereinafter: the Convention) in 1990. These are intergovernmental agreements i.e. these legal acts were not originally part of the Community legal system. After the accession of some more Member States to the Agreement and the Convention, they entered into force in 1995.[21]

The principle of the Agreement is the abolishment of internal border checks among its signatories. In order to implement this objective the Agreement drew up a detailed list of measures to be agreed upon. The Convention defined more elaborated rules on abolishing internal border checks, strengthening external borders, harmonising visa policy, and regulating movement of third country nationals among its signatories in Articles 1-25. Further rules were set out on combating irregular immigration[22], allocating responsibility for asylum requests[23], addressing criminal judicial cooperation and police cooperation issues[24], and creating a database which is the Schengen Information System (SIS) in Articles 92-119.[25]

The abolishment of internal border checks obviously entails higher security risks. As STEVE PEERS explains "the underlying logics of Schengen rules was that there must be extensive 'compensatory' measures, including a common visa policy and a transfer of checks to the external borders of the signatories, in order to ensure that internal border checks could be abolished without a corresponding loss of security"[26]. The Agreement and the Convention are the core legislation preparing the field for the SIS.

It shall be mentioned that there were three segments to ensure the security in the foreseen *Schengenland*. The SIS decreases the security deficit inside the Schengen area;

[19] OJ L 239, 22.9.2000, pp. 13-18.
[20] OJ L 239, 22.9.2000, pp. 19-62.
[21] An Annex of the 1997 Amsterdam Treaty communitarised the Schengen *acquis*.
[22] *Ibid,* Art. 26-27, p. 25.
[23] *Ibid,* Art. 28-38, pp. 25-28.
[24] *Ibid,* Art. 39-91, pp. 28-42.
[25] See also: Peers, Steve, *EU Justice and Home Affairs Law*, "Oxford European Community Law Series", 2nd ed., Oxford and New York, Oxford University Press, 2006, p. 97.
[26] *Ibid.*

in parallel, the Visa Information System (VIS) gives a reliable reference point for the selection of the entering third country nationals and avoids visa shopping. The third missing segment was the asylum component. The other IT systems could be inefficient if common minimum standards are not required for the asylum applications. The EURODAC is the large-scale IT system filling the gap. It has been set up for being an EU wide tool that helps to determine which Member State is responsible for examining an asylum claim.

The EURODAC is a coherent part of the "Dublin process". The Schengen Implementing Convention also contains measures in relation to asylum law, which were replaced by the measures of the Dublin Convention[27]. The Dublin Convention was signed by all members of EEC in 1990 and entered into force in 1997; and it was part of Community law. The Dublin Convention was replaced by the Dublin II Regulation[28] in 2003, which refined the responsibility of the Member State related to asylum application procedure.[29]

Not all of the Member States were ready to accept the idea of the common visa and common asylum policy in order to counterbalance the abolishment of the internal borders. Some of them (especially the United Kingdom) did not want to join either the Schengen Agreement or the Schengen Implementing Convention. These could be additional reasons why these legal acts took a longer period to enter into force.

The 1992 Maastricht Treaty is the first milestone in the field of Justice and Home Affairs (JHA), since it gave rise to the so-called pillar system. Concerning visa and border issues, the TEU introduced two important articles. Article 100c was inserted into the EC Treaty. The Community got the scope of authority for example to "determine the third countries whose nationals must be in possession of a visa when crossing the external borders of the Member States"[30] and to "adopt measures related to a uniform format for visas"[31]. In Article K.1 there are other provisions delegated the competence to the third pillar such as the "asylum policy"[32], rules on the crossing of external borders of the

[27] Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention, 19.8.1997, OJ C 254, pp. 1-12.
[28] 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, pp. 1-10.
[29] Peers, Steve, *EU Justice and Home Affairs Law, op. cit.*, p. 303.
[30] Treaty on European Union, OJ C 191, 29.7.1992, Art. 100c(1).
[31] *Ibid*, Art. 100c(3).
[32] *Ibid*, Art. K.1(1).

Member States "and the exercise of controls thereon"[33], and the " immigration policy and policy regarding nationals of third countries"[34].[35] The division of competence for visas between the First and Third Pillars under the Maastricht Treaty is a result of political compromise among the Member States. That is the reason why the Council adopted an across-the-pillar approach where the circumstances required so.[36]

Meanwhile, the Schengen Implementing Convention entered into force in March 1995. On the one hand, the measures of the Convention were implemented. On the other hand, the Executive Committee adopted further measures belonging to the sphere of visa and border control issues.

1.2. Separated Incorporation

The Treaty of Amsterdam[37] gave more power to the EC in connection with delicate questions. The Third Pillar of the Maastricht Treaty was regarded as an anteroom of certain themes by a number of Member States, which shall be communitarised. At the price of three Member States' opt-out, the Amsterdam Treaty communitarised many areas which were previously within the scope of the Third Pillar.[38] It should be noted herein that these opt-outs pertain to the application of the so-called Schengen *acquis* that had not been the part of the community law before the Amsterdam Treaty.

The 1997 Amsterdam Treaty fundamentally changed the structure of JHA which might be the most important achievement of the Treaty[39]. The progressive establishment of the area of freedom, security and justice became the aim of the European Community. This endeavour has been based on the idea of the free movement of persons.

Title IV was added to the EC Treaty by the Treaty of Amsterdam addressing "visa, asylum, immigration and other policies related to free movement of persons". Concerning visa and border issues, the tools to achieve to above-mentioned goals are set out in Article 62 EC. Article 62(1) EC clearly refers to the abolishment of the internal border checks stating the "the absence of any controls on persons, be they citizens of the Union or

[33] *Ibid*, Art. K.1(2).
[34] *Ibid*, Art. K.1(3). See also in particular: *ibid*, Art. K.1(3)a-c.
[35] See also: Peers, Steve, *EU Justice and Home Affairs Law*, *op. cit.*, pp. 98-100.
[36] Meloni, Annalisa, *Visa Policy within the European Union Structure*, Berlin, Springer, 2006, pp. 138-141.
[37] Treaty of Amsterdam Amending the Treaty on European Union, the Treaties establishing the European Communities and Relates Acts, OJ C 340, 10.11. 1997, pp. 1-144.
[38] Meloni, Annalisa, *op. cit.*, p. 124.
[39] Cf. Treaty on European Union, *op. cit.*, Art. K.9.

nationals of third countries, when crossing internal borders". Other related measures such as those concerning asylum and immigration policy, external and internal border control and judicial cooperation in civil matters became First Pillar issues, and consequently the part of the EC law since the Treaty of Amsterdam came into force. Visa policy as a whole was transferred to the First Pillar, too. However, as MELONI highlighted, the nature of visa policy, "because of its ramifications, continues to be a subject with straddles all the Pillars of the Union."[40] It "reflects such a state of affairs."[41]

The communitarisation of the Schengen Agreement and the Schengen Implementing Convention, respectively of the Schengen *acquis* was a great achievement of the 1997 Amsterdam Treaty. Accordingly, the enclosed protocol of the Treaty of Amsterdam set for the implementation of the Schengen Agreement and the related legislation to the framework of the European Union to achieve the communitarisation of external border checks such as the abolishment of internal border checks and the merger of external border checks.[42] The Treaty of Amsterdam entered into force on 1 May 1999. After that date, the Schengen *acquis* was inducted to the First or to the Third Pillar depending on their jurisdiction and these legislations has become coherent part of EC law, i.e. the acceding countries shall accept them.[43]

The United Kingdom of Great Britain and Northern Ireland and the Republic of Ireland have never signed either the Schengen Agreement or the Schengen Implementing Convention. Referring to their special status, these countries do not have to apply the Schengen Agreement and the related Schengen *acquis*.[44] The Treaty of Amsterdam gave the third opt-out to the Republic of Denmark. The country has the right to decide case by case about the application of new EC legislations on the field of the Schengen *acquis*.[45] The protocols effect on the common asylum law, too, i.e. they shall be taken into account in connection with the "Dublin process" and consequently in relation to the EURODAC.

[40] Meloni, Annalisa, *op. cit.*, p. 141.
[41] *Ibid.*
[42] Protocol integrating the Schengen *acquis* into the framework of the European Union, OJ C 340, 10.11. 1997, pp. 93-96.
[43] Council Decision 1999/436/EC of 20 May 1999 determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen *acquis*, OJ L 176, 10.7.199, pp. 17-30. Cf. Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen *acquis* for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the *acquis*, OJ L 176, 10.7.1999, pp. 1-16.
[44] Protocol on the position of the United Kingdom and Ireland, OJ C 340, 10.11. 1997, pp. 99-100.
[45] Protocol on the position of Denmark, OJ C 340, 10.11. 1997, pp. 101- 102.

The 1997 Amsterdam Treaty inserted Article 63(1) and 63(2) into the EC Treaty, conferring powers upon the Community to adopt measures concerning asylum and international protection. Asylum powers were subject initially to standard rules applying Title IV (First Pillar). The Treaty attached a Protocol on asylum for nationals of Member States of the European Union.[46]

Consequently, the achievement of the area of freedom, security and justice became one of the aims of the European Union. As it was highlighted above, this requirement faced a cross-pillar task, i.e. the policies on free movement and on immigration, asylum and visas belonged to the First Pillar, while police and judicial cooperation in criminal matters fell within the scope of the Third Pillar. Before the entry into force of the Amsterdam Treaty, the cross-pillar nature of the visa and the external and internal border control and security issues was recognised in the Vienna Action Plan. "As the Vienna Action Plan emphasized, the concepts of freedom, security and justice are inseparable: 'one cannot be achieved in full without the other two'[47]."[48] As a provision of the Vienna Action Plan, the common procedure of seeking asylum building on common standards was assigned. The ambition was built on the "Community-binding feature" of the Dublin Convention. Consequently, the conclusions of the 1999 Tampere Summit set out an ambitious agenda for developing a "Common European Asylum System" (hereinafter: CEAS),[49] inter alia, the promptly realisation of the system for the identification of asylum seekers (EURODAC).[50]

The 2001 Treaty of Nice[51] supplemented the related policies to JHA in connection with the First and in relation to the Third Pillar, too. The Treaty of Nice contains changes regarding the decision-making. The Treaty extended the enhanced cooperation to the Third Pillar, as well.

Regarding large-scale IT systems, the so-called Hague Programme[52] enumerated further tasks: the application of SIS II, a review of the powers of the border agencies, the establishment of the Common European Asylum System, the eventual creation of visa

[46] Peers, Steve, *EU Justice and Home Affairs Law*, *op. cit.*, pp. 301-302.
[47] Action Plan of the Council and the Commission on How to Implement the Provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice, OJ C 19, 23.1.1999, p. 2.
[48] Meloni, Annalisa, *op. cit.*, p. 163.
[49] Cf. CEAS and fundamental rights: Kaponyi, Erzsébet, "A Közös Európai Menekültügyi Rendszer és az alapvető jogok védelme", *Pro Publico Bono Online Támop Speciál,* 1(1), pp. 1-58
[50] Peers, Steve, *EU Justice and Home Affairs Law*, *op. cit.*, p. 302.
[51] Treaty of Nice Amending the Treaty on European Union, the Treaties establishing the European Communities and Certain Related Acts, OJ C 80, 10.3.2001, pp. 1-87.
[52] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005. pp. 1-14.

officers, a report on interconnection between information systems and continued integration of biometrics.[53]

To handle challenges of the area of freedom, security and justice, the European Council endorsed the Stockholm Programme[54]. This program handles the SIS II and the VIS as key objectives.[55] The European Council invited the Commission "to undertake a feasibility study on EURODAC as a supporting tool for the entire CEAS, while fully respecting data protection rules"[56].

1.3. A Non-Pillar Europe for the Unified Management

The Constitutional Treaty would have significantly changed the structure of JHA if it had come into force. The Treaty of Lisbon[57] inherited the substantive changes proposed in the Constitutional Treaty. Because of the disappearance of the Pillars, the decision-making procedure of measures in relation to the area of freedom, security and justice is basically the ordinary legislative procedure. The European Union

> "[...] shall ensure the absence of internal border controls for persons and shall frame a common policy on asylum, immigration and external border control, based on solidarity between Members States [...]"[58].

The Treaty confirmed the tendency towards the integration of external border controls, since it investigates the establishment of a Union policy on border checks.[59] The protocols on the special status of the United Kingdom, Ireland and Denmark are included in the Treaty with some minor amendments[60].

---

[53] Cf. Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, Prüm, 27.5.2005, source: 10900/05 Prüm Convention, Brussels, 7.7.2005; and cf. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, pp. 1-11.
[54] 17024/09 The Stockholm Programme – An open and secure Europe serving and protecting the citizens, Brussels, 2.12.2009.
[55] *Ibid*, p. 57.
[56] *Ibid.*
[57] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 115, 9.5.2008, pp. 1-388.
[58] Treaty on the Functioning of the European Union, OJ C 83, 3.30.2010, Art. 67(2), p. 73.
[59] *Ibid*, Art. 77, pp. 75-76.
[60] Protocol (No 20) on the application of certain aspects of article 26 of the Treaty on the Functioning of the European Union to the United Kingdom and to Ireland, OJ C 115, 9.5.2008, pp. 293-294. Protocol (No 21) on the position of the United Kingdom and to Ireland in respect of the area of freedom, security and

In connection with common asylum policy, the Treaty of Lisbon states that

> "[...] [t]he Union shall develop a common policy on asylum, subsidiary protection and temporary protection with a view to offering appropriate status to any third-country national requiring international protection and ensuring compliance with the principle of *non-refoulement*"[61].

The Lisbon Treaty closed the process started by the 1997 Amsterdam Treaty, since the Third Pillar abolished and the decision-making procedure concerning the area of freedom, security and justice was reviewed.

It means that the existing law enforcement large-scale IT systems operating in the area of freedom, security and justice, i.e. SIS, VIS and EURODAC, could be integrated into a single European agency, into the eu-LISA, in such a way that overcomes the problems derives from the cross-pillar nature of the systems' origin.[62] It is an important development, since the original proposals of the European Commission[63] should have encompassed the cross-pillar settings. Therefore, after the Lisbon Treaty became applicable, Commission proposals could be merged into a single one[64].

Taking the smart boarders initiative of the European Commission[65] into account, it endeavours for the establishment of new large-scale IT systems such as European level entry/exit system (EES) and a registered traveller programme (RTP) that can be considered as planned law enforcement large-scale IT systems. According to the today's treaty and secondary law provisions, it is practicable legally and technically that the eu-LISA may host, manage and develop their (at least EU level) operations.[66]

The fact that current treaty arguments made it possible to manage existing and as well as planned law enforcement large-scale IT systems jointly confirms the existence of

---

justice, OJ C 115, 9.5.2008, pp. 295-298. Protocol (No 22) on the position of Denmark, OJ C 115, 9.5.2008, pp. 299-303.

[61] Treaty on the Functioning of the European Union, *op. cit.*, Art. 78, p. 76.

[62] See also: Dóczi, Zoltán, "The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice", *Acta Juridica Hungarica*, 54(2), 2013, pp. 164-183.

[63] COM(2009) 293 final 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, Brussels, 24.6.2009; 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.

[64] COM(2010) 93 final Amended Proposal a Regulation (EU) No .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, Brussels, 19.3.2010.

[65] 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.

[66] See also: Smart Borders Package, *op. cit.*

a common resultant as unified management of the systems is a joint approach to the common challenge of securing and facilitating people movement.

***

The detailed analysis of core legislations are indispensable to understand the legal development and the today's practice and nature of EU law enforcement large-scale IT systems. The area of freedom, security and justice still faces challenges. That is why the European Commission drafted the so-called Post-Stockholm Programme[67]. It fosters policy tools to support more intensely the idea of "an open and secure Europe". Attributes of law enforcement large-scale IT systems and their unified management are envisioned to be streamlined in order to implement the Programme.[68]

Programmes, action plans and communications[69] are compasses of future legislation, since common challenges need unified approach to handle them.

[67] COM(2014) 154 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions An open and secure Europe: making it happen, Brussels, 11.3.2014.
[68] By today, the so-called Ypres Guidelines are set out. However, the large-scale IT systems are mentioned shortly. Cf. EUCO 79/14 European Council 26/27 June 2014: Conclusions, Brussels, 27.6.2014, pp. 1-6.
[69] See also: COM(2015) 240 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions A European Agenda on Migration, Brussels, 13.5.2015.

2. The Development of Existing Law Enforcement Large-Scale IT Systems Operating in the Area of Freedom, Security and Justice

The abolishment of internal border checks and common procedures at external borders keep on fostering European decision-makers to establish law enforcement large-scale IT systems in the area of freedom, security and justice. The decrease of security deficit by control of migration flows consists of three endeavours: common border control policy, common visa policy and common asylum policy.

Law enforcement large-scale IT systems are highly important for the border security strategy, since among others systematic data gathering and data exchange of information concerning (mainly but not exclusively) third country nationals happen through them.

The European Union realised the opportunity of exploiting information power by the establishment of law enforcement large-scale IT systems following the analogy of the concerned policy areas. Thus, the legal instruments of the SIS, VIS and EURODAC were adopted by the European decision-makers. On the whole, irregular migrants found in Member States can be registered in the SIS, but irregular migration defies this registration itself. Those who enter through asylum procedures are registered in EURODAC (among others) and those who enter using a legal channel, i.e. being issued a visa are registered by the VIS.

In the next subchapters, development and tasks of existing law enforcement large-scale IT systems are to be highlighted in order to give a background for the evaluation of SIS, VIS and EURODAC operational managements' integration. The analysis is crucial to understand the common grounds and possible connections with eu-LISA, while eu-LISA will be observed in the next chapter. Their development processes are detailed in light of interaction among them and their environment and their institutional arrangements are included as well. Furthermore, findings characterise day-by-day operation, i.e. functioning of the systems. The used mixed approach is of assistance to establish what social preferences of EU internal security and migration policies are reflected through them.

Findings of the author's preceding publications are used for the current chapter.[70]

[70] Dóczi, Zoltán, The Development, the Integration and the Assessment, *op. cit.*, mainly pp. 165-171; Dóczi, Zoltán, "Internal Security of *Schengenland*: What do we need SIS II for?", *BiztPol Affairs*, 2(2), 2014, pp. 18-28, used for subchapter 2.1.

2.1.Every End has a Start: Cyclic Dynamics of SIS Development

SIS supports common border control policy of the borderless Europe's home affairs and mainly as parts of that, internal security and migration policies. It took more than ten years to get SIS II on track. Thousands of working hours were devoted to development of the newest, i.e. second generation of the Schengen Information System (SIS II) until it has become operational on 9th April, 2013.

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[71]) to obtain information regarding certain categories of persons, vehicles and objects.

The very first version of 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[72] Manual, which governs subsequent exchanges of information following a 'hit' in the SIS."[73] Factual data are stored on the SIS but the SIRENE bureaus make it possible to exchange "soft" data such as criminal intelligence information. The power of the Executive Committee and its working groups was transferred by the Treaty of Amsterdam to the Council and to its working groups. SIS consists of two fundamental elements: the central database (called C-SIS) that is located in Strasbourg (in France) together with its back-up located in Sankt Johann im Pongau (in Austria) and the national SIS-bases (called N-SIS) are established in all of the participating states.

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.[74] There are six broadly defined reasons for which information can be included on the SIS. These are the so-called types of SIS 'alerts'.[75] Persons are concerned in case of being requested for extradition; undesirable in

[71] Schengen Implementing Convention, OJ L 239, 22.9.2000, Art. 92(1), p. 42.
[72] It stands for Supplément d'Information Requis à l'Entreé NationalE.
[73] Peers, Steve, "Key Legislative Developments on Migration in the European Union: SIS II", *European Journal of Migration and Law*, 10(1), 2008, p. 79.
[74] Schengen Implementing Convention, *op. cit.*, Art. 94(3), p. 43.
[75] See: *ibid*, Art. 95-100., pp. 43-45.

the territory of a participating State; minor of age, mentally ill patients, and missing persons or in danger with an aim of ensuring their own protection; requested by a judicial authority, such as witnesses, those quoted to appear for notification of judgement and absconders; suspected of taking part in serious offences and having to be the subject of checks or a surveillance control. Objects stored in SIS are the following: motor vehicles under a surveillance control and lost, stolen, or misappropriated vehicles, banknotes, identity documents, blank identity documents, firearms.

SIS has been communitarised as a Schengen *acquis* in 1999 with the entry into effect of the Treaty of Amsterdam. According to protocols on the special status of the United Kingdom and Ireland, they did not join the SIS, since they do not apply the Schengen *acquis*.

The original SIS has already been updated to "SIS 1+". Reasons for change were quite technical; the infrastructure was insufficient to linking the Nordic countries to SIS.[76] Thus, Schengen Implementing Convention SIS rules were amended in 2004 and 2005 giving access for judicial authorities, Europol, Eurojust and with another regulation the vehicle registration authorities to SIS data.

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 Member States decided to develop and to build up the second generation SIS till March 2007. However, 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 that the accession of those new Member States out of the ten that are ready to join to the Schengen area shall happen with the accession to SIS 1+, while SIS II should have been operational in the enlarged *Schengenland* by 2008. This proposal came from Portugal for the development of a "SIS One4 All" which is basically the extension of the then existing SIS 1+, a solution which had previously been understood to be technically impossible.[77]

The operational phase of SIS II has been launched on 9th April, 2013 (with a significant delay). New functions were added to the second generation SIS compared to the previous ones including storing biometric data, new categories of data and the

[76] Cf. the incorporation of the Nordic Passport Union into the Schengen area.
[77] Peers, Steve, Key Legislative Developments, *op. cit.*, pp. 81-82.

possibility of running searches based on incomplete data.[78] Therefore, the functioning of SIS has been extended to provide for the fight against terrorism[79] and modified to enable the storage of photographs and fingerprints after 11 September, 2001. The expansion of SIS II with biometric information 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.[80] Legal instruments of SIS II have a further novelty concerning the access of data, i.e. persons in the EU terrorist list based on decisions by the Sanctions Committee of the UN Security Council can be included in the SIS.[81] Its core is to pose entry and stay ban signals on persons listed by the Sanctions Committee and the Council. Previously entry and stay ban signal in this case was applicable solely by national decision. Furthermore, copy of a European Arrest Warrant is enclosed to signals for arrest and surrender persons or persons wanted for extradition.

SIS II contributes to public security and public policy and safeguarding of security within the area of freedom, security and justice of the European Union. It is composed by three parts. The first is the central system ("Central SIS II") containing a technical support function ("CS-SIS") containing a database, the "SIS II database" and a uniform national interface ("NI-SIS"). Secondly, there are national systems ("the N.SIS II") in each Member States, consisting of the national database which communicate with the Central SIS II. An N.SIS II may contain a data file ("national copy"), including a complete or a partial copy of the SIS II database. The third part of SIS II is the communication infrastructure between the CS-SIS and the NI-SIS ("the communication infrastructure") that provides an encrypted virtual network dedicated to SIS II data and the exchange of data among SIRENE Bureaux. There is no change in relation to the accessing authorities.

[78] 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), p. 22.

[79] 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, pp. 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, pp. 44-48.

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

[81] Boeles, Pieter and Heijer, Maarten den and Lodder, Gerrie and Wouters, Kees, *European Migration Law*, Antwerpen and Oxford and Portland, Intersentia, 2009, p. 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, p. 15.

The Charter of Fundamental Rights of the European Union, especially its Article 45[82] shall be taken into account when applying the SIS II rules. However, it is less clear how the SIS relates to third country nationals. In the preamble of SIS II Regulation , it is said that further harmonisation of the provisions on the grounds for issuing alerts concerning third country nationals for the purpose of refusing entry or stay and the clarification of their use in the framework of asylum, immigration and return policies are needed. On the one hand, it is unfortunate that the express clause giving priority to other EU immigration and asylum legislation was dropped. On the other hand, it is still arguable that such legislation takes priority over the SIS II legislation even in the absence of an express rule to that effect.

To sum up, the stored data on SIS II are surrender persons or persons wanted for extradition on the basis of European or international arrest warrant; persons with entry and stay ban; missing persons; persons to be looked for to participate in judicial proceedings; persons and objects under target or covered control; documents, vehicle and other objects set out in law wanted or seizure in order to use as evidence.

The second generation of the Schengen Information System is an enormous step in the internal security of the Schengen area. Its augmented capacity may combat future challenges. New categories and signals are incorporated into SIS II, which can be interlinked as well helping investigation and law enforcement. SIS II is clearly a milestone. However, it is a single internal security segment of *Schengenland*, since, for example, SIS, not being a border registration system, has never contained travellers' information.

Finally, it must be mentioned that the United Kingdom of Great Britain and Northern Ireland has recently joined the SIS II only in case of law enforcement cooperation.[83] As of writing, Ireland is preparing for the same type of SIS II accession as the United Kingdom of Great Britain and Northern Ireland carried out. Bulgaria and Romania use SIS II only in case of law enforcement cooperation because they were not

[82] "Freedom of movement and of residence
1. Every citizen of the Union has the right to move and reside freely within the territory of the Member States.
2. Freedom of movement and residence may be granted, in accordance with the Treaty establishing the European Community, to nationals of third countries legally resident in the territory of a Member State."

[83] Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of parts of the provisions of the Schengen *acquis* on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, OJ L 36, 12.2.2015, pp. 8-10.

accepted to join the Schengen area. Croatia and Cyprus enjoy temporary derogations from joining the Schengen area. Both states are preparing to be integrated into SIS II.

2.2. The Rolling VIS

VIS aims at supporting the implementation of common visa policy. It facilitates the Schengen visa application procedure by more enhanced consular cooperation and consultations between central visa authorities. Its preliminary aim is commonly interpreted as preventing visa shopping. However, VIS facilitates checks at external border crossing points and in the national territories and contributes to the prevention of threats to internal security of participating countries as well.

The so-called Santiago Plan[84] included proposals, inter alia, on visa policy and on information exchange and analysis on migration flows. Regarding visa policy, it recommended the annual review of visa lists, the inclusion of photo and (other) 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.[85] 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)[86] provides the legal basis for the development of the system. VIS Regulation[87] 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.

VIS is accessible for visa authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum. The technical set-up of the system is similar to the SIS. The new visa system has a central database (C-VIS), an

[84] Proposal for a Comprehensive Plan to Combat Illegal Immigration and Trafficking of Human Beings in the European Union, OJ C 142, 14.6.2002, pp. 23- 36.
[85] Meloni, Annalisa, *op. cit.*, p. 178.
[86] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004, pp. 5-7.
[87] 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, pp. 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, pp. 129-136.

interface at the national level (N-VIS) and local access points (terminals) for police, immigration authorities and consular posts.[88]

The VIS can serve as an instrument to detect and identify those irregular migrants who travelled into the EU legally at any border, and then overstayed.[89] It is not a law enforcement tool. However, it gives law enforcement access. VIS is for facilitating border and police checks, to combat fraud, to improve consular cooperation and to prevent visa-shopping. The VIS facilitated the application of the Dublin II Regulation[90] and facilitates the application of the Dublin III Regulation[91] as well according to Article 21 and 22 of the VIS Regulation[92]. Asylum authorities have access to search the VIS with fingerprint data, but solely for the purposes of determining the country responsible for the examination of an asylum application and of examining an asylum application. However, if the fingerprints of the asylum seeker cannot be used or the search fails, the authorities may carry out the search with the data set out above. Moreover, the VIS data substantially contribute to the prevision, detection or investigation of terrorist offences and of other serious criminal offences. As it is set out by Council Decision 2008/663/JHA[93], in specific cases, national authorities and Europol may request access to data entered into the VIS for the purpose of preventing, detecting and investigating terrorist and criminal offences. The process is called consultation. Access to the VIS for consultation by Europol is limited to its mandate.

There are 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.[94]

Only the following categories of data are recorded in the VIS: data on the applicant and on the visas requested, issued, refused, annulled, revoked or extended; as concerns

[88] Broeders, Dennis, *op. cit.*, p. 86.
[89] *Ibid*, p. 85.
[90] Council Regulation (EC) No 343/2003, *op. cit.*
[91] Cf. Ch. II. 2.3.
[92] Regulation (EC) No 767/2008, *op. cit.*, Art. 21-22, pp. 70-71.
[93] Council Decision 2008/633/JHA, *op. cit.*
[94] Boeles, Pieter and Heijer, Maarten den and Lodder, Gerrie and Wouters, Kees**,** *op. cit.*, p. 424.

biometrics photographs and fingerprint data; and links to previous visa applications and to the application files of persons travelling together. Each application file is stored in the VIS for a maximum of five years. Only the country responsible has the right to amend or delete data it has transmitted to the VIS. Ten-digit finger and a digital photograph are collected from persons applying for a visa. Ten-digit finger scans are not required from children under the age of twelve or from people who physically cannot provide finger scans. Frequent travellers to the Schengen area do not have to give new finger scans every time they apply for a new visa. Once finger scans are stored in VIS, they can be re-used for further visa applications over a five-year period. At the external borders of the Schengen area, finger scans of visa holders may be compared against those held in the database. A mismatch does not mean that entry will automatically be refused. It will merely lead to further checks on the traveller's identity.

The Schengen Borders Code has been harmonised with the VIS by a regulation[95]. 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.[96] As STEVE PEERS recalled "the initial three-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."[97]

The Visa Code[98] 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.[99] 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.[100]

---

[95] 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, pp. 56-58.
[96] Peers, Steve, "Legislative Update: EC Immigration and Asylum Law, 2008: Visa Information System", *European Journal of Migration and Law*, 11(1), 2009, p. 84.
[97] *Ibid.*
[98] 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, pp. 1-58.
[99] *Ibid*, Art. 54(6)b, p. 24.
[100] *Ibid*, Art. 57(3), p. 26.

Not only SIS II started its operation with delay but also the operation of VIS was otherwise engaged. VIS has been operational since 11 October, 2011.[101] However, the VIS will have been applied step by step, i.e. region by region, which are the so-called regional rollouts. The Commission adopted Decision 2010/49/EC[102] (first three regions), Implementing Decision 2012/274/EU[103] (another eight regions) and Implementing Decision 2013/493/EU[104] (remaining twelve regions) to define twenty-three regions for rollouts. As of writing, the last region covered by VIS is number eighteen.[105]

11 October, 2014 is a clear milestone in relation to the operational functioning of VIS, since it is the date from which verification of fingerprints at Schengen external borders became mandatory. It means that by arrivals at an external border of the Schengen area biometric data of visa holders are checked to confirm their identity. It leads to more accurate processing and greater security. However, it might lead to added time at the border crossing. As of writing, no reports are available on its evaluation.

According to the Post-Stockholm Programme, the completion of worldwide rollout of the VIS is mentioned as one of the tools for achieving "EU's interest to be more open to visitors, contributing to economic growth" "while maintaining a high level of security".[106]

2.3. A Prudent Progress: The Development of EURODAC

EURODAC is a database that stores and compares fingerprints of asylum applicants and irregular migrants apprehended in connection with the irregular crossing of an external border. It was established to allow Member States to determine the state

[101] Commission Implementing Decision 2011/636/EU of 21 September 2011 determining the date from which the Visa Information System (VIS) is to start operation in a first region, OJ L 249, 27.9.2011, Art. 1, p. 19.
[102] 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, pp. 62-64.
[103] Commission Implementing Decision 2012/274/EU 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, pp. 20-22.
[104] Commission Implementing Decision 2013/493/EU of 30 September 2013 determining the third and last set of regions for the start of operations of the Visa Information System (VIS), OJ L 268, 10.10.2013, pp. 13-16.
[105] Commission Implementing Decision 2015/731/EU of 6 May 2015 determining the date from which the Visa Information System (VIS) is to start operations in the 17th and 18th regions, OJ L 116, 7.5.2015, pp. 20-21.
[106] COM(2014) 154 final *op. cit.*, pp. 5-6.

responsible for examining an asylum application according to the Dublin Convention that turned into Dublin II Regulation[107] and which is now the Dublin III Regulation[108].

The EURODAC Regulation[109] was adopted in 2000, and the Council adopted the implementing rules[110] in 2002. The system became operational on 15 January, 2003.[111] Originally, EURODAC facilitates the application of the Dublin Convention developing to Dublin II Regulation, which makes it possible to determine the country responsible for examining an asylum application. The New EURODAC Regulation[112] was adopted in order to streamline provisions ruling the system with Dublin III Regulation. All the regulations highly contribute to the building and/or functioning of the Common European Asylum System.

As of writing, it shall be underlined that Dublin III Regulation may be subject to amendments in order to be streamlined with judgement *MA and Others vs. Secretary of State for the Home Department*[113] aiming at better regulation on the best interest of the child.[114] Moreover, the Commission predicted a further reform of the Dublin Regulation by March, 2016.[115]

---

[107] Cf. Ch. II. 1.2.

[108] Regulation (EU) No 604/2013 of the European Parliament and the Council of June 26 2013 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), OJ L 180, 29.6.2013, pp. 31-59.

[109] 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, pp. 1-10.

[110] 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, pp. 1-5.

[111] Peers, Steve (ed.), *EU Immigration and Asylum Law: Text and Commentary*, "Immigration and Asylum Law and Policy in Europe", vol. XII., Leiden, Martinus Nijhoff Publications, 2006, p. 259.

[112] Regulation (EU) No 603/2013 of the European Parliament and the Council of June 26 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 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 on requests for the comparison 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), OJ L 180, 29.6.2013, pp. 1-30.

[113] *MA and Others vs. Secretary of State for the Home Department,* Case C-648/11, request for a preliminary ruling, judgement of 6 June 2013.

[114] Cf. COM(2014) 382 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 604/2013 as regards determining the Member State responsible for examining the application for international protection of unaccompanied minors with no family member, sibling or relative legally present in a Member State, Brussels, 26.6.2014.

[115] COM(2015) 490/2 final Communication to the European Parliament, the European Council and the Council Managing the refugee crisis: immediate operational, budgetary and legal measures under the European Agenda on Migration, Brussels, 29.9.2015, p. 13.

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. The system is basically assessable for asylum authorities and competent control authorities in connection with irregular border crossings (except for turn backs). 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 of asylum applicants and aliens are defined. The following data are collected for any asylum applicants over fourteen 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.[116]

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 System (which will have the capacity to store fingerprints)."[117] In December 2008, the Commission proposed the first three measures that would constitute the second phase of

[116] Boeles, Pieter and Heijer, Maarten den and Lodder, Gerrie and Wouters, Kees, *op. cit.*, pp. 424-425.
[117] Peers, Steve (ed.), *EU Immigration and Asylum Law, op. cit.,* p. 272.

the Common European Asylum System, namely, amendments to the EURODAC Regulation, the Dublin II Regulation and the Reception Conditions Directive[118].[119]

The 2010 Belgian Presidency was committed to the speedy completion of the Common European Asylum System. The modification of Dublin and EURODAC Regulations and the Long Term Residence and Qualification Directives were prioritised with ensuring coherence in relation to the recast of the Reception Conditions and Procedures Directives.[120] Therefore, the legislative package of the Common European Asylum System includes six legislative proposals that EU Member States have committed to adopt by 2012.[121] Therefore, an amended proposal[122] was born aiming at the fostered transmission of fingerprint records and the involvement of Europol and national law enforcement authorities.

The Common European Asylum System (CEAS) was born along the six legislative proposals that actually embodied as revised directives. All of them were adopted by 2013. They together constellate "EU as an area of protection" as it is commonly referred to. The revised Dublin Regulation or as it has been proposed to call

---

[118] 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.

[119] Peers, Steve, Legislative Update, *op. cit.*, p. 71.

[120] 13703/2010 Common European Asylum System – State of Play, Brussels, 27.9.2010.

[121] 15848/10 "Press Release, 3043rd Council meeting, Justice and Home Affairs", *Europa Press Releases RAPID*, Brussels, 8-9.11.2010.

[122] 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.

above the Dublin III Regulation and the revised EURODAC Regulation or as it has been proposed above the New EURODAC Regulation are of primary importance for the current analysis.

The Dublin III Regulation enhances the protection of asylum seekers during the process of establishing the State responsible for examining the application, and clarifies the rules governing the relations between states. It creates a system to detect early problems in national asylum or reception systems, and address their root causes before they develop into fully-fledged crises. It improves the effectiveness of Dublin procedures with shorter deadlines that may resulted in less risk of absconding and of human smuggling. It enhanced the protection of unaccompanied minors as well. More emphasis on the unity for the family may be observed by incorporating provisions on dependents. The regulation creates more harmony with today's asylum *acquis.*

The New EURODAC Regulation streamlines provisions ruling the EURODAC system with Dublin III Regulation and as well as finetunes its operation with new asylum *acquis.* It is applicable from 20 July, 2015.

The technical arrangements of the new EURODAC have slightly changed laying more emphasis on security. Namely, the Central System encompass not only the Central Unity but also a Business Continuity Plan and System. The new EURODAC consists of the Central System and Communication Infrastructure between the Central System and Member States.[123] Enhanced data security provisions can be observed[124] that may aim at counterbalancing the below, most crucial development.

Terrorists may abuse existing arrangements by hiding identity as irregular migrants or asylum seekers. The New EURODAC Regulation allows law enforcement access to the EU database of the fingerprints of asylum seekers, i.e. to new EURODAC under strictly limited circumstances in order to prevent, detect or investigate the most serious crimes, such as murder, and terrorism. Based on the New EURODAC Regulation, law enforcement access means that designated authorities of Member States for law enforcement purposes and Europol may request the comparison of fingerprint data with those stored in the Central System for law enforcement purposes.[125] In case of Europol,

[123] Regulation (EU) No 603/2013, *op. cit,*, Art. 3(1), p. 8.
[124] Cf. *ibid,* Art. 31-35, pp. 19-21.
[125] *Ibid,* Art. 1(2), p. 7.

its competent and designated unit serves as National Access Point. Access to new EURODAC by Europol is limited to its mandate.[126]

The granted law enforcement access is the most relevant novelty of the new EURODAC system, since it indicates a change in security perceptions in EU internal security and migration policies.

***

The so far outlined development process of existing law enforcement large-scale IT systems operating in the area of freedom, security and justice shows a reactive attitude, i.e. reactive to perceived security challenges. Their development process is decidedly inherent although relevant cooperation started out of EC/EU treaty regime. It is also supported by the fact that the systems were created separately but they keep on entering into more enhanced interaction with each other and with their environment.

[126] *Ibid,* Art. 7(2), p. 9.

3. Eu-LISA: Operation and Repercussions

The development of existing law enforcement large-scale IT systems operating in the area of freedom, security and justice has been analysed in the previous chapter. It shall be kept in mind that the integration of their operation management established another, independently observable law enforcement large-scale IT system called eu-LISA.

In order to be able to use the proposed methodological tool extendedly to all segments of EU law enforcement large-scale systems, it shall be examined whether the joint operational management of existing specific law enforcement large-scale IT systems changed their functioning. In addition, if it has been changed, the way, the nature and the consequences of the change shall also be explained.

As it is expected, the combination of institutionalist description of eu-LISA with the analysis of interactions among the Agency, the systems and their environment (cf. functionalist mindset) finetune the preliminary results and face theory (i.e. legal provisions and legislative purpose) with reality.

Henceforward it is fundamental to consider how the newest segment of EU law enforcement large-scale IT systems' joint operational management contributes to EU migration and internal security policies.

The European Commission prepared the proposal and related legal instruments for the establishment of an agency for the operational management of large-scale IT systems in the area of freedom, security and justice[127] in June 2009. The new regulatory agency that is the eu-LISA was established by January 2012. It merged the operational management tasks of the further developed version of SIS, VIS and EURODAC and it is flexible to add other existing and potential new systems. Eu-LISA took up its responsibilities on 1 December, 2012.[128]

Breaking the above analysis down, firstly, it is worth considering why the establishment of the Agency was legally predetermined, since the previous hints for its establishment points out perceived security deficit. Moreover, options for its installations may serve as points of reference.

Then it is essential to understand the aims and the basic tasks of eu-LISA in order to evaluate its scope taking into account the principle of subsidiarity and proportionality.

[127] COM(2009) 293 final, *op. cit.* and COM(2009) 294 final, *op. cit.*
[128] Regulation (EU) No 1077/2011, op. cit., Art. 38, p. 17.

Focusing on general and governance structure of eu-LISA, its legal basis is analysed. It raises the problem of the territorial scope affecting on its governance structure.

Finally, the relationship of eu-LISA with other EU agencies is observed. Therefore, a subsection concentrates on the legal instruments of the SIS II, VIS and EURODAC in order to identify the EU level agencies that have access to and/or influence on the large-scale IT systems. The status of these organisations is defined in the everyday work of eu-LISA. For that, a layer model is presented to highlight the interrelations.

Findings of the author's preceding publication is used for the current chapter as well.[129]

3.1. Legal Predestination

Patterns for the legislative integration process of law enforcement large-scale IT systems working for EU public safety can be observed. Hence, the found patterns are followed as essential milestones that serve as connection points for the legal predestination to the installation of a European Agency for their operational management.

The EU Member States want to foster the integration of the information systems for ten 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. [...]"[130].

The fundamental legislation of SIS II[131] was adopted on 20 December, 2006. This is the SIS II Regulation. Worthy of note, the SIS II has more legal instruments[132]. Article 15(1) of the SIS II Regulation states the followings:

---

[129] Dóczi, Zoltán, The Development, the Integration and the Assessment, *op. cit.*, mainly pp. 172-181.
[130] The Hague Programme: strengthening freedom, security and justice in the European Union, *op. cit.*, p. 7.
[131] Regulation (EC) No 1987/2006, *op. cit.*
[132] 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, pp. 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, pp. 63-84.

> "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. [...]".

Until 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.[133] 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)." [134]

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

> "[...] 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. [...]"[135].

It means that these proposals had to be published in 2009. According to the Joint Statement, the Agency had to take up fully its activities in 2012.[136]

The same legislative techniques have been used in case of the adaptation of legal instrument of the Visa Information System (VIS)[137]. The VIS Regulation was adopted on 9 July, 2008[138]. After a transitional period, the Management Authority had to be founded[139]. During that period, the Commission was responsible for the operational management of VIS, which may delegate its power to two Member States[140].

---

[133] Regulation (EC) No 1987/2006, *op. cit.,* Art. 15(4), p. 11.
[134] *Ibid,* Art. 4(3), p. 8.
[135] 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, p. 102.
[136] Peers, Steve, Key Legislative Developments, pp. 86-87.
[137] Regulation (EC) No 767/2008, *op. cit.* and Council Decision 2008/633/JHA, *op. cit.*
[138] Regulation (EC) No 767/2008 *op. cit.*
[139] *Ibid,* Art. 26(1), p. 72.
[140] *Ibid,* Art. 26(4), p. 72.

Consequently, the central VIS is located in Strasbourg (France) and the back-up central VIS in Sankt Johann im Pongau (Austria)[141]. [142]

A Joint Statement of the European Parliament, the Council and the Commission on Article 26 relating to operational management of VIS[143] 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. [...]"[144].

The third IT system is the EURODAC. Its interoperability shall be ensured in line with the Hague Programme. The Commission issued proposals to amend the EURODAC Regulation, the Dublin II Regulation and the Reception Conditions Directive[145], which, inter alia, promote the harmonisation of the EURODAC with other IT systems.

One of the proposals[146] intended to implement a new recital as Recital (11) into the Dublin II Regulation in order to tone in with the VIS Regulation although the recitals are not legally binding. However, 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[147] suggested replacing Article 4 of Council Regulation (EC) No 2725/2000[148] with the followings among others:

> "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.
> [...]

---

[141] *Ibid*, Art. 27, p. 73.
[142] Peers, Steve, Legislative Update, pp. 86-87.
[143] 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, p. 102.
[144] *Ibid.*
[145] 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.*
[146] COM(2008) 820 final, *op. cit.*, Recital 28; cf. COM(2008) 820 final (Recast), *op. cit*., Recital 28.
[147] COM(2008) 825 final, *op. cit.*
[148] Council Regulation (EC) No 2725/2000, *op. cit.*

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 Agency was legally foreordained, which could have signed the perception of some security deficit in *Schengenland*.

The mentioned EURODAC related measures, namely the Dublin III Regulation and the New EURODAC Regulation were adopted a year later, in 2013. The New EURODAC Regulation not only incorporates eu-LISA provisions but also grants access for Europol to EURODAC amending eu-LISA Regulation[149] as well after becoming applicable on 20 July, 2015. It also supports the conjectured tendency of integration and its legal predetermination that implies an enhanced desire for security if social preferences are concerned.

3.2. Roadmap to a New Regulatory Agency

The undertaking of this subsection is to demonstrate the aims and the basic tasks of eu-LISA. The European Commission elaborated five options for its establishment. Hence, the options, the elected one and the legal and technical conditions of the Commission's impact assessment[150] are analysed in order to evaluate the scope of eu-LISA taking into account the principle of subsidiarity and proportionality.

Both the principle of subsidiarity and of proportionality are laid down in Article 5 of the Treaty on European Union.[151] Subsidiarity ensures that decisions are taken as closely as possible to the citizens and that constant checks are made to verify that action at Union level is justified in light of the possibilities available at national, regional or local level. Specifically, it is the principle whereby the Union does not take action (except in the areas that fall within its exclusive competence), unless it is more effective than action

[149] Regulation (EU) No 603/2013, *op. cit.*, Ch. VIII, pp. 22-23.
[150] 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.
[151] Consolidated Version of the Treaty on European Union, OJ C 326, 26.10.2012, Art. 5, p. 18. Cf. Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality, *ibid*, pp. 206-209.

taken at national, regional or local level. It is closely bound up with the principle of proportionality, which requires that any action by the Union should not go beyond what is necessary to achieve the objectives of the Treaties. Similarly to the principle of subsidiarity, the principle of proportionality regulates the exercise of powers by the European Union. It seeks to set actions taken by the institutions of the Union within specified bounds. Under this rule, the involvement of the institutions must be limited to what is necessary to achieve the objectives of the Treaties. In other words, the content and form of the action must be in keeping with the aim pursued (aim-alignment).

As it has been detailed above, the European Commission, the Council and the European Parliament, in joint statements attached to the SIS II and VIS legal instruments, committed the Commission to present, within two years of the entry into force of the SIS II and VIS legal instruments, the necessary legislative proposals, following an impact assessment containing a substantive analysis of alternatives from the financial, operational and organisational perspective, to entrust an agency with the long-term operational management of the VIS, of the Central SIS II and of parts of the Communication Infrastructure. The EURODAC would need to be upgraded in terms of capacity after the new Member States joined the EU in 2004 and 2007. The biometric matching, synthesising the above mentioned findings, in the form of service-oriented architecture of Biometric Matching System (BMS), is, in the first instance, made available for the VIS. It is likely to be provided on a larger stage for SIS II and EURODAC. Accordingly, the operational management solution for EURODAC has also been reviewed in the impact assessment of the Commission (hereinafter impact assessment).[152] Combining the systems, on the one hand, in a joint Agency could provide opportunities for considerable synergies such as sharing facilities, staff and common technology platform. On the other hand, these systems cannot function properly without a long-term central operational management authority, which ensures uninterrupted flow of data, operational management of the systems and continuity, notwithstanding it has been legally predetermined as well.

The impact assessment defines proper criteria in order to compare the opportunities of alternatives. The Commission relied on the following factors: the efficient management of the systems taking their critical character and their 24/7 availability into account; the need to involve the views of all stakeholders and the roles

[152] *Ibid.*

of the EU institutions; the heterogeneous group of participating countries; the need for (cost-) efficient management and for the timely and adequate funding; the importance of effective data protection and supervision; the effective mechanisms and redress for abuse or faults causing damage; the principle of subsidiarity and proportionality and the added value of EU action.[153] The Commission chose five options to evaluate in the impact assessment based on these criteria using the qualitative and the quantitative approaches regardless of the alterations introduced by the Treaty of Lisbon.

The "Baseline" (option 1) proposed to continue the existing practice of the operational management of SIS II and VIS created for the transitional period, i.e. the Commission is responsible for their operational management functions. However, the Commission would entrust two Member States with the operational management tasks. Respectively, the operational management set-up of EURODAC would remain under the responsibility of the Commission. Ergo, "the Commission would remain responsible and accountable for the management of the large-scale IT systems, while the Member States would remain responsible for day-to-day operational management tasks."[154]

The "Baseline+" (option 2) is the same as the "Baseline" option, with one main difference: the Commission would also entrust two Member States with the operational management tasks of EURODAC as well.

"Europol for SIS II and Commission for VIS and EURODAC" is presented as option 5 in the impact assessment. Before the disappearance of the pillar system, this option was more problematic, since the Europol was a third-pillar agency and it would have been responsible for the first-pillar element of the SIS II. Thus, the involvement of Community stakeholders would have been very limited. Not calculating with this problem, based on the qualitative assessment of the impact assessment, this option remains the worst, since this solution is not so transparent and it does not fit the provisions of liability and redress effectively. However, it is flexible to add other existing and potential new systems, and it is financeable as well.

Option 4 is the "FRONTEX for SIS II, VIS and EURODAC". It would entail changes in the FRONTEX Regulation and in its governance structure. Efficient operational management under this option, as the impact assessment emphasised, would require relocating the systems to the FRONTEX site or to a facility nearby.[155] Following

[153] *Ibid,* pp. 10-17.
[154] *Ibid,* p. 17.
[155] *Ibid,* p. 18.

the qualitative assessment, this option emerges as one of the preferred options. However, following the qualitative assessment, it has become clear that this option is less cost-effective than the chosen one.

Option 3, "a new Regulatory Agency" was found to be the best alternative among the analysed opportunities. On the one hand, according to this option, the new-born Agency is responsible for the long-term operation management of SIS II, VIS and EURODAC, and eu-LISA shall organise trainings related to the use of SIS II, VIS and EURODAC.[156] It is still true in relation to EURODAC after the New EURODAC Regulation became applicable.[157]

On the other hand, the Agency shall develop and manage other IT systems.[158] The initiatives for the development of new (law enforcement) large-scale IT systems shall be in line with the desires of European legislators, and of course, their establishments shall be based on the legislative procedures foreseen in the Treaties.

One of the basic aims of all the options presented in the impact assessment 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 operation. However, technical interoperability, i.e. interconnectedness, has never been targeted, since in this way, aim-assigned operation of the systems would be distorted causing serious disproportionality.

Option 3, the related Commission proposals[159] and the adopted Regulation[160] respect 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 eu-LISA 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. The technical arrangements of new EURODAC is slightly changed laying more emphasis on security. Namely, the Central System encompasses not only the Central Unity but also a Business Continuity Plan and System.[161]

---

[156] Regulation (EU) No 1077/2011, *op. cit.*, Art. 3-5, p. 6.
[157] Regulation (EU) No 603/2013, *op. cit.*, Art. 38(1), p. 22.
[158] Regulation (EU) No 1077/2011, *op. cit.*, Art. 6, p. 7.
[159] COM(2009) 293 final, *op. cit.* After the Lisbon Treaty, equivalence with COM(2010) 93 final, *op. cit.*
[160] Regulation (EU) No 1077/2011, *op. cit.*
[161] Regulation (EU) No 603/2013, *op. cit,*, Art. 3(1)a, p. 8.

As the European Data Protection Supervisor (hereinafter EDPS) highlighted in his opinion[162], during the legislative and public debate "concerns have been voiced about the possible creation of a 'big brother agency'."[163] 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."[164]

The eu-LISA Regulation 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.[165] On the one hand, after the entry into force of the Treaty of Lisbon, the fundamental rights and freedoms shall be more carefully respected by the European institutions. On the other hand, accountability of the European Agencies is ensured by the European Parliament and the European Data Protection Supervisor. Furthermore, the European Court of Justice[166] and the General Court have full jurisdiction over eu-LISA activities.

3.3. Governing Operational Management: Eu-LISA Structures

Following the presentation of the aims and the main tasks of the eu-LISA, its general and governance structure are in focus. This subsection is about to detail aims, tasks and operation of the Agency. Firstly, the general structure is presented that inevitably raises the problem of territorial scope which is called *la géométrie variable* (variable geometry). Then the governance structure of the Agency is summed up.

Eu-LISA took up its responsibilities on December 1, 2012.[167] It was envisioned to provide a viable and long-term solution for the operational management of EU law enforcement large-scale IT systems. EURODAC, VIS and SIS II are all essential instruments in the implementation of EU asylum, migration and border management policies. At a later stage, the Agency may develop into a centre of excellence for the

[162] 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.
[163] *Ibid,* Point 24.
[164] *Ibid,* Point 25.
[165] Regulation (EU) No 1077/2011, *op. cit.,* Art. 21, 28, 29 and 26, pp. 13-14.
[166] *Ibid,* Art. 24, p. 13.
[167] Regulation (EU) No 1077/2011, op. cit., Art. 38, p. 17.

development and operational management of other future systems in EU migration and internal security policy area.

The core task of the Agency is to keep the IT systems under its responsibility functioning 24 hours a day, seven days a week, ensuring the continuous, uninterrupted exchange of data between national authorities. The Agency is also responsible for adopting and implementing security measures, organising training for IT experts on the systems under its management, reporting, publishing statistics and monitoring research activities. According to eu-LISA Regulation, the Agency needs to maintain the complete separation of data in the three systems and ensure that security and data protection requirements are fully met.

General Structure

By the creation of eu-LISA, the establishment of a new regulatory agency was found the best alternative. On the one hand, according to this option, the Agency is responsible for the long-term operation management of SIS II, VIS and EURODAC, and the Agency shall organise trainings related to the use of the mentioned systems.[168] On the other hand, the Agency shall develop and manage other IT systems.[169] It means that the operational management of existing EU law enforcement large-scale IT systems is integrated (but not interconnected). Moreover, if so decided, the Agency is opened for new-coming systems as well.

According to the impact assessment, the eu-LISA should have been a first pillar agency with accompanying acts covering third pillar legal issues. Since the proposals were submitted, the Treaty of Lisbon 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 able to merge the two previous proposals[170]. The only disputable point of the EDPS's approach is that the cited article concerns police cooperation. The SIS II is more related to the police cooperation. However, the VIS and the EURODAC system are clearly connected to the common visa and the asylum policy.

[168] Regulation (EU) No 1077/2011, *op. cit.*, Art. 3-5, p. 6.
[169] *Ibid*, Art. 6, p. 7.
[170] COM(2009) 293 final, *op. cit.* and COM(2009) 294 final, *op. cit.* were merged to COM(2010) 93 final, *op. cit.*

Eu-LISA is responsible for the protection of personal data.[171] In that way, the application of the Treaty of Lisbon 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."[172]

On 19 March, 2010, the European Commission merged the two previous proposals into one united proposal pursuant to Article 293(2) of the TFEU.[173] The amended proposal is the equivalent of the two previous proposals. Besides the clarification of the legal basis of the Agency, there is not any significant amendment. The united proposal suggested the Title V of TFEU as the legal basis of the Agency. Article 87(2)(a) remained as one of its legal bases. Finally, the accepted Regulation[174] refers to the articles of Title V of TFEU as the legal basis of the Agency.

As the legal basis of eu-LISA was merged under Title V of the Treaty of Lisbon, the 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 Treaty of Lisbon with some minor amendments.[175] Eu-LISA Regulation constitutes the development of the Schengen *acquis* and builds on the provisions of EURODAC related measures. Hence, *la géométrie variable* of the Agency is highlighted taking into account the changed legislative framework and the *non-Schengen* EU Member States not obtaining opt-out on the Schengen *acquis*.

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 EURODAC Regulation, following an international agreement[176]. Denmark did not take part in adopting the new EURODAC Regulation, but, along with Norway, Iceland, Switzerland and Liechtenstein, it participates in the asylum (but not law enforcement) elements of EURODAC via agreements with the EU.

The United Kingdom and Ireland are not part of the Schengen area in accordance with the protocol on their special status. These countries do not take part in the adoption

[171] 5039/10 Opinion of the European Data Protection Supervisor *op. cit.*, Points 15-17.
[172] *Ibid*, Point 15.
[173] COM(2010) 93 final, *op. cit.*
[174] Regulation (EU) No 1077/2011, *op. cit.*
[175] See: Ch. II.1.3.
[176] 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, pp. 38-43.

of the provisions of Schengen *acquis* and are not bound by them or subject to their application insofar as they related to VIS.[177] However, that the United Kingdom of Great Britain and Northern Ireland has recently joined the SIS II only in case of law enforcement cooperation. As of writing, Ireland is preparing for the same type of SIS II accession as the United Kingdom of Great Britain and Northern Ireland carried out.[178] The United Kingdom and Ireland are bounded by the new 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.[179]

Based on Recital (33) of eu-LISA Regulation, the United Kingdom notified the Council about her intention to take part in the adaptation of the regulation based on her Protocol annexed to the treaties. It means that the United Kingdom is bound by the regulation and she is subject to its application. However, this fact does not affect the application of the VIS Regulation concerning the United Kingdom. Having regard to Recital (34), Ireland did not take part in eu-LISA Regulation in the beginning until her later request to opt in.[180]

Concerning the association of Norway and Iceland with the implementation, application and development of the Schengen *acquis*[181], these countries are associates in SIS II and VIS. Furthermore, they are also associates with the EURODAC related

[177] 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, pp. 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, pp. 20-23.
[178] Cf. Ch. II. 2.1.
[179] Regulation (EU) No 603/2013, *op. cit*,, Recital (52), p. 6; and Commission Decision C(2014)9310/F1 on the request by Ireland to accept Regulation EU No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 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 on requests for the comparison 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), 11.12.2014.
[180] Commission Decision C(2014)9310/F1, *op. cit.*
[181] 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, pp. 36-49.

measures.[182] The same legalisation technique was used concerning the association of Switzerland.[183]

Liechtenstein joined the agreements between the EU and Switzerland on the basis of protocols attached to the original agreements.[184] However, the Principality has been fully involved in large-scale IT systems as associate in the SIS II, VIS and EURODAC based on the protocols that are enclosed to the agreements concerning the association of Switzerland referred to in the previous paragraph.[185]

Based on the accession treaties, Bulgaria, Croatia, Cyprus and Romania are the signatories of the Schengen Agreement, and the Schengen *acquis* are binding them. However, there are norms that are still not applicable, i.e. the mentioned states shall not implement all these rules. On the one hand, there is the Cyprus dispute. On the other hand, Schengen accession of Bulgaria and Romania is politically not supported in the Council. In case of Croatia, as of writing, systems are to be developed. Overall, as a point of reference, these countries still do not participate in VIS. Although, they participate in SIS II in case of law enforcement cooperation. In addition, they participate in EURODAC as well due to asylum *acquis* (cf. mainly CEAS).

The non-mentioned other twenty-one EU and Schengen Member States apply the Schengen rules, asylum *acquis*, SIS II, VIS, EURODAC and eu-LISA Regulation.

---

[182] 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, pp. 40-47.

[183] 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, pp. 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, pp. 5-17.

[184] 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, pp. 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, pp. 39-49.

[185] 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, pp. 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, pp. 8-12.

Governance Structure

In terms of the governance structure, eu-LISA shall facilitate the appropriate representation of its users as far as decision-making structures are concerned. Based on eu-LISA Regulation, its structure and organisation, i.e. institutional arrangements are presented below. The Agency is a Union body and has legal personality.[186] Its administrative and management structure comprise a Management Board, an Executive Director and Advisory Groups.

The Management Board is composed 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.[187] The Chairperson and its alternate are elected by the Management Board among its members for a two-year term, which may be once renewed. Nevertheless, 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.[188] 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.[189] 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 Agency.[190] Generally, the decisions shall be taken by a majority of the members with a right to vote.[191]

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 Executive Director shall be appointed based on his or her personal merits, experience in the field of large-scale IT-systems and administrative, financial and management skills. The Management Board shall take the decision by a two-thirds majority of all members with a right to vote. The European

[186] Regulation (EU) No 1077/2011, *op. cit.,* Art. 10(1), p. 7.
[187] *Ibid,* Art. 13, p. 9.
[188] *Ibid,* Art. 14, p. 10.
[189] Cf. *Ibid,* Art. 16, p. 10 and Art. 37, p. 17.
[190] *Ibid,* Art. 16(3), p. 10.
[191] *Ibid,* Art. 16(1), p. 10.

Parliament shall adopt an opinion setting out its view of the selected candidate. The term of office of the Executive Director may be extended once for up to three years. The Executive Director shall be accountable to the Management Board for his/her activities.[192] 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.[193]

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 program 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. 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.[194]

According to an adopted amended, Europol may appoint a representative to the EURODAC Advisory Group as well.[195] It was embodied in the New EURODAC Regulation that amended eu-LISA Regulation. Its Article 19(3) is replaced in a way that grants Europol representative at the EURODAC Advisory Group.[196] The replacement is applicable from 20 July, 2015. By the same date, based on New EURODAC Regulation, law enforcement access to EURODAC is given to designated authorities of Member States for law enforcement purposes and to Europol that may request the comparison of

[192] *Ibid,* Art. 18, pp. 11-12.
[193] *Ibid,* Art. 17, pp. 10-11.
[194] *Ibid,* Art. 19, p. 12.
[195] COM(2012) 254 final, *op. cit.*, p. 60.
[196] Regulation (EU) No 603/2013, *op. cit,,* Art. 38(5), p. 23.

fingerprint data with those stored in the Central System for law enforcement purposes.[197] Access to new EURODAC by Europol is limited to its mandate.[198]

It is true that EURODAC makes it easier for Member States and the Schengen associated countries to determine responsibility for examining an asylum application by comparing fingerprint datasets. Moreover, it is still a large database of fingerprints of not only applicants for asylum and but also irregular immigrants found. However, the mentioned new law enforcement access shifts the emphasis concerning the aims of EURODAC.

Overall, the Member States and the Schengen associated countries play an important role in controlling the systems as they are represented in the Management Board. The board and the Executive Director carry out together the day-to-day management of eu-LISA. It is necessary to establish the Advisory Groups to support the Management Board on system-specific issues in order to address observations 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 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."[199]

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.[200]

3.4. Repercussions of Eu-LISA Structures: A Layer Model

This subsection is to concentrate on the legal instruments of the SIS II and VIS and EURODAC in order to identify the EU level agencies that have access to and/or influence on existing EU law enforcement large-scale IT systems. Hence, the status of

[197] *Ibid,* Art. 1(2), p. 7.
[198] *Ibid,* Art. 7(2), p. 9.
[199] SEC(2009) 837, *op. cit.,* p. 23.
[200] *Ibid,* p. 100.

these organisations is to be defined in the everyday work of eu-LISA. 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 eu-LISA. Europol and Eurojust have access to SIS II data based on the Article 41 and Article 42 of Council Decision 2007/533/JHA.[201] Europol also has access to VIS data in accordance with Council Decision 2008/633/JHA.[202]

The eu-LISA Regulation gives a legal solution for the involvement of the intentions of the Europol and Eurojust in the eu-LISA work 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.[203]

Article 19(1)d of the eu-LISA Regulation 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 provided.

An amended proposal of the Commission aimed 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.[204] As it has been emphasised above, the presented amended proposal was embodied in the New EURODAC Regulation that amended eu-LISA Regulation as well. Its Article 19(3) is replaced in a way that grants Europol representative at the EURODAC Advisory Group.[205] As far as the Management Board is concerned, the New EURODAC Regulation replaced Article 15(4) of eu-LISA

[201] Council Decision 2007/533/JHA, *op. cit.*, p. 77.
[202] Council Decision 2008/633/JHA, *op. cit.*
[203] Regulation (EU) No 1077/2011, *op. cit.*, Art. 19(3), p. 12.
[204] COM(2012) 254 final, *op. cit.*, pp. 59-60.
[205] Regulation (EU) No 603/2013, *op. cit.*, Art. 38(5), p. 23.

Regulation *mutatis mutandis,*[206] i.e. Europol became observer concerning all existing EU law enforcement large-scale IT systems related issues at the meetings of the Management Board. As referred to, replacements are applicable from 20 July, 2015.

The second layer is the *management level*. It encompasses the Agency level and the relations across law enforcement large-scale IT systems. All these relations are regulated in separate legislative acts. It has been explicitly stated in Article 1(4) of the eu-LISA Regulation as well.

As of now, two "inter law enforcement large-scale IT system acts" are applicable. The VIS facilitated the application of the Dublin II Regulation and facilitates the application of the Dublin III Regulation as well by granting access to asylum authorities to search the VIS fingerprint data solely for the purpose of determining the country responsible for the examination of an asylum application and of examining an asylum application. If the fingerprints of the asylum seeker cannot be used or the search fails, the authorities may carry out the search using other VIS data.[207]

Moreover, the VIS has been harmonised with the Schengen Borders Code by a regulation[208]. The Visa Code[209] is 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 with the purpose of refusing entry, it indicates a ground for the refusal of the visa.[210]

As it has been mentioned, according to the New EURODAC Regulation EURODAC became accessible for designated authorities (including Europol) for law enforcement purposes. As far as conditions for access concerned, EURODAC data is accessible, inter alia, after VIS data have been consulted without leading to the establishment of identity of data subject.[211] VIS data in this case shall be consulted first only in case of law enforcement purposes set out in VIS Decision 2008/633/JHA.[212]

Article 6 of eu-LISA 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 considering "across system" relations and the agency level together as another layer, called the management level.

---

[206] *Ibid,* Art. 38(3), p. 23.
[207] Regulation (EC) No 767/2008, *op. cit.,* Art. 21-22, pp. 70-71.
[208] Regulation (EC) No 81/2009, *op. cit.*
[209] Regulation (EC) No 810/2009, *op. cit.*
[210] *Ibid,* Art. 54(6)b, p. 24.
[211] Regulation (EU) No 603/2013, *op. cit.,* Art. 20(1), p. 14.
[212] Council Decision 2008/633/JHA, *op. cit.,* Art. 5(1), p. 132.

Having VIS and EURODAC relation concerning the determination of the country responsible for the examination of an asylum application, having also SIS II and VIS relation in connection with enforcing entry ban, and having the recently established VIS and EURODAC relation concerning conditions for granting access in case of law enforcement purposes, indirect interconnectedness of EU law enforcement large-scale IT systems is observed on the management level. It can be supported by the fact that the same authorities (however, maybe not the same units) may be designated to access the systems, since it is the responsibility of the Member State to set her own public administration up. Joint institutional arrangements of designated authorities (cf. Europol access as well) result in indirect interconnectedness that may be mitigated by intra-institutional rules of procedures.

The third layer is the *cooperation level*. As mentioned above, Europol and Eurojust are involved in the work of eu-LISA 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 called the cooperation level.

The Europol and the Eurojust are connected to other JHA agencies via formal cooperation agreements. The main focus of these acts is to strengthen the operative cooperation among law enforcement agencies. The JHA agencies have established an extended cooperation framework based on bilateral cooperation and information exchange. Moreover, a multilateral cooperation is planned among them.[213] JHA agencies usually exchange their draft work programmes prior to their final adoption. Therefore, they have deeper understanding of other's activities promoting synergies and avoiding duplications while respecting each other's mandate.

Taking these four JHA agencies into account, there was not a formal working agreement only between Eurojust and FRONTEX before the establishment of eu-LISA.[214] However, it was planned and fostered by the Commission, too. Operational cooperation exists between Europol and FRONTEX and between Europol and Eurojust, i.e. regular exchange of information in the framework of their operation. Europol and FRONTEX exchange strategic information mainly related to irregular immigration and cross-border crimes.[215] The Memorandum of Understanding on a Table of Equivalence

[213] 5816/10 Interim report on cooperation between JHA Agencies, Brussels, 29.1.2010; and 5676/11 Draft Scorecar2d – Implementation of the JHA Agencies report, Brussels, 25.1.2011.
[214] *Ibid.*
[215] 5816/10 Interim report on cooperation, *op. cit.*, p. 5. Cf. 5676/11 Draft Scorecard, *op. cit.*

allows the Eurojust and the Europol to exchange information up to and including the level of "restricted".[216]

The missing cooperation segment i.e. cooperation between FRONTEX and Eurojust was established by a 2013 Memorandum of Understanding.[217] It also includes exchange of strategic information, inter alia, "such as trends and challenges faced related to serious cross-border crime".[218]

These interrelations could have complementary influence on the operational practice of eu-LISA, since Eurojust, Europol and FRONTEX shall work together for the Standing Committee on operational cooperation on internal security (commonly referred to as COSI).[219] Furthermore, the Standing Committee shall help to ensure consistency of their actions.[220]

Analysing the legal instruments of the SIS II, VIS and EURODAC, EU level agencies have been identified that have access to and/or influence on the EU law enforcement large-scale IT systems. The proposed layer model segments the observable functioning of eu-LISA as well as the systems operating under its umbrella. The current approach helps to compare the primary functioning of EU law enforcement large-scale IT systems with the today's operation of them that may highlight aim-alignment, proportionality and connectedness as well. It is of assistance to apply the proposed methodical tool focusing on the primary research question.

***

As it was expected, the combination of institutionalist description of eu-LISA with analysis of interactions among the Agency, the systems and their environment finetune the preliminary results derived from the fragmented analyses of single EU law enforcement large-scale IT systems.

In order to be able to use the proposed methodological tool extendedly to all segments of EU law enforcement large-scale systems, it has been examined whether the

[216] *Ibid,* p. 6. Cf. 5676/11 Draft Scorecard, *op. cit.*
[217] Memorandum of Understanding on Cooperation between Frontex and Eurojust, Warsaw, 18.12.2013.
[218] *Ibid,* Art. 4(2)a, p.4.
[219] 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), p. 50.
[220] *Ibid,* Art. 5(2), p. 50.

joint operational management of existing specific law enforcement large-scale IT systems changed their functioning.

4. What does Present Tell? Inferring from Units to Multitude

Mapping up existing EU law enforcement large-scale IT systems and having considered how the newest segment of EU law enforcement large-scale IT systems' joint operational management contributes to EU migration and internal security policies, in line with the current theoretical framework, social preferences can be observed that are reflected through the systems. It means that the arrangements of the observed systems are inducted to the established indicators that are relevant to social preferences. With the help of this process, social preferences of the multitude, that means EU migration and internal security policies in this particular case, can be inferred. The procedure characterises the mentioned policy areas more sophisticatedly. However, it does not mean and it is not claimed that these characteristics are equal to the social preferences of EU migration and internal security policies. It appears also in the preliminary research question, since the systems are observed with the aim of establishing social preferences of the policy areas that are reflected through the systems and not social preferences of EU migration and internal security policies in general.

To establish social preferences of EU internal security and migration policies that are observed through law enforcement large-scale IT systems operating in the area of freedom, security and justice, the following steps have been reached.

It has been proven that the development process of the observed law enforcement large-scale IT systems operating in the area of freedom, security and justice is inherent based on findings of institutionalist analysis that has mapped underlying social processes since the formation of the systems.

The design and operation of the existing specific law enforcement large-scale IT systems operating in the area of freedom, security and justice have been observed giving functionalist exploration of SIS, VIS and EURODAC.

Combining institutionalist description of eu-LISA with analysing interactions among the Agency, the systems and their environment (functionalist mindset) have finetuned the functioning and consequences of the integrated operational management of existing specific EU law enforcement large-scale IT systems.

According to the proposed methodological tool, it is conjectured that these results reflected through the three proposed indicators can answer the primary research question. Namely, results elaborated in terms of accountability for acts, respect of human rights

standards and transparent operation can characterise social preferences of EU internal security and migration policies in the current theoretical framework. The aim of the current chapter is to arrange foregoing results along the three indicators. In that way, accepting the presumptions, the primary research question is answered.

Based on the given answer, it is also conjectured in line with the proposed methodological tool that analysing the above three indicators the relationship of the examined law enforcement large-scale IT system(s) with social beneficiality can be determined. Since it is a double conjecture, i.e. indirect inference, it shall be challenged to be proven that is carried out in a later phase.

Findings of the author's preceding publication is used for the current chapter this time as well.[221]

4.1. Sailing through the Bermuda Triangle

Accepting information power interpreted as access to information and the control over its distribution, it has been proven that information technology used in law enforcement large-scale IT systems has special, *Big Brother features*, which can be characterised by the position of the systems in social processes. A pure type identification of information power used in law enforcement large-scale IT systems has been defined by the position of information power in social processes with the combination of control society paradigm including surveillance society and risk society theories with the theoretical framework of intelligence cycle approach. Establishing the demand and supply sides of law enforcement large-scale IT systems, it has been revealed that decision makers are interested in a deeper cooperation to increase the efficiency and the amount of the stored data and of the access quality. Conversely, even decision makers shall harmonise their endeavours with the checks and balances of the rule of law. This double requirement defines the perceptions of the political players and of the state administration, which builds up the *surveillant assemblage* nature of law enforcement large-scale IT systems.

The Aristotelian roots of democratic theory address polity focusing on the way to achieve good, just and stable polity. Interpreting law enforcement large-scale IT systems as social institutions hedging socially constructed threats, their institutional arrangements

[221] Dóczi, Zoltán, The Development, the Integration and the Assessment, *op. cit.,* mainly pp. 181-183.

shall reflex onto polity criteria set by democratic theory. All social institutions can be interpreted in their environment. So that the institutional arrangements of law enforcement large-scale IT systems shall be measured by 'how good, how just and how stable' they are in their environment. In this context, they are used as independent variables.

Therefore, it has been proposed to use accountability for measuring 'good', application of human rights standards for measuring 'just' and transparency for measuring 'stable' as indicators for social measurement of law enforcement large-scale IT systems.

In what follows, foregoing results are arranged along these three indicators. It is started with the human rights perspective, the accountability and transparency problems follow all the more because human rights standards several times serve as points of reference for accountability.

Respect of Human Rights Standards

By emphasising that the European Union's accession to The Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter referred to as ECHR) will complete the system of protection in this field, the European Commission recognises the close relationship between fundamental rights system of the ECHR and the EU.[222] So that in the first instance, it is worth considering data protection guarantees of Article 8 of ECHR as core benchmark for related human rights standards connected to the observed EU law enforcement large-scale IT systems.

Article 8 of ECHR establishes the right to respect for private and family life as follows

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[222] Cf. Szalayné Sándor, Erzsébet, "Alapjogok (európai) válaszúton – Lisszabon után", *Jogtudományi Közlöny,* 68(1), pp. 15-27.

Proportionality is now an increasingly difficult concept to apply facing a new kind of, non-limited terror. Hence, facing the threat of a strategic terrorist attack, proportionality accompanies with the question of how much surveillance is enough. In this way, the necessity test of proportionality can be formulated such as whether the same information can be secured by means that are more innocuous.[223]

The European Court of Human Rights (hereinafter ECtHR) highlights the relationship between Article 8(1) and Article 8(2) of ECHR, inter alia, in *Van Kück v. Germany* case, whereas the ECtHR stipulates that

> "while the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves"[224].

Further, the ECtHR emphasises that the boundaries between the positive and negative obligations of the State under Article 8 of ECHR are not easy to define, as the applicable principles are rather similar. The fair balance is the matter of equilibrium between the general interest and the interests of the individual where, in both situations, the State enjoys a particular margin of appreciation.

It is crucial in relation to the current analysis, since as MS. BOEHM underlines in her comprehensive monograph on information sharing and data protection in the area of freedom, security and justice "the scope of Article 8 of ECHR covers the following activities: storage, release as well as different forms of collection and processing of and access to personal data."[225] Thus, it is justified to establish Article 8 ECHR as core benchmark for related human rights standards in connection with EU law enforcement large-scale IT systems, since these systems proceed and grant access to biometric data such as fingerprints and facial images.

As far as ECtHR decisions are concerned, the storage of communication information, the retention of cellular samples, DNA profiles and fingerprints constitutes an interference with the right to respect for private life. From the current point of view,

---

[223] Cf. Aldrich, Richard, J., "Transatlantic Intelligence and Security Cooperation", *International Affairs (Royal Institute of International Affairs 1944-)*, 80(4), pp. 734-736.
[224] *Van Kück v. Germany,* Application no. 35968/97, judgment of 12 June 2003, para 70.
[225] Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Heidelberg, Springer, 2012, p. 33.

the practise related to retention of fingerprints of ECtHR is important to observe. The first relevant judgements[226] addressing the question of whether the retention of fingerprints alone amounts to an interference was highly controversial. As a development, in a further, more recent case of *S. and Marper v. the United Kingdom,* the ECtHR clarified that fingerprints contain exclusive information about an individual allowing for precise identification in a wide range of circumstances. Thus, retention of this information without the consent of the individual concerned cannot be regarded as neutral or irrelevant.[227] According to the judgement,

> "the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns."[228]

The protection of personal data is not an unlimited right. However, the demanded aim and the significance of the limitation shall be in line reciprocally, which is an essential condition for the constitutional, i.e. due process restriction of rights.

In case of SIS II, the Charter of Fundamental Rights of the European Union, especially its Article 45[229] shall be taken into account applying the SIS II rules. However, as it has been referred to above, it is less clear how the SIS relates to third country nationals. In the preamble of SIS II Regulation , it is said that further harmonisation of the provisions on the grounds for issuing alerts concerning third country nationals for the purpose of refusing entry or stay and the clarification of their use in the framework of asylum, immigration and return policies are needed. On the one hand, it is unfortunate that the express clause giving priority to other EU immigration and asylum legislation was dropped. On the other hand, it is still arguable that such legislation takes priority over the SIS II legislation even in the absence of an express rule to that effect.

In this context, it is worth considering that the introduction of biometric data was heavily disputed, since dangers arising out of the use of biometric data were subject to

---

[226] *Mc Veigh and others v. United Kingdom,* Application no. 8022/77, Commission decision of 18 March 1981; *Kinnunen v. Finland,* Application no. 18291/91, Commission decision of 13 October 1993.
[227] Boehm, Franziska, *Information Sharing and Data Protection*, *op. cit.*, p. 42.
[228] *S. and Marper v the United Kingdom,* Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 85.
[229] "Freedom of movement and of residence
1. Every citizen of the Union has the right to move and reside freely within the territory of the Member States.
2. Freedom of movement and residence may be granted, in accordance with the Treaty establishing the European Community, to nationals of third countries legally resident in the territory of a Member State."

several studies since the creation of SIS.[230] Criticism is mainly referred to in relation to the storage of data that is claimed to have quasi permanent and distinctive nature due to the application of varying national law.

Article 106 (1) of the Schengen Implementing Convention[231] establishes, as BOEHM refers to, "the 'owner principle' that only the state originally entering the data has permission later to change, modify or delete them."[232] The provision related to the responsibility of the contracting states guarantees that the data entered in the SIS are accurate, up to date and lawful.

Article 111 of the Schengen Implementing Convention[233] gives an individual the right to bring an action to correct, delete or obtain information or compensation related to its data in the SIS before the courts or a competent authority under national law. The final decisions are mutually enforceable in the Schengen States. However, there are cases in practice when the functioning of this provision is doubted.[234]

Generally, the individual rights standard acknowledged in the SIS is in principle maintained in the SIS II.[235] Bearing in mind, that SIS II contains data for the following two categories as minor of age, mentally ill patients, and missing persons or in danger with an aim of ensuring their own protection and persons requested by a judicial authority, such as witnesses, those quoted to appear for notification of judgement and absconders. Taking the above presented *S. and Marper v. the United Kingdom* case, the ECtHR demands a different treatment of biometric data of persons who have been convicted of an offence and those who have never been convicted (e.g. only suspected) as well as the respect of the age of the person whose data are entered in the database. Accordingly, further safeguards relating to the protection of witness data as well as to data of minors should have been included in the SIS II legal instruments.

As far as time limits of data storage concerned, data in SIS II is stored only for the time required to achieve the purpose for which it was entered. Both the Schengen Implementing Convention and the SIS II instruments provide for a review of the need to

---

[230] Mahmood, Shiraz, "The Schengen Information System: An Inequitable Data Protection Regime", *International Journal of Refugee Law*, 7(2), 1995, pp. 179-200.
[231] Schengen Implementing Convention, *op. cit.*, Art. 106(1), p. 46.
[232] Boehm, Franziska, *Information Sharing and Data Protection*, *op. cit.*, p. 272.
[233] Schengen Implementing Convention, *op. cit.*, Art. 111, p. 47.
[234] Cf. the case of Mr. and Mrs. Moon; for further analysis see: Brouwer, Evelin, "The Other Side of the Moon: The Schengen Information System and Human Rights: A Task for National Courts", CEPS Working Document No. 288/April 2008, Centre for European Policy Studies, 2008, http://www.ceps.eu/files/book/1642.pdf, [27.10.2014.].
[235] Boehm, Franziska, *Information Sharing and Data Protection*, *op. cit.*, pp. 271-275.

continue storage not later than three years after the date of introduction into the SIS. The maximum of the storage period is five or ten years.

Besides the criticism, there is also an important improvement relating to the right of information of third country nationals who are subject to an alert, since about the issued alerts, these persons

> "shall be informed in accordance with Articles 10 and 11 of Directive 95/46/EC. This information shall be provided in writing, together with a copy of or a reference to the national decision giving rise to the alert, as referred to in Article 24(1)."[236]

However, for EU-nationals, the general right to be informed is not established. EU-nationals shall act in order to be informed about their inclusion in the SIS.[237]

This option, i.e. the right to request access to data relating to him/her that has been entered in SIS II, and to have factually inaccurate personal data corrected or unlawfully stored personal data deleted, is provided for both categories of personal scope. However, information may not be communicated to the data subject if this is indispensable for the performance of a task in connection with an alert or for the protection of the rights and freedoms of third parties. Regarding the exercise of their rights of correction and deletion, individuals are informed about the follow-up as soon as possible, and in any event no later than three months from the date of their application for correction or deletion. It is possible for any person to bring an action before the competent courts or authorities to access, correct, delete, or obtain information or compensation in connection with an alert relating to him/her. Processing sensitive categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and data concerning health or sex life) in SIS is prohibited.

For the analysis of VIS, the VIS Regulation is observed preliminary. However, the related Council Decision is taken into account as well.[238] As it has been highlighted, the collected and stored data by VIS concern short-stay, transit and airport transit visas, visas with limited territorial validity and long stay visas. Ten-digit finger scans and a digital photograph are collected from persons applying for a visa. Frequent travellers to the Schengen area do not have to give new finger scans every time they apply for a new

[236] Regulation (EC) No 1987/2006, *op. cit.,* Art. 42(1) p. 19.
[237] Council Decision 2007/533/JHA, *op. cit.,* Art. 58, p. 81.
[238] Regulation (EC) No 767/2008, *op. cit.* and Council Decision 2008/633/JHA, *op. cit.*

visa. The first record is linked with a possible previous application file and with application files of persons travelling together (group, spouse and children).

The processing of biometric data enables Schengen States to verify and identify the visa applicants aiming at the prevention of irregular immigration. Ten-digit finger scans are not required from children under the age of twelve or from persons who physically cannot provide finger scans. The usage of fingerprints facilitates the comparisons as whether the person showing the visa corresponds to the person who has originally obtained the visa. Moreover, by comparison of fingerprints with all VIS data, fingerprints identify persons not being in possession of identification papers or trying to use false identification data.

VIS data are kept generally up to a maximum of five years and that includes all data entered by the visa authorities of the Schengen States[239] including data relating to applications that have been withdrawn, closed or discontinued.[240] A record of each VIS entry shall be kept at the Schengen State and at eu-LISA for one year after the deletion of the data in the VIS.[241] However, these records "may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security."[242] Nevertheless, the retention period can be extended in case the data are required for "monitoring procedures which have already begun."[243] If an applicant has acquired the nationality of a Member State or of a Schengen associated country or the Schengen State entering the data decides to delete them, the data and the links shall be removed without any delay.[244] BOEHM underlines the lack of time limit in relation to data retrieved from the VIS and then kept in national files. As she points at Article 30 of the VIS Regulation, it is possible in line with the purposes of the VIS and in individual cases for the period of "no longer than necessary in that individual case."[245]

Up till now, in comparison of the ECtHR demand of biometric data treatment related to persons who have been convicted of an offence and those who have never been as well as the respect of the age of the person, VIS shows a more sophisticated approach

[239] In the current section, the author deliberately uses Schengen States for referring to VIS-user States in contrast to the concrete text of the applicable legislation aiming at expressing the real situation caused by the accommodation of *la géométrie variable* (variable geometry).
[240] Regulation (EC) No 767/2008, *op. cit.,* Art. 23(1), p. 71.
[241] *Ibid,* Art. 34, p. 75.
[242] *Ibid,* Art. 34(2), p. 75.
[243] *Ibid.*
[244] *Ibid,* Art.23 (1), p. 71. and Art. 24-25, p. 72.
[245] Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* p. 291 quotes from Regulation (EC) No 767/2008, *op. cit.,* Art. 30(1), p. 74.

than SIS. For minor of age with regard to fingerprints, the twelve-year age limit is established. Deadlines for data retention are fixed and the use of such data is aim-aligned to the purposes of VIS. It is valid for data retrieved from the VIS and then kept in national files.[246]

Not only visa applicants but also persons issuing an invitation or liable to pay the applicant's subsistence cost during the stay are informed of the identity of the controller, the purpose of the data processing in the VIS, the categories of recipients of the data, including Europol and the so-called designated authorities, the data retention period, the existence of their right to access and the right to request rectification or deletion of their data, as well as of the right to receive information on the procedures for exercising those rights and even of the contact details of the national data protection authority responsible for hearing their claims.[247] Rules for individuals to obtain access to the data stored in the VIS and to have them corrected and deleted are subjected to national law.[248] These rights can be exercised in any Schengen State that subsequently has to contact the responsible Schengen State originally entering the data in the VIS.[249] In case the Schengen State corrects or deletes the data, it has to notify the person concerned that the relevant action has been taken.[250] As for guarantee, cooperation between Schengen States is also ensured.[251] Moreover, national data protection authorities shall assist, advise and remain available throughout possible proceeding for persons concerned in exercising their rights.[252] Liability for damages caused by unlawful data processing is also governed by national law.[253]

As it has been mentioned, VIS aims at the facilitation of entry for those whom a visa is required. A visa in itself is a (conditional) entry permit, since it is the right of the sovereign to decide on the admission of non-nationals. However, these procedures shall be objective and due processes to be in line with generally accepted human rights standards.

EURODAC is a database that stores and compares fingerprints of asylum applicants and irregular migrants apprehended in connection with the irregular crossing

[246] Regulation (EC) No 767/2008, *op. cit.*, Art. 30(3), p. 74.
[247] *Ibid*, Art. 37, p. 76 – mainly Art. 37(1)a-f.
[248] *Ibid*, Art. 38(1), p. 76.
[249] *Ibid*, Art. 38(2)-(3), p. 76.
[250] *Ibid*, Art. 38(4), p. 76.
[251] *Ibid*, Art. 39, p. 77.
[252] *Ibid*, Art. 39-40, p. 77.
[253] *Ibid*, Art. 33, p. 75.

of an external border. As far as the EURODAC is concerned and as it has been mentioned above, the following data are collected for any asylum applicants over fourteen 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. So, in relation to the ECtHR test, the age limit has to be emphasised. Moreover, the same age limit is applied in relation to apprehended irregular migrants.[254]

Data are collected and sent to the Central Unit via national access points. The maximum time limit for data storage is ten years for asylum seekers.[255] The data have to be erased *mutatis mutandis* as in case of VIS, i.e. as soon as the applicant has acquired citizenship of a Member State, however, they must be blocked as soon as the applicant is recognised and admitted as refugee.[256] The storage limit for irregular external border crossers generally is two years.[257] In addition, applying the same legal technique, in case the person acquires citizenship, obtains a residence permit or leaves the EU territory, the data shall be erased.[258] By turning the New EURODAC Regulation applicable, there was a single but important change in relation to the storage period. The storage limit in case of irregular external border crossings decreased to eighteen months.[259]

Member States may not conduct searches in or get data transferred by another Member State apart from the data resulting from the comparison.[260] Only the Member State or the Central Unit on request of the Member State entering the data has the right to amend or erase them.[261] These provisions have remained under the New EURODAC Regulation with streamlining of changing Central Unit to Central System and supplementing a public list of designated authorities.[262] If a Member State does not agree with the fact that the data stored in the central database are factually incorrect or unlawfully recorded, it must explain to the person concerned the reasons for the decision together with information explaining the steps to be taken if the person concerned does not accept the explanation given (how to bring a complaint before court, provide financial

[254] Council Regulation (EC) No 2725/2000, *op. cit.,* Art. 8(1), p. 4.
[255] *Ibid,* Art.6, p. 4.
[256] *Ibid,* Art. 7, p. 4 and Art 12, p. 6.
[257] *Ibid,* Art. 10(1), p. 5.
[258] *Ibid,* Art. 10(2), p. 5.
[259] Regulation (EU) No 603/2013, *op. cit,,* Art. 16, pp. 12-13.
[260] Council Regulation (EC) No 2725/2000, *op. cit.,* Art. 15(3), p. 7.
[261] *Ibid,* Art. 15(1), p. 7.
[262] Regulation (EU) No 603/2013, *op. cit,,* Art. 27, p. 17.

or other assistance etc.).[263] A novelty of the New EURODAC Regulation is that this procedure concerns not only the data subject (i.e. the person concerned) but also "any person" may request it.[264]

In addition to the rights of access, correction and/or deletion, the rights of the persons concerned include broader information right that includes the right to be informed about the identity of the controller, the purpose for processing, the recipients of the data, the existence of the right of access and rectification of data and the obligation to have fingerprints taken.[265] The information is generally to be provided when the fingerprints are taken.[266] For irregular external border crossers, there is an exception, since in general such information is to be provided when the data of the illegal residents are transmitted to the Central Unit.[267] Moreover, the obligation can be dropped in case

> "the provision of such information proves impossible or would involve a disproportionate effort."[268]

This situation was changed by the application of the New EURODAC Regulation, since the information on individual rights and data protection issues shall be given both to asylum applicants and to irregular external border crossers

> "in writing, and where necessary, orally, in a language that he or she understands or is reasonably supposed to understand"[269].

In the case of EURODAC, liability is governed by national law as well.[270] That is more explicitly emphasised in the New EURODAC Regulation.[271]

Concluding EURODAC, it is visible that from the current point of view, is more precisely regulated compared to SIS. However, it is also exposed to the same phenomena.

By the creation of EURODAC, the criminalisation of asylum seekers were proven and criticised by several authors.[272] The discussion is still ongoing in case of the New

[263] Council Regulation (EC) No 2725/2000, *op. cit.*, Art. 18(6), p. 8.
[264] Regulation (EU) No 603/2013, *op. cit,*, Art. 29(5), p. 19.
[265] Council Regulation (EC) No 2725/2000, *op. cit.*, Art. 18(1), p. 8.
[266] *Ibid.*
[267] *Ibid.*
[268] *Ibid.*
[269] Regulation (EU) No 603/2013, *op. cit,*, Art. 29(1), p. 18.
[270] Council Regulation (EC) No 2725/2000, *op. cit.*, Art. 17(2), p. 7. Cf. Regulation (EU) No 603/2013, *op. cit.*, Art. 37(2), p. 22.
[271] Regulation (EU) No 603/2013, *op. cit,*, Art. 37(3), p. 22.
[272] See as an early example: van der Ploeg, Irma, "The illegal body: 'Eurodac' and the politics of biometric identification", *Ethics and Information Technology*, 1(4), 1999, pp. 295-302.

EURODAC Regulation, too.[273] As a common point of reference, the nature of taking fingerprints can be established. In criminal law, according to the mainstream literature, the benchmark of taking them is a suspected serious crime (that may be taken in custody or detention on remand). In the context of migration and asylum law, this criterion is loosened to a significant extent, i.e. no suspicion of serious crimes is required, but instead, a serious doubt regarding a person's identity. Moreover, in case of EURODAC, seeking international protection is an established ground for them. As far as the above ECtHR test is concerned, MS. BROUWER underlines in relation to EURODAC that

> "[e]ven if one assumes that this purpose [i.e. the establishment of the State responsible for the examination of a request for asylum] is to be considered as a legitimate aim in the sense of Article 8 ECHR, the question remains if the chosen instrument is necessary or even effective."[274]

Eu-LISA shall perform the tasks of the "Management Authority" as it has pointed out above presenting its creation. It means that all of the existing legal instruments of SIS, VIS and EURODAC shall govern its own structure. Being technically responsible, the specific rules with regard to the purpose of processing, access rights, security measures and further data protection requirements applicable to each of the systems are not affected. The Agency in itself is subject to Regulation 45/2001[275], since it is an EU body with legal personality[276] as it has been elaborated above. It means that an internal data protection officer shall (additionally) supervise the Agency.[277] The accepted eu-LISA Regulation refers to specific articles of Title V of TFEU as the legal basis of the Agency. It is more welcome than the proposal appointing (the whole) Title V of TFEU as the legal basis. However, the presented legal bases are used quite extensively.[278]

Eu-LISA Regulation refers to rather wide-ranging tasks including the operational management of the three mentioned systems and the development and management of

[273] Roots, Lehte, "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies,* 5(2), pp. 108-129.
[274] Brouwer, E.R., "Eurodac: Its Limitations and Temptations", *European Journal of Migration and Law,* 4(2), 2002, p. 244.
[275] 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, pp. 1-22.
[276] Regulation (EU) No 1077/2011, *op. cit.*, Art. 10(1), p. 7.
[277] *Ibid,* Art. 28, p. 14.
[278] "TFEU and in particular Article 74, Article 77(2)(a) and (b), Article 78(2)(e), Article 79(2)(c), Article 82(1)(d), Article 85(1), Article 87(2)(a) and Article 88(2)", *ibid,* p. 1.

other large-scale IT systems "based on Articles 67 to 89 TFEU"[279] meaning the application of the whole Title V of TFEU (Area of Freedom, Security and Justice).

The potential threat that may fundamentally change the nature of the existing EU law enforcement large-scale IT systems is interoperability. As of now, it is prohibited.[280] However, the text of eu-LISA has left the question open stating that

> "large-scale IT systems shall not exchange data or enable sharing of information or knowledge, unless so provided in a specific legal basis."[281]

Eu-LISA cannot act on its own to create new large-scale IT system. The initiative for the development of such system that practically may operate in any particular or all segments of the area of freedom, security and justice shall be based on the specific and precise request of the Commission.[282] The European Parliament, the Council and the European Data Protection Supervisor where concerned shall be kept updated about the development.[283] Regarding the wide-ranging scope of the Agency that could theoretically develop and manage any large-scale IT system in the area of freedom, security and justice, the risks of errors and abuse should be taken into account. However, the monitoring of a single operator instead of three different means the usage of same standards. Nevertheless, the risk of interoperability or direct interconnectedness shall be considered, since the existing systems are using the same infrastructure enhancing technical feasibility of a merger.

Accountability for Acts

The foregoing presentation of human rights standards helps analysing the accountability aspect, since several times the above-mentioned relationship with those standards serves as points of reference for accountability. EU accession to ECHR will enhance accountability for alleged human rights violations granting a new forum, the ECtHR to enforce lawful operations.

The nature of EU rules in relation to individual data shall be borne in mind. There are other regimes such as in the United States of America where personal data are sold

[279] *Ibid,* Art. 1(3), p. 6.
[280] Cf. *ibid,* Art. 1(4), p. 6.
[281] *Ibid.*
[282] *Ibid,* Art.9 (1), p. 7.
[283] *Ibid.*

and bought like goods in a market, i.e. they are widely traded. EU provisions limit the commodity-like use of personal data. Moreover, the EU Privacy Directive and also its reform proposal[284] include an extraterritorial guarantees that requires adequate, i.e. in line with EU norms, protection of personal information transferred from Member States.[285]

The first supervisory authority of law enforcement large-scale IT systems was established in relation to SIS. The joint supervisory authority supervised compliance with data protection rules in connection with CS-SIS, i.e. the central infrastructure.[286] The joint supervisory authority consisted of two representatives from national supervisory authorities.[287] The joint supervisory authority was not a forum for reconciling potential conflicts may arise among Member States in relation to data entry to SIS. Its role was more like an advisory group that can be justified by its delivered non-binding opinions.[288] Member States were responsible for the supervision of N.SIS. Therefore, in line with the principles of subsidiarity and proportionality, the guarantee system related to the supervision of individual rights was divided. The Joint Supervisory Authority ceased to exist on 9 April, 2013 as of SIS II has become operational.

As becoming SIS II operational, data protection supervision has changed. Supervision of the SIS II is structured differently from the rules of the Schengen Implementing Convention. Its supervision is based on cooperation between the European Data Protection Supervisor and the national data protection authorities whereby the latter remain responsible for the N.SIS II.[289] The EDPS checks the personal data processing activity of eu-LISA as being responsible for the operational management of the CS-SIS.[290] National data protection authorities and EDPS shall meet at least twice a year to improve their cooperation, it means studying common problems, drawing up harmonised proposals for joint solutions and assisting each other in carrying out audits and

[284] 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, pp. 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, pp. 1-22. Cf. COM(2012) 11 final Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.12012.

[285] See also: Newman, Abraham L., "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Protection Directive", *International Organisation,* 62(1), 2008, pp. 103-130.

[286] Schengen Implementing Convention, *op. cit.,* Art. 114-115, pp. 47-48.

[287] *Ibid,* Art. 115(1), p. 47.

[288] *Ibid,* Art. 115, p. 47-48.

[289] Council Decision 2007/533/JHA, *op. cit.,* Art. 62, p. 82.

[290] Cf. *Ibid,* Art. 61, p. 81.

inspections. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the eu-LISA in every two years.[291] This cooperation mechanism indicates a more enhanced supervision of SIS II than of SIS was supervised. Moreover, the CS-SIS supervision as a general responsibility of the EDPS is a welcome change.

Monitoring of the VIS is shared between the national data protection authorities and the EDPS like the SIS II. The national data protection authorities implement the national part of the VIS including the monitoring of the transmission of data to and from the VIS.[292] It is welcome that it is explicitly stated that Schengen States must further ensure that these authorities are sufficiently equipped with resources to fulfil their tasks. Moreover, national data protection authorities shall carry out an audit of the data processing operations of the national VIS at least every four years.[293] The EDPS is responsible for monitoring the processing of personal data by eu-LISA as being accountable for the management of the central VIS and the national interfaces.[294] The EDPS, like the national authorities, shall make an audit on data proceeding activities of eu-LISA related to VIS and submit the report to the European Parliament, the Council, the Commission and the national data protection authorities.[295] In VIS related tasks, eu-LISA shall give requested information to EDPS, grant access for EDPS to all documents and to its records, and allow him/her access to all its premises.[296] Cooperation among the EDPS and national data protection authorities are designed *mutatis mutandis* compared to SIS II. Supporting comprehensive supervision, it means that meetings are held at least twice a year to coordinate mutual assistance and to examine difficulties of interpretation.[297] A joint report of activities shall be sent to the European Parliament, the Commission and the eu-LISA every two years.[298]

Currently supervision over the data processing of the EURODAC Central Unit is carried out by the EDPS. In relation to EURODAC, the national data protection authorities are responsible for monitoring the collection and transmission of the

[291] *Ibid,* Art. 62(2-3), p. 82 together with Regulation (EC) No 1987/2006, *op. cit.,* Art. 46(2-3) p. 120.
[292] Regulation (EC) No 767/2008, *op. cit.,* Art. 41(1), p. 77.
[293] *Ibid,* Art. 41(3) and 41(2), p. 77.
[294] *Ibid,* Art. 42(1), p. 77.
[295] *Ibid,* Art. 42(2), p. 77.
[296] *Ibid,* Art. 42(3), p. 77.
[297] *Ibid,* Art. 43(1), p. 77.
[298] *Ibid,* Art. 43(3), p. 78.

fingerprint information to the Central Unit at national level whereas national authorities shall have access to advice from persons with sufficient knowledge of fingerprint data.[299]

The EURODAC Supervision Coordination Group ensures coordination between the EDPS and the national data protection authorities. However, the current scope of functioning of the joint supervisory authority as the EURODAC Regulation establishes resembles the above joint supervisory authority set out for SIS by the Schengen Implementing Convention.[300] The New EURODAC Regulation gives legal basis to the cooperation of EDPS and national data protection authorities under EURODAC Supervision Coordination Group.[301] Moreover, the new provisions bring in line EURODAC supervision structure with the ones of SIS II and VIS.[302]

The same arrangements for existing EU law enforcement large-scale IT systems enhance accountability of the systems by unified procedures.

However, in relation to EURODAC, the role of DubliNet[303] shall be underlined as far as accountability is concerned. Points of connections are to be highlighted in the transparency subsection arise from the legal provisions governing the large-scale IT systems and are relevant to other EU bodies. However, DubliNet establishes interactions based on and not as part of neither the previous, nor the New EURODAC Regulation.[304] DubliNet is a secure electronic network of transmission channels between the national authorities dealing with asylum applications. However, the data protection guarantees of the DubliNet system that allows for additional data exchange were not sufficiently developed before the approval of the Dublin III Regulation[305], since the Regulation establishing the DubliNet includes technical details of the organisation of DubliNet, but does not refer to data protection guarantees. Dublin III Regulation has solved this problem by stipulating that DubliNet information exchange shall solely be used for the purpose set out in Article 31(1) of the Dublin III Regulation[306] restricting the aim of DubliNet data

[299] Council Regulation (EC) No 2725/2000, *op. cit.*, Art. 13, p. 6. and Art. 19, p 9.
[300] *Ibid,* Art. 20, p. 9.
[301] Regulation (EU) No 603/2013, *op. cit.*, Art. 32, pp. 19-20.
[302] *Ibid,* Art. 30-32, pp. 19-20.
[303] Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 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 222, 5.9.2003, pp. 3-23.
[304] *Ibid,* Art. 18(1), p. 8.
[305] Regulation (EU) No 604/2013, *op. cit.*
[306] *Ibid,* p. 47.

processed.[307] In this way, Dublin III Regulation and related data protection standards have become applicable to DubliNet as well.

As liability of existing EU law enforcement large-scale IT systems is in question, their liabilities are governed by national law as it has been mentioned in the preceding subsection.

Eu-LISA as joint operator is liable to its acts without prejudice of the governed systems' liability. Eu-LISA is an EU body with legal personality[308] being liable for contractual and non-contractual relations having national courts and the Court of Justice of the European Union jurisdiction over it.[309] As an EU body handling public money, it is accountable to the Commission's Accounting Officer, the Court of Auditors and the European Commission's European Anti-Fraud Office (OLAF). As it has been presented in the governance structure subsection, eu-LISA shall keep up-dated and is politically responsible to the European Parliament, the Council and, where data protection issues are concerned, the European Data Protection Supervisor. Again, eu-LISA Regulation refers to rather wide-ranging tasks including the operational management of the three mentioned systems and the development and management of other large-scale IT systems "based on Articles 67 to 89 TFEU"[310] meaning the application of the whole Title V of TFEU (Area of Freedom, Security and Justice). Main concerns in this context arise relating to the absence of a definition of the large-scale IT system and to the wider scope, referring to Title V of TFEU embracing different policies such as rules on border checks, asylum and immigration as well as judicial cooperation in civil and criminal matters and police cooperation.

Limitations to possible modifications of the existing EU law enforcement large-scale IT systems and to the future ones shall derive from Title V of TFEU, since both are (at least partly) governed by these provisions. Mechanisms under Title V of TFEU designate the limits of accountability of these systems. Non-binding peer evaluation within the area of freedom, security and justice facilitates accountability of the systems if a Member State is concerned, since Article 70 of TFEU establishes the following:

> "Without prejudice to Articles 258, 259 and 260, the Council may, on a proposal from the Commission, adopt measures laying down the arrangements whereby Member States, in collaboration with the Commission, conduct objective and impartial evaluation of the

[307] *Ibid*, Art. 31(3), p. 48.
[308] Regulation (EU) No 1077/2011, *op. cit.*, Art. 10(1), p. 7.
[309] *Ibid*, Art. 24(1)-(4), p. 13.
[310] *Ibid*, Art. 1(3), p. 6.

> implementation of the Union policies referred to in this Title by Member States' authorities, in particular in order to facilitate full application of the principle of mutual recognition. The European Parliament and national Parliaments shall be informed of the content and results of the evaluation."[311]

Key characteristics of peer review procedures were established by STINE ANDERSEN.[312] These are, inter alia, the following: they are multilateral; the resolution is non-binding and may include compliance recommendations; the procedures are primarily transparent, but may involve confidential information; the European Parliament and national Parliaments shall be informed of the content and results of the evaluation; review takes place on a regular basis; and Commission plays a central and semi-political role.

Accountability is an important factor if migration is interpreted in security context, since, paraphrasing CARRERA[313] from another context, the misinterpretation and overuse of exceptions (i.e. concepts of public policy and national security) that are purely justified on behalf of security may undermine the very roots of an area of freedom in the EU.

Transparent Operation

In this subsection, among other factors relevant to transparency criteria, points of connections arising from the legal provisions governing the existing EU large-scale IT systems and are relevant to another EU bodies are to be highlighted.

Above findings concerning general structure of eu-LISA indicate challenges for transparent operation coming from inside eu-LISA, i.e. from intra-institutional arrangements. As the legal bases of eu-LISA were merged under articles of Title V of the Treaty of Lisbon, the Agency is affected by *la géométrie variable* deriving from the protocols on the positions of the United Kingdom, Ireland and Denmark, since these protocols are included in the Treaty of Lisbon with some minor amendments.[314] Eu-LISA Regulation constitutes the development of the Schengen *acquis* and builds on the provisions of EURODAC related measures. *La géométrie variable* of the Agency is bound by legislative framework of the Lisbon Treaty, by the problem of Schengen

[311] Treaty on the Functioning of the European Union, *op. cit.*, Art. 70, p. 74.
[312] Andersen, Stine, "Non-Binding Peer Evaluation within an Area of Freedom, Security and Justice", in Holzhacker, Ronald L. and Luif, Paul (ed.), *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*, New York, Springer, 2014, pp. 29-48.
[313] Carrera, Sergio, "What Does Free Movement Mean in Theory and Practice in an Enlarged EU?", *European Law Journal*, 11(6), 2005, p. 721.
[314] See: Ch. II.1.3.

associate countries and by *non-Schengen* EU Member States not obtaining opt-out on the Schengen *acquis*. With regard to the accommodation of *la géométrie variable,* it has been claimed that it may cause delays in setting annual budget and work programme due to the fact that 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. So that complex and non-transparent structure of rules and procedures is needed to accommodate *la géométrie variable*. It reduces the level of supervision giving more places to the risk of function creep.

For the analysis of transparent operation arising from inter-institutional arrangements, the layer model[315] has been developed. The distinguished management and cooperation levels concern the criteria of transparency.

The management level encompasses, inter alia, "across system" relations. Originally, two "inter law enforcement large-scale IT system acts" were applicable. The VIS facilitated the application of the Dublin II Regulation and facilitates the application of the Dublin III Regulation as well by granting access to asylum authorities to search the VIS fingerprint data solely for the purpose of determining the country responsible for the examination of an asylum application and of examining an asylum application, if the fingerprints of the asylum seeker cannot be used or the search fails, the authorities may carry out the search using other VIS data.[316] Moreover, the VIS has been harmonised with the Schengen Borders Code by a regulation[317]. 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.[318] EURODAC has become accessible for designated authorities (including Europol) for law enforcement purposes. As far as conditions for access are concerned, EURODAC data has become accessible, inter alia, after VIS data have been consulted without leading to the establishment of identity of data subject.[319] VIS data in this case shall be consulted first only in case of law enforcement purposes set out in VIS Decision 2008/633/JHA.[320]

[315] See: Ch. II.3.4.
[316] Regulation (EC) No 767/2008, *op. cit.,* Art. 21-22, pp. 70-71.
[317] Regulation (EC) No 81/2009, *op. cit.*
[318] *Ibid,* Art. 54(6)b, p. 24.
[319] Regulation (EU) No 603/2013, *op. cit.,*, Art. 20(1), p. 14.
[320] Council Decision 2008/633/JHA, *op. cit.,* Art. 5(1), p. 132.

Having VIS and EURODAC relation concerning the determination of the country responsible for the examination of an asylum application and of the examination of an asylum application, having also SIS II and VIS relation in connection with enforcing entry ban, and having the recently established VIS and EURODAC relation concerning conditions for granting access in case of law enforcement purposes, indirect interconnectedness of EU law enforcement large-scale IT systems is observed on the management level. It can be supported by the fact that the same authorities (however, probably not the same units) may be designated to access the systems, since it is the responsibility of each Member State to set her own public administration up. Joint institutional arrangements of designated authorities (cf. Europol access as well) result in indirect interconnectedness that may be mitigated by intra-institutional rules of procedures.

It is also debatable that the whereabouts of the transferred data are often not clarified, e.g. into which databases the data are introduced and which third parties get access to the data. It is not explained before the data transfer. Different accessing actors may lead to extension of authorities possibly using the transferred data. Time limits for storing the data in the original database may also be extended by the data transfer to other databases.[321]

Europol and Eurojust are involved in the work of eu-LISA on the agency and management 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 acts is to strengthen the operative cooperation among EU law enforcement agencies. The JHA mentioned four agencies have established an extended cooperation framework based on bilateral cooperation and information exchange. Moreover, a multilateral cooperation is planned among them.[322] According to BOEHM, inter-agency information sharing has been found to be accompanied with unsatisfactory data protection framework.[323] These interrelations could have complementary influence on the operational practice of eu-LISA, since Eurojust, Europol and FRONTEX shall work together for the Standing

[321] Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* p. 369.
[322] 5816/10 Interim report on cooperation between JHA Agencies, Brussels, 29.1.2010; and 5676/11 Draft Scorecar2d – Implementation of the JHA Agencies report, Brussels, 25.1.2011.
[323] See: Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* pp. 342-344.

Committee on operational cooperation on internal security (commonly referred to as COSI).[324] Furthermore, the Standing Committee shall help to ensure consistency of their actions.[325]

The accommodation of *la géométrie variable* within the eu-LISA together with indirect interconnectedness and the less safeguarded data transfer to JHA agencies of the observed large-scale IT systems are significant concerns related to transparent operation. Analysing the legal instruments of the SIS II, VIS and EURODAC, EU level agencies have been identified that have access to and/or influence on the EU law enforcement large-scale IT systems. Indirect interconnectedness may distort aim-assigned operation of the systems causing serious disproportionality. Moreover, the potential threat that may fundamentally change the nature of the existing EU law enforcement large-scale IT systems is interoperability that is, as of now, prohibited "unless so provided in a specific legal basis". [326]

***

As BIGO explained, profiling immigrants establishes a group of potential travellers who are not permitted to enter due to abstract virtual profiles of unwanted persons. These profiles are one of the products of large-scale IT systems' operation, since using information power profiles are created to prevent law breaching. This group will never see Europe, since people with almost the same profile have already been there and expelled.[327]

4.2. Social Preferences and Social Beneficiality

The main intention of the current subsection is to summarise the social preferences of EU internal security and migration policies that are observed through law enforcement large-scale IT systems operating in the area of freedom, security and justice. According to the proposed methodological tool, it is conjectured that results reflected through the

[324] 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), p. 50.
[325] *Ibid*, Art. 5(2), p. 50.
[326] Regulation (EU) No 1077/2011, *op. cit.*, Art. 1(4), p. 6.
[327] Bigo, Didier, "The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts", *Security Dialogue*, 45(3), 2014, p. 219.

three above indicators can answer the question by characterising social preferences of EU internal security and migration policies in the current theoretical framework.

It is also conjectured in line with the proposed methodological tool that analysing the indicators the relationship of the examined law enforcement large-scale IT system with social beneficiality can be determined. Since it is a double conjecture, i.e. indirect inference, it shall be challenged to be proven that will be carried out in the next section.

The smart, appropriate combination of the judicious use of information technology with the discriminating and sensible patterns of intelligence cooperation could guarantee that activities of security and intelligence organizations do not erode the qualities of freedom in a democracy; instead, they can sustain and extend liberties.[328]

As it has been established above, evaluating an observed law enforcement large-scale IT system's optimality following the measurement along the three indicators, it is important that the indicators shall balance each other. The reason for it derives from the starting point. In democratic theories, the *Dahlian 'polyarchy',* i.e. the pluralist interplay of groups is viewed as democracy. HUNTINGTON worried about a 'democratic distemper' in which citizens demand more than the system can deliver. Therefore, the transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement.

Society's acceptance of new technologies in law enforcement has three levels such as the technology and research, the technology and privacy, and the technology and society.[329] Concerns with a new technology will decrease if that technology is fully integrated and accepted in the society. Social measurement of law enforcement large-scale IT systems may be of assistance in relation to the evaluation of their level of acceptance as well.

Respect of human rights standards has been interpreted alone, inside the systems. Accountability for acts indicator has dealt with internal and external factors. Transparent operation has focused on the environment of the systems. Results of the indicators cannot be interpreted in absolute terms, i.e. it is rather a philosophical question to establish levels for how good their functioning is. Therefore, the relative relationship of the indicator results is proposed to be measured. For this, a simple but appropriate tool is chosen. Patterns of all the systems drawn up by the indicators are summed up via a SWOT analysis.

[328] Aldrich, Richard, J., Transatlantic Intelligence and Security Cooperation, *op. cit.*, p. 736.
[329] Pattavina, April (ed.), *Information Technology and the Criminal Justice System*, *op. cit.*, pp. 261-271.

The centralisation of operational management is a **strength**, since focused knowledge and sufficient personal resources might be an advantage in the daily work with the systems including the monitoring of only one operator instead of three different databases. The institutionalisation of the operational management creates clear ground for the accountability. The accountability of eu-LISA is ensured by EU institutions. Furthermore, the Agency provides a visible and dedicated structure that is also more visible and approachable for the civil society. The long-term cost efficiency is guaranteed by the fostered usage of the same technical solutions and by the preparation, development and operational management tasks related to other IT large-scale systems, which might be delegated to eu-LISA. 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 installations also indicates synergies in installations, operational management and monitoring.

Conversely, the accommodation of *la géométrie variable* is a **weakness** in the future operation of the systems, since eu-LISA 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 Agency's work. Furthermore, the Agency is not cost-efficient in short-term. The costs and time of setting up the Agency and the transition to new location (i.e. to the new Tallinn headquarters) result in the loss of key staff, training costs and could result in delays in planning and deployment; which means discontinuity. In short-term, there are also high overheads that 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 Agency's organisation, due to legislative procedures and discussion about location, governance structure, employment of staff 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 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 Agency can be avoided if the scope of (possible) activities of the Agency are limited and clearly defined in the founding legal instrument. The application of ordinary legislative procedure decreased the risk of this factor. The eu-LISA Regulation is clear and enumerates well-defined tasks. However, the possibility of function creep is a clear **threat**. In any case, the risk that one day the different systems will be directly interconnected since they are using the same infrastructure and it is technically feasible to do so, should be considered. Indirect interconnectedness may distort aim-assigned operation of the systems causing serious disproportionality. Moreover, the potential threat that may fundamentally change the nature of the existing EU law enforcement large-scale IT systems is interoperability, that is, as of now, prohibited "unless so provided in a specific legal basis".[330] Having VIS and EURODAC relation concerning the determination of the country responsible for the examination of an asylum application and the examination of an asylum application, having also SIS II and VIS relation in connection with enforcing entry ban, and having the recently established VIS and EURODAC relation concerning conditions for access in case of law enforcement purposes, indirect interconnectedness of EU law enforcement large-scale IT systems is observed on the management level.

[330] Regulation (EU) No 1077/2011, *op. cit.*, Art. 1(4), p. 6.

Table 1. SWOT Analysis of the Existing EU Law Enforcement Large-Scale IT Systems

	Positive	Negative
Internal	**Strengths**	**Weaknesses**

	• long-term cost efficiency
	  ○ centralisation (resource pooling)
	• institutionalisation
	  ○ visibility and approachability for the civil society
		• costs and time of setting up the Agency and transition to new location
		• accommodation of *la géométrie variable*
		  ○ setting up complex governance and management structures

External	**Opportunity**	**Threat**

	• preparation, management and development of other large-scale IT systems	• possibility of function creep
		  ○ indirect interconnectedness
		  ○ technical possibility of direct interconnectedness
		  ○ legal possibility of interoperability

Establishing that what socially beneficial is based on the above examined criteria and aspects, the establishment of eu-LISA has economic advantages in the long run. The highlighted strengths and the opportunities constitute the added-value of the Agency, which are the followings: 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 tendency for connectedness. The establishment of eu-LISA 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 according to the examined aspects, criteria and processes, and regarding the presuppositions.

As it has been established above, transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement. The potential threat that may fundamentally change the nature of the existing EU law enforcement large-scale IT systems is interoperability. The tendency for interoperability is paved by indirect interconnectedness. Moreover, taking the management level of the layer model, it is also debatable that the whereabouts of the

transferred data are often not clarified, e.g. into which databases the data are introduced and which third parties get access to the data. It is not explained before the data transfer. It is again underlined that different accessing actors may lead to extension of authorities possibly using the transferred data. Time limits for storing the data in the original database may also be extended by the data transfer to other databases. Moreover, less unsatisfactory data transfer is observable not only on the management but also on the cooperation level.[331]

All in all, economies of scale and security orientation compromise the respect of human rights standards. Therefore, according to the proposed method local tool, institutional arrangements are not constellated optimally concerning social beneficiality.

However, the eu-LISA Regulation 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.[332] On the one hand, after the entry into force of the Treaty of Lisbon, the fundamental rights and freedoms shall be more carefully respected by the European institutions. On the other hand, accountability of the European Agencies is ensured by the European Parliament and the European Data Protection Supervisor. Furthermore, the European Court of Justice[333] and national courts have full jurisdiction over eu-LISA activities.

The so far outlined development process of existing law enforcement large-scale IT systems operating in the area of freedom, security and justice shows a reactive attitude, i.e. reactive to perceived security challenges. Their development process is decidedly inherent although relevant cooperation stated out of EC/EU treaty regime. It is also supported by the fact that the systems were created separately but they keep on entering into more enhanced interaction with each other and with their environment.

To sum up social preferences that are reflected through the systems of EU migration and internal security policies, a more security-oriented pattern is observable that is reactive to the perceived threats from the environment. Therefore, in a non-pillar Europe, a unified management approach has been accepted to handle a commonly perceived challenge. For that, information power is used more extensively slowly approaching the existing systems.

[331] Boehm, Franziska, *Information Sharing and Data Protection, op. cit.*, p. 369.
[332] Regulation (EU) No 1077/2011, *op. cit.,* Art. 21, 28, 29 and 26, pp. 13-14.
[333] *Ibid,* Art. 24, p. 13.

This process can be justified from the realist, sovereignty-based position. However, transparency and human rights shall not be compromised endlessly, since, as a greedy feature of intelligence, it is hard to establish how much surveillance is enough.

It is crucial to pay attention to the limitations of the above results. BIGO established three universes for "(in)securitization practices of EU border control".[334] The military/navy universe deals with solid borders where borderline is interpreted as a wall. For the internal security universe, borders are management activity of filtering and sorting, thereby, borders are liquid. The database analysts' universe is characterised by mobile borders and networked interoperable databases making borderlines smart and gaseous. Using his terminology, the current results shall be interpreted as observing gaseous borders with the mind-set of the internal security universe.

***

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 existing and planned Schengen an EU migration and asylum *acquis*.

[334] Bigo, Didier, The (in)securitization practices, *op. cit.*, pp. 209-225, quoted from the title.

III. Testing Projection Capacity: Challenging First Results

The preliminary aim of the current chapter is to challenge the first results derived from the observation of the existing law enforcement large-scale IT systems operating in the area of freedom, security and justice.

In line with the proposed methodological tool, these systems have been measured using the three established indicators that characterise social preferences reflected through these systems onto EU migration and internal security policies. Having these patterns, social beneficiality of the existing systems has been estimated by indirectly inferring from the statement, that transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement.

The main finding in relation to social beneficiality established on the observed social preferences is that economies of scale and security orientation of the existing EU law enforcement large-scale IT systems compromise the respect of human rights standards. So that, according to the proposed methodological tool, institutional arrangements are not constellated optimally concerning social beneficiality.

The received results derived from social preferences are double conjectured, so that they shall be challenged to be proven. Thus, it has been proposed that observing law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice, the projection capacity of the proposed methodological tool can be tested. Projection capacity in this context means the capacity of the above established indicators (accountability for acts, respect of human rights standards and transparent operation) to determine social beneficiality of the observed system. The test here equals with the comparison of social preferences reflected through the planned and the existing law enforcement large-scale IT systems operating in the area of freedom, security and justice.

Firstly, the comparability of the existing and planned systems shall be examined. Deriving from the characteristics of the existing ones, the mentioned systems are comparable if they tackle the same challenges of the area of freedom, security and justice. In this context, it means balancing security needs of *Schengenland* and facilitating people movement within, to and outwards the area by using information power. To handling the dichotomy, an analogy is needed as benchmark. For the purpose, EU return and readmission policy is adequate, since it handles security perspective as long as dealing with competing provisions of the right to leave and of the obligation to (re)admit to

facilitate (mainly forced) migration flows. Therefore, benchmarking for comparability is to be elaborated first.

Then, planned systems shall be selected for comparison. While it should be borne in mind that eu-LISA is capable of incorporating the operational management of further law enforcement large-scale IT systems regardless of current arrangements.[335]

If comparability is proven and all relevant EU law enforcement large-scale IT systems are selected, these systems' planned design, i.e. institutional arrangements are analysed aiming at establishing and ordering them around the three above indicators of accountability for acts, respect of human rights standards and transparent operation. Determining social preferences, social beneficiality of the concerned systems is ascertained based on the proposed methodological tool.

Today's social preferences are reflected in nowadays decided plans. It means that if the same social preference patterns come out of the analyses of existing and planned systems, the social beneficiality of the existing law enforcement large-scale IT systems can be determined based on and accepting the presumptions of the proposed methodological tool. Therefore, the last step is the comparison of results coming from the examination of the existing and the planned systems. In this way, indirect interference of indicators' projection capacity is challenged.

1. Benchmarking: EU Return and Readmission Policy

In the context of the European Union policies, it is highly true that programmes, action plans and communications are compasses of future legislation, since commonly perceived challenges seek unified approach to handle them. In this way, the most long-range document is the so-called Post-Stockholm Programme[336]. The Programme sees the policy area effective if the benefits of migration and integration is maximised while a credible approach to irregular migration and return is granted. It means that patterns for future continue to be organised around secured and facilitated migration flows for EU security.

The endeavour of facilitating migration flows has a clear (but not exclusive) connotation to foster legal migration of desired persons, i.e. those, who come to that part

[335] See: Ch. II.3.3.
[336] COM(2014) 154 final, *op. cit.*

of labour market, where there is a specific workforce shortage. At this time, migration is for security, since migration may result in a higher economic output that may counterbalance negative social security processes. Therefore, migration supports (social) security.

Migration and security are more coordinate in case of international protection seekers. Granting refuge is an indisputable obligation for all states. COMMISSIONER MALMSTRÖM underlined that practically there is no legal way for potential protection seekers to enter the territory of the EU. According to the 1951 Convention Relating to the Status of Refugees, claim may be lodged solely subsequent to the entry to the State concerned. It catalyses irregular crossings as well as human smugglers and traffickers became travel agents carrying protection seekers to the territory of the EU. It results in obvious security threats. Ms. MALMSTRÖM considered resettlement as an appropriate tool to facilitate this specific migration flow.[337]

Handling irregular migration, migration and security establish a clear dichotomy. From this aspect, EU return and readmission policy secures migration flows by sending back persons not having the right to enter to or stay in the territory of the EU (and of Schengen associated countries). Moreover, this policy area aims at facilitating return flows. In a comprehensive approach, EU return and readmission policy uses all EU law enforcement large-scale IT systems, since, for example, entry bans are stored in SIS, refused visa appliers may be matched using VIS, irregular migrants apprehended in connection with the irregular crossing of an external border get into EURODAC. Therefore, as benchmark for the planned EU law enforcement large-scale IT systems, EU return and readmission policy is selected.

Return migration including readmission seen as a tool for its facilitation is an important issue on the agenda because of its impact on all countries. Return migration has in the past decades emerged as a critical element of migration policies. By counterbalancing influx, return of migrants unable or unwilling to remain in a host State may support to maintain asylum systems and regular immigration programmes. Moreover, return may contribute to the sovereign right of the State to determine who should enter and remain on her territory and under what conditions.

[337] Malmström, Cecilia, *Europe and migrants – progress and setbacks,* The Tore Browaldh Lecture 2014, "Tore Browaldh Lecture Series", Gothenburg University, School of Business, Economics and Law, 3.11.2014, 16.15-18.00.

According to mainstream point of departure for the right to leave,[338] three international instruments are often cited; namely Article 13 of The Universal Declaration of Human Rights (1948) (hereinafter: UDHR), Article 12 of the International Covenant on Civil and Political Rights (1966) (hereinafter: ICCPR) and Article 5 of the International Convention on the Elimination of All Forms of Racial Discrimination (1965) (hereinafter: ICERD).[339]

The "own country" concept set out by UDHR, i.e. return to the country of nationality is to be seen as an absolute right, is controversial, since it is related to the admission of own nationals by their own will. By admitting own nationals, the state responds to an individual claim applying the human right to return to own country. Although Article 12(2) of the ICCPR[340] may be subject to restriction, since it does not differentiate neither among nationals and non-nationals and nor among documented or irregular status.

The right to leave derives from the will of the individual. However, it would be meaningless without a corresponding State obligation to readmit. As COLEMAN states, "this obligation is implied" by the existence of the right to leave.[341]

In case of readmission and forced return, the will of leaving is missing from the side of the individual. However, the right of the Sate to expel non-nationals is seen as a part of sovereignty, which can be used as limitations set out in international instruments.[342] States have interests in controlling border crossings for various (social, economic or political) reasons. At the same time, the failure of control can cause serious security challenges.[343]

---

[338] For an excellent synthesis see: Perruchoud, Richard, "State sovereignty and freedom of movement", in Opeskin, Brian and Perruchoud, Richard and Redpath-Cross, Jillyanne (ed.), *International Migration Law,* New York, Cambridge University Press, 2012, pp. 123-151.

[339] UNHR Article 13 (2) states that "Everyone has the right to leave any country, including his own, and to return to his country,"; ICCPR Article 12 (4) states that "No one shall arbitrarily be deprived of the right to enter his own country"; ICERD Article 5 (d) (ii) states that "States Parties undertake […] to guarantee the right to everyone […] to leave any country, including one's own, and to return to one's country."

[340] "Everyone shall be free to leave any country, including his own."

[341] Coleman, Nils, European Readmission Policy: Third Country Interests and Refugee Rights, "Immigration and Asylum Law and Policy in Europe", vol. 16, Leiden, Martinus Nijhoff Publishers, 2009, p. 29.

[342] Perruchoud, Richard, *op. cit.*, pp. 137-147.

[343] Adamson, Fiona B., "Crossing Borders: International Migration and National Security", *International Security*, 31(1), p. 176.

At least one state shall be responsible for each person, which is sought also by the international legal order. Thus, it is a State obligation to accept a readmitted national who is expelled from another country.[344]

The obligation to accept a voluntary or forced returnee is the question of nationality, since only the state is obliged to accept the returnee whose nationality the person concerned possesses.

The sole case mentioned in the mainstream literature when non-national "returnees" are considered to be obliged to be accepted is the concept of *bon voisinage* or (good) neighbourliness. COLEMAN[345] presents HAILBRONNER's views on *bon voisinage*[346] as follows. (Good) neighbourliness is the application of the same international environmental law principle which in this case makes the neighbouring country responsible for irregular migrants accusing the neighbouring country of not managing irregular migration flows efficiently enough. COLEMAN shares HAILBRONNER's point according to which the author sates that the lack of general practice and of *opinio juris* prevents *bon voisinage* to be accomplished as customary norm. However, it has a significant political nature becoming a bargaining chip lacking reciprocity in practice for which the requested Sates receive some form of compensation.[347]

As the above reasoning indicates, in theory, no State would explicitly oppose the rule obliging to (re)admit own nationals. Problems in practice emerge in a situation when an insufficiently documented or undocumented migrant is coupled with a less cooperative requested State, since in this case the ability to demonstrate nationality (i.e. identification process) defines the success of readmission. The burden of proof is shifted to the requesting State. If the requested State is not cooperative in identification, e.g. sharing birth registry data (in fact, there is no such registration in some countries), the fate of readmission is sealed. Moreover, it is accepted that irregular migrants cannot be combated if they cannot be removed or retuned.

The worst-case scenario occurs, when even if the irregular migrant is identified (and arrested), and the return decision is taken due process, the removal may not be certain. Practical difficulties may come in case of forced return. The requested State may

[344] Cf. Hailbronner, Kay, "Readmission Agreements and the Obligation on States under Public International Law to Readmit their Own and Foreign Nationls", *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht,* vol. 57, 1997, p. 20.
[345] Coleman, Nils, *op. cit.*, pp. 41-45.
[346] Hailbronner, Kay, *op. cit.*, pp. 1-49.
[347] Coleman, Nils, *op. cit.*, pp. 43-45.

argue the nationality of the migrant in question, and/or may refuse to issue travel a document to him/her that is indispensable for return (think of a transit in another country due to flight schedules when the consent of the transit State is needed). The requested State may either be unwilling or unable to cooperate.

What practice makes more complex, irregular migrants are detained except for some cases. If the requesting State fails to prove nationality or the requested State is unwilling or unable to cooperate, i.e. the removal is not carried out; the law-breaching migrant cannot be detained endlessly due to general human right provisions. From this point of view, a fairly and lawfully proceeded State shall tacitly tolerate the unlawful stay of an irregular migrant on her territory.

State sovereignty may be an obstacle when a State is requested to readmit an alleged national. However, "practical or procedural obstacles to readmission of nationals, imposed by any requested state, do not present an *opinion juris* or practice to the customary norm"[348] of admitting own nationals.

The aim of concluding readmission agreements is clearly to implement forced return of irregular migrants. The agreements set out reciprocal obligations on Contracting Parties, as well as administrative and operational procedures to facilitate return and transit of persons who do not, or no longer fulfil the conditions of entry to, presence in or residence in the requesting State including nationals of the other party or parties, third country nationals and stateless persons.

PERRUCHOUD properly evaluates readmission agreements in this context saying that despite of positive, facilitating nature of the agreements they face some challenges. Notably, less account is taken to the interests of counties of origin and transit and documents accepted as proof of nationality may fail to meet the benchmark generally accepted in international law.[349]

However, the large and growing number of such agreements may arguably be an indicator of the absence of a customary norm. Thus, these agreements may be interpreted as State tool to manage obstacles deriving from the practical challenges of readmission and return.

The cooperation in return and readmission matters between the EU and Third Countries may be based on EU Readmission Agreements setting out general and

[348] *Ibid*, p. 35.
[349] Perruchoud, Richard, *op. cit.*, p. 147

procedural mutual obligations concerning in which case and how to take back irregularly residing individuals on the territory of a Contracting Party.[350]

From a Member State's perspective, EU Readmission Agreements are of assistance if the return decision is made in accordance with the procedural guarantees established by the Return Directive[351] and the relevant EU asylum *acquis*[352]. COLEMAN argues[353] that the main motivation for an EU level readmission policy was to extract fostered cooperation from Third Countries in the policy area using the negotiation weight of the European Union.

The relation between EU and Member State Readmission Agreements can be characterised by the criterion of shared competence as derived from the Treaty on the Functioning of the European Union. Member States may conclude Readmission Agreements with Third Countries which have not signed such EU level agreements, otherwise, the European Commission could not be granted a mandate to negotiate EU Readmission Agreement. If a Member State concluded a Readmission Agreement with a given third country prior to the EU agreement, its applicability is limited to the provisions not regulated in the EU Readmission Agreement. In case contradictory or overlapping provisions are included in the agreements, the EU level one has the priority over a Member State agreement.[354] After an EU Readmission Agreement is concluded, Member States may conclude implementing protocols with the State concerned.

It is generally perceived in relation to Member States' attitude that readmission agreements are mostly considered as effective tools to facilitate returns and tackle irregular migration. It may be considered as the lack of general practice and of *opinio juris* preventing (good) neighbourliness to be accomplished as customary norm.

***

[350] Cf. a more detailed paper by Balázs, László, dr., "A visszafogadási egyezmények alkalmazásának tapasztalatai az Európai Unióban, illetve a hazai joggyakorlatban", *Migráció és Társadalom,* 1(2), 2012, pp. not indicated.
[351] Directive 2008/115/EC of the European Parliament and the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nations, OJ L 348, 24.12.2008, pp. 98-107.
[352] Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status, OJ L 326, 13.12.2005, pp.13-34.
[353] Coleman, Nils, *op. cit.*, pp. 55-57.
[354] *Ibid,* p. 108.

Readmission Agreements are complementary tools to the customary obligation to (re)admit own nationals, since the agreements affirm readmission obligations and facilitate return based on listed grounds in national law coupled with agreed means of evidence and established procedures. However, in practice, the success of return operations depends on well-meaning cooperation of the concerned States including the requesting, the requested and the transit State.

2. Selection

The main purpose of the current section is to select those planned EU law enforcement large-Scale IT systems that are suitable for comparison with the existing ones based on the benchmarking criteria.

The above comprehensive approach, again, takes the handling of security and facilitation dichotomy as core idea. EU return and readmission policy fits the purpose. Moreover, the policy area uses all EU law enforcement large-scale IT systems as tools, since, again, for example, entry bans are stored in SIS, refused visa appliers may be matched using VIS, irregular migrants apprehended in connection with the irregular crossing of an external border get into EURODAC. Therefore, as benchmark for the planned EU law enforcement large-scale IT systems, EU return and readmission policy is selected.

In the flow of European integration, three, in the beginning, separated policy areas have been elaborated for handling the challenges of the cross-border security deficit caused by the fall of Schengen internal borders. Also in these policy areas information power is used to facilitate migration flows. For managing the common internal security risks of *Schengenland*, slow approaching policy areas can be observed, namely, common border control policy, common visa policy and common asylum policy.

The common visa and the common asylum policy areas are aimed to be covered comprehensively by VIS and EURODAC. However, common border control policy area is not fully covered by SIS. This fragment gives opportunity to develop new and from the current research's point of view relevant EU law enforcement large-scale IT systems.

Having accepted the above mentioned and regarding EU level proposals submitted as of writing, the planned functioning of RTP, EES and as well as the patterns of PNRs shall be examined. All these planned systems intent to bridge the gap in border control

policy by aiming at contributing to a more effective border crossings registration. The proposed systems incorporate the dichotomy of secure and facilitate migration flows. In the meantime, they fit to the used limitations to law enforcement large-scale IT system, since they are designed to use information power of mass data gathering.

In case of RTP and EES, the comparability is supported with the capacity of eu-LISA to incorporate the development and the operational management of further law enforcement large-scale IT systems regardless of current arrangements.

As it has been demonstrated, PNRs fit for further analysis. However, it should not be forgotten that the use of PNRs is more regarded as criminal intelligence tool. Therefore, in the current theoretical framework, the analysis of PNRs shall be limited to their functioning related to border crossings registry tool. That is why patterns of PNRs are deliberately used as unit of analysis, since for example proposed PNR cooperation in general is inappropriate due to the current scope of research.

The European Border Surveillance System (hereinafter: Eurosur) gradually introduces a mechanism enabling authorities of the Member States carrying out border control to cooperate and share operational information with each other and FRONTEX in order to strengthen the external border control of the Schengen area, especially in its Southern and Eastern parts, as well as at its marital and land borders, and increase fight against irregular migration and cross-border crime.

FRONTEX coordinates the operational cooperation among the Member States concerning the management of external borders. It assists Member States in the training of national border guards. FRONTEX may be at the assistance of the Member States in organising joint return operations. Moreover, its mechanisms can be a tool to increase technical and operational assistance at certain external border sections. The amendment of the FRONTEX Regulation was necessary in order to ensure the proper and well-defined functioning of FRONTEX as the explanatory memorandum of the Commission had highlighted.[355]

The amended FRONTEX Regulation guarantees more effective use of information concerning the following two aspects. On the one hand, FRONTEX is now able to develop and operate information systems that enable swift and reliable exchanges

[355] COM(2010) 61 final Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), Brussels, 24.2.2010, p. 2.

of information regarding emerging risks at the external borders.[356] On the other hand, due to the modification, FRONTEX is responsible for providing

> "the necessary assistance to the development and operation of a European border surveillance system and, as appropriate, to the development of a common information sharing environment, including interoperability of systems."[357]

The latter is very important from the comparative point of view, since this provision guaranteed a link with the so-called Eurosur Regulation[358]. Within the framework of Eurosur, a secured computerised communication network has recently been set up to exchange data and facilitate the coordination of activities between the so-called National Coordination Centres and with FRONTEX enabling participating authorities to instantly see and assess the situation at and beyond the external borders.

The main aim of Eurosur, inter alia, is to reduce the number of irregular migrants entering the EU undetected. The modified FRONTEX Regulation and the Eurosur Regulation foster the more effective use of information power among the countries in the area of freedom, security and justice. The tendency of the progress is clear. More and more actions are implemented and planned; the information power fosters the aspiration for more enhanced cooperation among the countries of the Schengen area.

However, in case of Eurosur, it does not tackle the dichotomy of secure and facilitate, in this case, borders as it has been established as common a feature by the benchmark. Taking again three universes of BIGO for "(in)securitization practices of EU border control"[359], Eurosur concerns solely the military/navy universe deals with solid borders where borderline is interpreted as a wall. Eurosur deals with border security using the concept of information power. Although, it does not incorporate neither the liquid, managerial nor the gaseous, smart facilitation of migration flows, in this particular case, at the Schengen external borders. Therefore, Eurosur does not fit to comparison.

To sum up, using the above benchmark, for challenging the first results in line with the proposed methodological tool, the planned functioning of RTP, EES and as well as the patterns of PNRs is to be examined. Due to border crossings registration purposes,

---

[356] Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 304, 22.11.2011, Art. 1(3)(vi), p. 6.
[357] *Ibid.*
[358] Regulation (EU) No 1052/2013 of the European Parliament and the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ L 295, 6.11.2013, pp. 11-26.
[359] Bigo, Didier, The (in)securitization practices, *op. cit.*, pp. 209-225, quoted from the title.

they are appropriate for comparison based on the benchmarking tool, since these systems (at least partially cf. PNRs) are designed to be able to host secure and facilitate dichotomy using information power.

3. Planned EU Law Enforcement Large-Scale IT Systems

The aim of the current section is to present and evaluate those planned EU law enforcement large-scale IT systems that are proved to be comparable in the above chapter.

Therefore, the planned design of RTP and EES together with patterns of PNRs are sketched firstly focusing on the prime movers of and key rationale of their envisioned establishment. During the analysis, special attention should be paid to interactions of the systems with their environment.

According to the proposed methodological tool, it is conjectured that results elaborated in terms of accountability for acts, respect of human rights standards and transparent operation can characterise social preferences of EU internal security and migration policies in the current theoretical framework. So that, secondly, features of the mentioned planned EU law enforcement large-scale IT systems are arranged along the three indicators.

Based on the got outcome related to the indicators, it is also conjectured in line with the proposed methodological tool that analysing the above three indicators the relationship of the examined law enforcement large-scale IT systems with social beneficiality can be determined. Therefore, thirdly, social preferences and social beneficiality are established if accepting the presumptions.

3.1. Design

PNR data are unverified information submitted by passengers that are collected and kept by carriers (mainly in their departure control and reservation systems) for their own commercial purposes. PNR includes several pieces of information on the travel such as personal details, travel dates, itinerary, ticket information (including seat and baggage) and payment details. PNR data are used for law enforcement purposes worldwide. Moreover, the EU has bilateral agreements, based on which it transfers PNR data to

Canada and to Australia and to the United States.[360] Its advance analysis is of relevance for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Therefore, it is more regarded as criminal intelligence tool. National PNR systems have been started to be created EU-wide. Therefore, the Commission submitted the first EU PNR proposal[361] in 2007. However, it stuck in the decision-making. Due to the entry into force of the TFEU, the first proposal was revised and the so-called Proposal for an EU PNR[362] was submitted in 2011. According to the current theoretical framework, its border crossings registration relevant features are detailed constellating patterns of PNRs.

Proposal for an EU PNR aims at the collection of PNR data submitted by air carriers. It shall be used for law enforcement purposes solely in case of prevention, detection, investigation and prosecution of terrorist offences and serious crime. Data is collected with push method, i.e. carriers synchronise their database real-time. Owing to such method, previously unsuspected criminals may be investigated also in a pre-emptive manner.[363]

The Proposal for an EU PNR aims at setting Passenger Information Units in each Member State for the purpose of storing and analysing PNR data received from air carriers.[364] The units transmit the results of their analyses and related PNR data of passengers to the designated national authorities, called the competent authorities, that are relevant in relation to prevention, detection, investigation and prosecution of terrorist offences and serious crime.[365] Exchange of information shall take place via Passenger Information Units except for in case of prevention of an immediate and serious threat.[366]

---

[360] Cf. Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82, 21.3.2006, pp. 15-19; Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to Australian customs service, OJ L 213, 8.8.2008, pp. 49-57; Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, pp. 5-14.

[361] COM(2007) 654 final Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Brussels, 6.11.2007.

[362] COM(2011) 32 final Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 2.2.2011.

[363] Mitsilegas, Valsamis, "Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, and Strengthening the State", *Indiana Journal of Global Legal Studies,* 19(1), pp. 54-55.

[364] COM(2011) 32 final, *op. cit.,* Art. 3(1), p. 21.

[365] *Ibid,* Art. 5(4), p. 23.

[366] *Ibid,* Art. 7, pp. 24-25.

The smart borders initiative presents the newest endeavour for the development of new (and related) law enforcement large-scale IT systems in the area of freedom, security and justice. A 2008 Communication of the European Commission[367] has given an outline of European smart borders as a beacon to be followed.

In summer 2011, the Council emphasised the responsibility of the Member States for the control and surveillance of the external borders. The European Border Surveillance System (with a target date of 2013) will have been developed further in order to ensure the effective management of and the application of same standards at the external borders.[368]

New technologies shall be harnessed to meet all the requirements including enhancing security and facilitating travel at the external borders. Therefore, the Commission set out main options for the way forward in its smart borders initiative. According to the initiative, the EES and the RTP should be introduced in order to tackle the above highlighted problem effectively.

The Smart Borders Package[369] was submitted by the European Commission on 28 February, 2013. The package consists of the RTP Proposal[370] and the EES Proposal[371]. Due to these proposals, the Schengen Borders Code[372] (hereinafter: SBC) shall be amended. Therefore, the third proposal of the package is the SBC amending Proposal[373].

Borders are smart if the speed of exchange of electronic data is superior to the speed of physical movement of the individual.[374] During this saved-time period, all the necessary checks are done. For that, all relevant information shall be submitted in advance. However, individuals using smart borders shall accept pre-registering their own personal information to be able to benefit from quick access of high technology.

---

[367] COM(2008) 69 final Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Preparing the next steps in border management in the European Union, Brussels, 13.2.2008.

[368] EUCO 23/11 European Council 23/24 June 2011, Conclusions, Brussels, 24.6.2011, point 23.

[369] Smart Borders Package, *op. cit.*

[370] COM(2013) 97 final Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, Brussels, 28.2.2013.

[371] COM(2013) 95 final Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, Brussels, 28.2.2013.

[372] Regulation (EC) 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105, pp. 1-32.

[373] COM(2013) 96 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), Brussels, 28.2.2013.

[374] Cf. Bigo, Didier, The (in)securitization practices, *op. cit.,* pp. 217-218.

Mistaking speed for freedom as BIGO reminds, persons may be refused to enter not because of any committed act but due to the profile associated with their data double.[375]

The reasoning for an RTP turns the above argumentation upside down. RTP aims at facilitation of frequent travellers' border checks underlining that today's rules applied in the same way to all third country nationals. RTP aims at the facilitation of the fast border crossing of this desired group that mainly comes for commercial purposes. By submission of personal data, candidates for RTP are envisioned to be pre-screened. As a result of profiling them, they may be granted with facilitated access to the Schengen area.

In the light of the EES Proposal, RTP efforts to remain Europe an attractive destination is clearer. EES is planned to be a law enforcement tool for monitoring overstayers, i.e. persons who stay longer in the Schengen area as it is allowed. Achieving it, all third country nationals over the age of twelve shall verify their identity by biometrics (solely fingerprints in this case) at least upon entry. Automatically the authorised stay is calculated upon arrival. By exiting at an external border, the length of stay is checked. Not leaving before the end date of the permitted stay, third country national concerned are planned to be listed for competent law enforcement agencies.

Technically, registered travellers will have a token verifying their supplementary rights of facilitated border crossings. RTP data will be managed by the token-Central Repository composing of a Central Repository (having a Principal repository and a Back-up repository), a Uniform Interface in each Member State, Uniform Interface, and the Communication Infrastructure between the Central Repository and the Network Entry Points.[376] Eu-LISA will be entrusted with the development and operational management of RTP[377] also modifying eu-LISA arrangements by adding a specific Advisory Group.[378] No JHA Agency participation has been mentioned at the Advisory Group so far. The planned structure reminds us of VIS design. However, National Systems shall also be developed and managed by the Member States.[379] The same technical structure is mirrored to EES except for tokens.[380] Eu-LISA will also be entrusted with the development and operational management of EES.[381] However, no EES specific Advisory Group is proposed.

[375] *Ibid,* p. 219.
[376] COM(2013) 97 final, *op. cit.,* Art. 2, p. 18 and Art. 21, pp. 30-31.
[377] *Ibid,* Art. 2(3), p. 18 and Art. 38, p. 39.
[378] *Ibid,* Art. 61, p. 49.
[379] *Ibid,* Art. 39(1)a-b, pp. 39-40.
[380] Cf. COM(2013) 95 final, *op. cit.,* Art. 6, p. 18 and Art. 25(1)a-b, p. 26.
[381] *Ibid,* Art. 2(2), p. 15 and Art. 24, pp. 25-26.

As far as the environment of Smart Borders Package is concerned, it is not new that by entry of third country nationals posed entry bans stored in SIS shall be filtered. Moreover, both RTP and EES are indirectly interconnected with VIS. For RTP, the checking procedure is alike as in case of applying for multiple-entry visa. EES will not collect fingerprints of visa holders but the visa sticker number.[382] Their biometrics (fingerprints and also photographs) are stored in VIS over the age of twelve. Third country nationals exempt from visa obligation shall submit their fingerprints over the age of twelve that will be stored in EES.[383] In this way, fingerprints of all third country nationals over the age of twelve entering the Schengen area will be stored for law enforcement purposes. Moreover, registered travellers will be recorded in EES. Practically, the planned systems will be indirectly interconnected with each other and with existing EU law enforcement larger-scale IT systems.

The Smart Borders Package envisions time and financial savings that can be reached with Automated Border Control systems. However, not all Member States operate such systems. The SBC amending Proposal will counterbalance the efforts of minimising red tape by preserving the issuance of written records to third country nationals containing the date and place of entry and exit if it is requested by them.[384]

In the current context, EU PNR will encompass unverified entry and exit data of all travellers including EU nationals. EES aims at establishing a verified border crossings registration mechanism for all third country nationals. While RTP is planned to create facilitated border crossings for frequent third country national travellers. Therefore, RTP shall not be regarded as a typical law enforcement large-scale IT system. It is more like a supplementary service for law-abiding third country nationals. However, RTP helps filtering out and facilitating the preferred migration flow contributing to the security of *Schengenland*.

3.2. Applying the Methodological Tool

Below the proposed methodological tool is applied to the selected planned EU law enforcement large-scale IT systems.

[382] *Ibid,* Art. 11(1), p. 20.
[383] *Ibid,* Art. 12(1-2), p. 21.
[384] COM(2013) 96 final, *op. cit.,* Art. 1(3)c, p. 11.

As it has been established, RTP is not regarded as law enforcement large-scale IT system. Its pre-screening mechanism definitely serves security purposes. Moreover, RTP aims at the facilitation of desired migration flows. Therefore, it may fit to analysis as far as the benchmarking is concerned. However, it is not associated with law enforcement purposes. It could serve as such if data on non-admitted persons would be retained for profiling purposes. RTP indirectly and complementarily helps law enforcement implementation. Therefore, due to the restricted notion of law enforcement large-scale IT systems used during the current research, RTP is analysed below only in those cases if it is (indirectly) related to law enforcement purposes.

Patterns of PNRs analysis shall be also limited due to the established theoretical framework of EU law enforcement large-scale IT systems. Therefore, the Proposal for an EU PNR is analysed to the extent of border crossings registration features, since its criminal intelligence tool potential shall be disregarded due to the established benchmark.

It means that EES fully and EU PNR border crossings registration features are observed below together with RTP relevant arrangements to law enforcement purposes. In the followings, these data are arranged along the three indicators developed by the proposed methodological tool. It is started with the human rights perspective the accountability and transparency problems follow all the more because human rights standards several times serve as points of reference for accountability.

Respect of Human Rights Standards

The Proposal for an EU PNR and the EES Proposal are fundamentally different in their points of reference concerning the respect of human rights standards. EU PNR will use unverified data for profiling purposes. Its results are planned to be used pre-emptively. Conversely, EES data contains biometrics, i.e. fingerprints aiming at the sanctioning perpetrated overstayings.

By collecting PNR data, due to the pre-emptive analysis passengers may not be admitted to the territory based on profiling. Persons may be denied to entry for acts predicted to be committed by them. This clearly colludes with the presumption of innocence. However, PNR data shall be used aligned to the aims of prevention, detection, investigation and prosecution of terrorist offences and serious crime. So that the aim of the proposed directive could be justified by countermeasuring serious security threat if its necessity and proportionality are proven.

It is welcome that the Charter of Fundamental Rights of the European Union and its provisions on personal data, on right to privacy and on right to non-discrimination are explicitly mentioned in a recital.[385] All these articles establish guarantees to all human beings in relation the Union actions. It is to be underlined, since the Proposal for an EU PNR aims collecting data on all passengers entering and leaving the Schengen area, i.e. of EU-nationals, of third country nationals and of stateless persons.

As for profiling passengers, the Proposal several times underlines that the assessment criteria, related decisions and any processing of PNR data shall not be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.[386]

The general data retention period is planned to be thirty days in case of full PNR data.[387] Upon expiry, information making it possible to identify passengers shall be masked out and the remaining data shall be retained for five years for profiling data analysis purposes. Special authorisation is needed for re-establishing PNR data in full.[388] In this way, the aim-aligned operation may be ensured. However, the Council made it clear that full PNR data shall be available for two years.[389] The proposed prolongation questions the aim-aligned data processing, since according to the original Proposal for an EU PNR data is practically available in full for the prevention, detection, investigation and prosecution of terrorist offences and serious crime until deletion after special and case-by-case authorisation. Eliminating the original barrier to data processing in full, due process operation is disputable.

In relation to data protection, the planned directive underlines that

> "every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation, and the right to judicial redress"[390]

and that shall be provided by each Member State. Specific provisions are envisioned to be established by the Member States due to the principle of subsidiarity and

[385] COM(2011) 32 final, *op. cit.*, Recital 31, p. 18.
[386] *Ibid*, Art. 4(3), p. 22 and Art. 5(6), p. 23 and Art. 11(3), p. 27.
[387] *Ibid*, Art. 9(1), p. 26.
[388] *Ibid*, Art. 9(2), p. 26.
[389] 9179/12 "Press Release, 3162th Council meeting, Justice and Home Affairs", *Council of the European Union Press*, Luxembourg, 26-27.4.2012, p. 8.
[390] COM(2011) 32 final, *op. cit.*, Art. 11(1), p. 27.

proportionality. It is very much welcome that the Proposal for an EU PNR ensures comprehensively the right of information at the time of booking the flight.[391]

HAYES and VERMUELEN started their analysis on fundamental rights impact of the Smart Border Package also[392] with the case of *S. and Marper v. the United Kingdom*.[393] It is due to the planned biometrics (fingerprints) processing of EES. The writers underline that EES in its current state presumes that third country nationals enter the Schengen area for residing there irregularly. Moreover, they miss the compliance with the asylum *acquis*, since a submitted asylum application may extend the right of residence overruling the original entry conditions.[394] EES could not be the sole basis of return decisions. However, it bridges a practical problem of return and readmission policy with merciless pragmatism. As it has been discussed above, in case of a non-cooperating requested State the burden of proof concerning identification is shifted to the requesting State in return and readmission matters.[395] The EES Proposal aims at granting opportunity to Member States to communicate data of third country nationals to third countries and international organisations (and private parties) including for the purpose of return.[396] The data that are planned to be submitted are suitable for identification purposes.[397] On the one hand, human rights guarantees are built in such as individual assessment, aim-alignment of data usage, not compromising the rights of refugees and persons requesting international protection including *non-refoulement*.[398] On the other hand, it strengthens the perception related to irregular entry aim of third country nationals.

As for general principles of EES, the system could be used solely if it is appropriate, necessary and proportional to the tasks of the competent authority.[399] For assessing this abstract formulation, HAYES and VERMUELEN cites[400] the *Huber v Bundesrepublik Deutschland* case, where in an essentially similar situation the Court of Justice of the European Union ruled that

---

[391] Cf. *ibid*, Art. 11(5), pp. 27-28.
[392] Cf. Ch. II.4.1.
[393] Hayes, Ben, Dr. and Vermeulen, Mathias, Borderline: The EU's New Border Surveillance Initiatives, "Assessing the Costs and Fundamental Rights Implications of EUROSUR and the 'Smart Borders' Proposal", Heinrich Böll Foundation, 2012, http://www.boell.de/downloads/DRV_120523_BORDERLINE_-_Border_Surveillance.pdf, [2.3.2013.], pp. 40-41.
[394] *Ibid*, pp. 47-48.
[395] Cf. Ch. III.1.
[396] COM(2013) 95 final, *op. cit.*, Art. 27, pp. 27-28.
[397] See also: *ibid*, Art. 19, p. 24.
[398] Cf. *ibid*, in particular Art. 27(2), p. 27 and Art. 27(2)a, p. 27 and Art. 27(3), p. 28.
[399] COM(2013) 95 final, *op. cit.*, Art. 8(1), p. 19.
[400] Hayes, Ben, Dr. and Vermeulen, Mathias, Borderline, *op. cit.*, p. 41.

> "such a register must not contain any information other than what is necessary for that purpose."[401]

It means that the EES Proposal is not sufficiently detailed meeting the above standard.[402] Also together with the welcome explicit reference to non-discrimination of third country nationals on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation and to fully respecting human dignity and integrity of the person,[403] these provisions do not counterbalance the above mentioned requirement.

The planned retention period for data storage is in line with the aim of sanctioning overstaying short stays. The information on who is on EU territory and who complies with the maximum allowed short stay of 90 days within any 180-day period, on nationalities and groups (visa exempt/required) of travellers overstaying and to support random checks within the territory to detect irregularly staying persons is to be available. In case of lack of exit record, the maximum storage of data will be five years.[404] EES data will be available for law enforcement agencies not only for verifying the conditions for entry and stay but also for verifying the identify of third country nationals if access would be given by competent EES national authorities.[405] It underlines the stigmatisation of all third country nationals suspecting them committing crime, especially entering for the reason of irregular stay.

As related to rights on data protection, the EES proposal uses the same techniques as the exiting EU law enforcement large-scale IT systems use. Persons shall be informed in writing about the collected data, the controller, length and purpose of retention, recipients and how to access, correct or delete stored data.[406] Inaccurate data shall be corrected, while unlawfully recorded ones shall be deleted.[407] If the Member State would not agree with inaccurate or unlawful data recording, it shall be explained in writing together with information on how to proceed further by bringing action of lodging a

---

[401] *Huber v Bundesrepublik Deutschland,* Case C-524/06, reference for a preliminary ruling, judgement of 16 December 2008, para 59. Cf. *ibid.*
[402] Hayes, Ben, Dr. and Vermeulen, Mathias, Borderline, *op. cit.,* p. 41.For a recent related analysis see also: Hendow, Maegan and Cibea, Alina and Kraler, Albert, "Using technology to draw borders: fundamental rights for the Smart Borders initiative", *Journal of Information, Communication and Ethics in Society,* 13(1), 2015, pp. 39-57.
[403] COM(2013) 95 final, *op. cit.*, Art. 8(2), p. 19.
[404] *Ibid,* Art. 20, p. 24.
[405] *Ibid,* Art. 18, pp. 23-24.
[406] *Ibid,* Art. 33, p. 30.
[407] *Ibid,* Art. 34, pp. 30-31.

claim.[408] It means that opinion of the Member State may be challenged.[409] Supervisory authority shall be available during the whole process.[410] Liabilities are governed by national laws.[411]

Concerning respect of human rights standards, the planned EU law enforcement large-scale IT systems follow the same patterns as the existing ones. In case of EES, moreover, path dependency is observable due to its planned incorporation into eu-LISA where all the existing systems are hosted.

Accountability for Acts

Again, it is worth underlining that accountability as from the point of the individual is detailed in the above human rights subsection, since, inter alia, due process and right to remedy are part of human right standards according to views of the author. In this part, accountability is related to institutions and to institutional arrangements. Therefore, it is worth to remind the distinguished features of EU rules in relation to individual data that prohibit the commodity-like use of personal data.[412]

By virtue of the Proposal for an EU PNR being a directive, accountability standards will be more precisely characterised in further national legislations. Therefore, national supervisory authorities of PNR will be established or designated to carry out national supervision related to national PNR operations.[413] The Member State cooperation mechanism in supervision is missing. It can be deduced from the supremacy of EU law. Moreover, it is true that no EU level actions are planned to be established. However, due to potential PNR data exchanges among the Member States, an explicit reference to cooperation obligation of Member States in supervisory tasks would be desired.

It is very much welcome that the Proposal for an EU PNR establishes not only feasibility and necessity review mechanism carried out by the Commission submitting it to the European Parliament and to the Council but also another review shall deal with operation done *mutatis mutandis*.[414] The latter shall dedicate

[408] *Ibid,* Art. 34(5), p. 31.
[409] *Ibid,* Art. 36(1), p. 32.
[410] *Ibid,* Art. 35, p. 31 and Art. 36(2), p. 32.
[411] *Ibid,* Art. 29(3), p. 29.
[412] Cf. Ch. II.4.1.
[413] COM(2011) 32 final, *op. cit.*, Art. 12, p. 28.
[414] *Ibid,* Art. 17, p. 30.

> "special attention to the compliance with standard of protection of personal data, the length of the data retention period and the quality of the assessments."[415]

Data security provisions are explicitly written in the EES Proposal.[416] EES supervision will be based on cooperation between the European Data Protection Supervisor and the national data protection authorities whereby the latter will remain responsible for the National System.[417] The EDPS will check the personal data processing activity of eu-LISA as being responsible for the operational management of, inter alia, the Central System and Network Entry Points.[418] National data protection authorities and EDPS shall meet at least twice a year to improve their cooperation, it means studying common problems, drawing up harmonised proposals for joint solutions and assisting each other in carrying out audits and inspections. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the eu-LISA in every two years.[419] It is welcome that it is explicitly stated that Member States must further ensure that national supervisory authorities are sufficiently equipped with resources to fulfil their tasks. Moreover, national data protection authorities shall carry out an audit of the data processing operations of the National System at least every four years.[420] In EES related tasks, eu-LISA shall give requested information to EDPS, grant access for EDPS to all documents and to its records, and allow him access to all its premises.[421]

The above EES arrangements support the reasoning of BOEHM in relation to her observations of potential harmonised data protection principles within the area of freedom, security and justice. [422] The above provisions are applied *mutatis mutandis* compared to the ones that govern existing EU law enforcement large-scale IT systems. In light of EES incorporation into eu-LISA, this phenomenon is considered as path dependency deriving from the closed approaching process of the existing systems that is embodied by the establishment of eu-LISA. EES planned provisions on self-monitoring and penalties[423] strengthen the views of MS. BOEHM[424] and path dependency.

---

[415] *Ibid,* Art. 17(2), p. 30.
[416] COM(2013) 95 final, *op. cit.,* Art. 28, pp. 28-29.
[417] *Ibid,* Art. 37-39, pp. 32-33.
[418] *Ibid,* Art. 38, p. 32-33.
[419] *Ibid,* Art. 39, p. 33.
[420] *Ibid,* Art. 37(2-3), p. 32.
[421] *Ibid,* Art. 38(3), p. 33.
[422] See: Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* here in particular the section on cooperation between data protection authorities is relevant, p. 418.
[423] COM(2013) 95 final, *op. cit.,* Art. 31-32, p. 30.
[424] Cf. Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* 9. Penalties in Case of Misuse, p. 418.

It is welcome that the EES Proposal establishes technical functioning and overall evaluation mechanism.[425] However, the first one addresses explicitly, inter alia, data retention period as whether it should be modified and access to authorities of third countries shall be granted.[426] The latter reference undoubtedly enhances stigmatisation.

Eu-LISA as planned developer and operational manager of EES will be liable to its acts without prejudice of the governed liability of EES. Accountability of eu-LISA in relation to operational management of EU law enforcement systems is analysed above together with observations on accountability of the existing systems.[427]

Transparent Operation

As it has been detailed in the previous chapters, *la géométrie variable* (variable geometry) deriving from the treaty arrangements may be causing function creeps in relation to the operation of EU law enforcement large-scale IT systems. In the current subsection, this phenomenon is interpreted together with extending the logics of the also above layer model to the observed planned systems.

As the legal bases of EU PNR and EES are articles of Title V of the TFEU, these systems are affected by *la géométrie variable* deriving from the protocols on the positions of the United Kingdom, Ireland and Denmark, since these protocols are included in the Treaty of Lisbon with some minor amendments.[428] The United Kingdom and Ireland may join PNR upon their wish, since it concerns juridical cooperation in criminal matters and police cooperation.[429] However, these States will not participate in EES, since EES is related to SBC in which they do not take part. Denmark in both cases will determine her participation. PNR and EES will be applicable for Bulgaria, Croatia, Cyprus and Romania. PNR, as has been addressed, concerns juridical cooperation in criminal matters and police cooperation so that their participation is clear. EES aims at the replacement of respective obligation to verify the length of stay and of stamping the passport of third country nationals that were to be applied by acceding Member States upon accession to the EU.

[425] COM(2013) 95 final, *op. cit.*, Art. 46(3-4), p. 35.
[426] *Ibid*, Art. 46(5), p. 35.
[427] See: Ch. II.4.1.
[428] See: Ch. II.1.3.
[429] Cf. COM(2011) 32 final, *op. cit.*, Recital 33, p. 19.

For the analysis of transparent operation arising from institutional arrangements, the layer model[430] has been developed. The distinguished management and cooperation levels concern the criteria of transparency. However, in case of the analysed planned systems cooperation level connections are not observed. Therefore, the management level of the layer model is extendedly applied to EU PNR and EES below. In this case, RTP is taken into account as well. In general, the explanatory power of RTP is limited, since RTP is indirectly and complementarily related to law enforcement purposes. However, analysing indirect interconnectedness RTP is relevant to the core question of the research.

The management level encompasses, inter alia, "across system" relations. SIS has a clear ground of indirectly interconnecting not only with VIS but also with RTP[431] in case of issued SIS alerts for the purpose of refusing entry. EU PNR and EES interconnectedness with SIS are less oblivious and more indirect. Upon arrival to an external border, SIS shall be checked so that EES or the checking method implementing (also) EES technically shall connect SIS entry ban alerts. 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. Its core is to pose entry and stay ban signals on persons listed by the Sanctions Committee and the Council. Previously entry and stay ban signal in this case was applicable solely by national decision. Furthermore, a copy of a European Arrest Warrant is enclosed to signals for arrest and surrender persons or persons wanted for extradition.[432] These data will be obviously of assistance in relation to EU PNR aiming at prevention, detection, investigation and prosecution of terrorist offences and serious crime.

Moreover, both RTP and EES are indirectly interconnected with VIS.[433] As far as RTP is concerned, the planned checking procedure is alike as in case of applying for multiple-entry visa presenting very low level of interconnectedness. EES will not collect fingerprints of visa holders but the visa sticker number.[434] Their biometrics (fingerprints and also photographs) are stored in VIS over the age of twelve. Third country nationals exempt from visa obligation shall submit their fingerprints over the age of twelve that will be stored in EES.[435] In this way, fingerprints of all third country nationals over the

[430] See: Ch. II.3.4.
[431] COM(2013) 97 final, *op. cit.,* Art. 15(1)g, p. 27.
[432] See also: Ch. II.2.1..
[433] See also about EES relationship with VIS and SIS II: Hayes, Ben, Dr. and Vermeulen, Mathias, Borderline, *op. cit.,* pp. 30-32.
[434] COM(2013) 95 final, *op. cit.,*, Art. 11(1), p. 20.
[435] *Ibid,* Art. 12(1-2), p. 21.

age of twelve entering the Schengen area will be stored for law enforcement purposes. EES is also planned to be accessible for examining and deciding on visa applications.[436]

Moreover, EES will be used for examining application for access to RTP as well.[437] It is implicitly confirmed by the RTP Proposal.[438] In case of RTP, alerts of Member States' national databases will be also an established ground for refusal.[439]

Deducing from the above mentioned, practically, the planned systems will be indirectly interconnected with each other and with existing EU law enforcement large-scale IT systems.

The accommodation of *la géométrie variable* together with indirect interconnectedness are concerns related to transparent operation. Indirect interconnectedness may distort aim-assigned operation of the systems causing serious disproportionality due to the multiple accessing actors. It can be supported by the fact that the same authorities (however, probably not the same units) may be designated to access the systems, since it is the responsibility of the Member State to set her own public administration up. Joint institutional arrangements of designated authorities result in indirect interconnectedness that may be mitigated by intra-institutional rules of procedures. In case of the observed planned systems, the above results related to indirect interconnectedness may be justified by their complementary nature. Moreover, the potential threat that may fundamentally change the nature of the EU law enforcement large-scale IT systems is interoperability that is, as of now, prohibited "unless so provided in a specific legal basis" if the system is hosted by eu-LISA. [440]

3.3. Social Preferences and Social Beneficiality of the Planned EU Law Enforcement Large-Scale IT Systems

The aim of the current subsection is to summarise the social preferences of EU internal security and migration policies that are observed through the planned and comparable law enforcement large-scale IT systems operating in the area of freedom, security and justice.

[436] *Ibid,* Art. 16, p. 23.
[437] *Ibid,* Art. 17, p. 23.
[438] COM(2013) 97 final, *op. cit.,* Art. 15(1)d, p. 27.
[439] *Ibid,* Art. 15(1)h, pp. 27-28.
[440] Regulation (EU) No 1077/2011, *op. cit.,* Art. 1(4), p. 6.

Comparable planned systems are EES, RTP restrictively to transparency due to its indirect and complementary relation to law enforcement purpose and patterns of PNRs, which are limited due to the established theoretical framework of EU law enforcement large-scale IT systems. Therefore, the Proposal for an EU PNR is concerned to the extent of border crossings registration features, since its criminal intelligence tool potential shall be disregarded due to the established benchmark.

According to the proposed methodological tool, it is conjectured that results reflected through the three above indicators can answer the question by characterising social preferences of EU internal security and migration policies in the current theoretical framework. Determining social preferences, social beneficiality of the concerned systems is ascertained.

Results of the indicators cannot be interpreted in absolute terms, i.e. it is rather a philosophical question to establish levels for how good their functioning is. Therefore, the relative relationship of the indicator results is proposed to be measured.

As far as the respect of human rights is concerned, the Proposal for an EU PNR and the EES Proposal are fundamentally different, since EU PNR will use unverified data for profiling purposes. Its results are planned to be used pre-emptively. In contract, EES data contains biometrics, i.e. fingerprints aiming at sanctioning perpetrated overstayings. Based on profiling results of PNR data, persons may be denied for acts predicted to be committed by them. This clearly colludes with the presumption of innocence. However, PNR data shall be used aligned to the aims of prevention, detection, investigation and prosecution of terrorist offences and serious crime. So that the aim of the proposed directive could be justified by countermeasuring serious security threat if its necessity and proportionality are proven. EES in its current state presumes that third country nationals enter the Schengen area for residing there irregularly. As for general principles of EES, the system could be used solely if it is appropriate, necessary and proportional to the tasks of the competent authority. However, it is proven to be not sufficiently detailed meeting the due process standard.

By virtue of the Proposal for an EU PNR being a directive, accountability standards will be more precisely characterised in further national legislations. The EES Proposal guarantees accountability on an appropriate level.

The accommodation of *la géométrie variable* together with indirect interconnectedness are concerns related to transparent operation. Indirect interconnectedness may distort aim-assigned operation of the systems causing serious

disproportionality due to the multiple accessing actors. In case of the observed planned systems, the above results related to indirect interconnectedness may be justified by their complementary nature.

To sum up social preferences that are reflected through the planned systems to EU migration and internal security policies, the pattern is clear. The perceived security challenges may compromise human rights that are handled by a comprehensive use of information power. EU PNR will emerge virtual bastions all around external borders. However, it may be explained by counterbalancing serious crimes. The proposed EES will stigmatise third country nationals giving a comprehensive tool to law enforcement agencies to sanction and in that way manage the outflow of irregular migration. It cannot be justified unless all third country nationals are perceived as potential threats. Therefore, the doors of Schengen are closing in the name of a more secured and opened Europe. However, it is not a dichotomy, since the envisioned tools aim at the managerial selection of incoming persons by establishing who are desired. Nevertheless, this utilitarian approach costs in terms of applied human rights standards.

It means that the managerial attitude of selecting desired persons from migration flows and security orientation compromise the respect of human rights standards. So that, according to the proposed method local tool, the proposed institutional arrangements are not constellated optimally concerning social beneficiality.

4. Establishing Projection Capacity

The proven comparability between the planned and the existing EU law enforcement large-scale IT systems makes it possible to challenge the determined social beneficiality of the existing systems aiming at establishing the potential projection capacity of the proposed methodological tool.

Its projection capacity means the capacity of the above established indicators (accountability for acts, respect of human rights standards and transparent operation) if being projected to determine social beneficiality of the observed system.

As point of reference, it is accepted that today's social preferences are reflected in nowadays decided plans. It means that if the same social preference patterns come out of the analyses of existing and of planned systems, the social beneficiality can be determined of the existing law enforcement large-scale IT systems based on and accepting the

presumptions of the proposed methodological tool. Therefore, the aim of this chapter is to compare the results coming from the examination of the existing and the planned systems. In this way, indirect interference of indicators' projection capacity is challenged.

Concerning respect of human rights indicator, based on profiling results of PNR data, persons may be denied to enter for acts predicted to be committed by them. It matches the universes established by BIGO.[441] EES is in line with the process started by VIS. However, the collection of data on all third country nationals that may be used for law enforcement proposes stigmatises by presuming irregular stay.

Accountability for acts criterion as long as EES arrangements are examined supports the reasoning of BOEHM in relation to her observations of potential harmonised data protection principles within the area of freedom, security and justice. [442] It means that the same pattern is observed in case of the planned and the existing systems.

The accommodation of *la géométrie variable* is more a TFEU Title V feature of the planned and existing systems in relation to transparency indicator. However, the found indirect interconnectedness may distort aim-assigned operation of the systems causing serious disproportionality due to the multiple accessing actors. In case of the observed planned systems, the above results related to indirect interconnectedness may be justified by their complementary nature. In case of the planned systems, cooperation level access is not observed directly.

Comparing social preferences that are reflected through the planned and the existing systems to EU migration and internal security policies assembling social beneficiality, in both cases it has been proven that the perceived security challenges that are handled by a comprehensive use of information power may compromise human rights. The security-oriented patterns are reactive to the perceived threats from the environment. The planned systems more comprehensively aim at the use of information power causing lowering potential of meeting high human rights standards. However, the planned systems are more complementarily interconnected indirectly with other systems.

The analysis of the planned systems derives from Commission proposals that are in practice based on the mapped perceptions of the Member States and relevant stakeholders. It may be challenged by taking into account that expected aims may be

[441] Bigo, Didier, The (in)securitization practices, *op. cit.*, pp. 209-225.
[442] See: Boehm, Franziska, *Information Sharing and Data Protection, op. cit.,* here in particular the section on cooperation between data protection authorities is relevant, p. 418.

reached using Automated Border Control systems that are just plans in several Member States.

Besides, it shall not be mistaken that the not optimal operation concerning social beneficiality is not the equal to optimal operation (in general). According to the proposed methodological tool, optimal operation in relation to social beneficiality depends on the aim of the legislator. In this case, optimum means meeting the three proposed indicators sufficiently.

In both cases of planned and existing systems, the human rights related indicator underperformed compared to the established standards. In the meantime, transparent operation has been found to be balanced with accountability. Therefore, in the current theoretical framework, the planned and the existing systems are found not to operate optimal concerning social beneficiality. As undelaying factor, reactive security-oriented patterns have been disclosed that are to be counterbalanced by a comprehensive use of information power compromising (high) human rights standards.

Accepting the above limitations, projection capacity of the proposed methodological tool is proven due to the revealed same patterns. In this way, observing law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice, the projection capacity of the proposed methodological tool is tested.

Accepting the limitations, the tool is suited to establish social preferences in different time and/or in different circumstances. Due to its standardised nature, comparing the results changes, i.e. dynamics could be demonstrated.

***

The presented systems are results of an intrinsic process whereby new connections are established for strengthening the whole structure. The distribution of information power and its comprehensive use build a new generation borderline around the area of freedom, security and justice.

IV. Conclusion: A Tool Measuring Social Preferences Reflected through Law Enforcement Large-Scale IT Systems

The developments and results are synthesised in this section. The main question of the research is to understand internal security and migration policies of the European Union through observing eu-LISA as the sole European Agency being a law enforcement large-scale IT system. Observing what kind of social preferences are reflected through the Agency, the EU internal security and migration policies can be more sophisticatedly characterised. The primary question is stretched by analysing all relevant law enforcement large-scale IT systems, i.e. those of which are operating in the area of freedom, security and justice.

For the analysis, a methodological tool is developed proposing the relative measurement of three indicators such as accountability for acts, respect of human rights standards and transparent operation. Indicators are examined through the development process of units of analysis (institutionalist approach) and through analysing the interactions among them and their environment (functionalist approach).

It is proven that the establishment of the systems was part of an inherent development by analysing the process; firstly, their relationship with EU treaties was observed in order to understand their today's multi-level governance more deeply. Then the exploration of the systems including eu-LISA follows in order to interpret the interactions among them and their environment.

As it is expected, the combination of institutionalist description of eu-LISA with analysis of interactions among the Agency, the systems and their environment (cf. functionalist mindset) finetune the preliminary results and face theory (i.e. legal provisions and legislative purpose) with reality.

The legal instruments originally establishing SIS and EURODAC were international legal acts that were communitarised. As the Member States recognised the importance of the common border control, common visa and common asylum policy in the fight against terrorism and cross-border crime, the treaties integrated these endeavours. The history of the European integration contains several examples for well-balanced political compromises. Thus, the opt-outs related to Schengen *acquis* could be

introduced in the treaties. The TFEU and the Charter of Fundamental Rights of the European Union mean a great progress in the history of third pillar integration, since basically the legislation of JHA acts moved to ordinary decision-making process which means a higher level of democratic control, in parallel, the Charter of Fundamental Rights of the European Union protects people against any infringements of their fundamental rights.

The established SIS, VIS and EURODAC are supporting the realisation of Community/Union policies in connection with 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 the systematic data gathering and the exchange of information (mainly) concerning third country nationals happen through them.

The SIS 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 to obtain information regarding certain categories of persons, vehicles and objects.

The VIS is a system for the exchange of visa data among its Member States. The VIS Regulation 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 EURODAC is a database that stores and compares the fingerprints of asylum applicants and irregular migrants apprehended in connection with irregular crossing of an external border. It was established to allow Member States to determine the state responsible for examining an asylum application.

The development of the operational management of these systems is not more than their integration into the eu-LISA. The installation of this Agency was legally predetermined by the existing and proposed legal instruments of SIS, VIS and EURODAC.

As it is established, transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement. The potential threat that may fundamentally change the nature of the existing EU law enforcement

large-scale IT systems is interoperability. The tendency for interoperability is paved by indirect interconnectedness. Moreover, taking the management level of the layer model, it is also debatable that the whereabouts of the transferred data are often not clarified, e.g. into which databases the data are introduced and which third parties get access to the data.

Respect of human rights standards has been interpreted alone, inside the systems. Accountability for acts indicator has incorporated internal and external factors. Transparent operation has been focused to the environment of the systems. Results of the indicators cannot be interpreted in absolute terms, i.e. it is rather a philosophical question to establish levels for how good their functioning is. Therefore, the relative relationship of the indicator results is proposed to be measured. For this, a simple but appropriate tool was chosen. Patterns of all existing systems drawn up by the indicators were summed up via a SWOT analysis.

In line with the proposed methodological tool, the measurement of the indicators characterised social preferences reflected through these systems. Having their patterns, the social beneficiality of these systems is estimated indirectly inferring from the statement, that transparency shall balance accountability without prejudice of human rights, which may constellate an optimal institutional arrangement.

The outlined development process of existing law enforcement large-scale IT systems operating in the area of freedom, security and justice shows a reactive attitude, i.e. reactive to perceived security challenges. Their development process is decidedly inherent although relevant cooperation started out of EC/EU treaty regime. It is also supported by the fact that the systems were created separately but they keep on entering into more enhanced interaction with each other and with their environment.

To sum up social preferences that are reflected through the systems of EU migration and internal security policies, a more security-oriented pattern is observable, which is reactive to the perceived threats from the environment. Therefore, in a non-pillar Europe, a unified management approach has been accepted to handle a commonly perceived challenge. For that, information power is used more extensively slowly approaching the existing systems.

Economies of scale and security orientation compromise the respect of human rights standards. So that, according to the proposed methodological tool, institutional arrangements are not constellated optimally concerning social beneficiality.

This process can be justified from the realist, sovereignty-based position. However, transparency and human rights shall not be compromised endlessly, since, as a greedy feature of intelligence, it is hard to establish how much surveillance is enough.

The obtained results of social beneficiality deriving from social preferences are double conjectured, so they shall be challenged to be proven. Therefore, the proposed methodological tool is applied to law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice. It also tests the projection capacity of the tool. Projection capacity in this context means the capacity of the above established indicators (accountability for acts, respect of human rights standards and transparent operation) if being projected to determine social beneficiality of the observed system. The test here equals to the comparison of social preferences reflected through planned and the existing law enforcement large-scale IT systems operating in the area of freedom, security and justice.

Before the application of the tool, comparability of the existing and planned systems was examined. Deriving from the characteristics of the existing ones, systems are comparable if they are tackling the same challenges of the area of freedom, security and justice. In this context, it means balancing security needs of *Schengenland* and facilitating people movement within, to and outwards the area by using information power. To handle the dichotomy, an analogy is needed as benchmark. For the purpose, EU return and readmission policy is proven to be adequate, since it handles security perspective as long as it deals with competing provisions of right to leave and of obligation to (re)admit to facilitate (mainly forced) migration flows.

Applying the above benchmark, comparable planned systems are EES, RTP restrictively to transparency due to its indirect and complementary relation to law enforcement purpose and patterns of PNRs, which are limited due to the established theoretical framework of EU law enforcement large-scale IT systems. Therefore, the Proposal for an EU PNR is concerned to the extent of border crossings registration features, since its criminal intelligence tool potential shall be disregarded due to the established benchmark.

According to the proposed methodological tool, it is conjectured that results reflected through the three above indicators can answer the question by characterising social preferences of EU internal security and migration policies in the current theoretical framework. Determining social preferences, social beneficiality of the concerned systems is ascertained.

To sum up social preferences of the planned systems that are reflected through the systems to EU migration and internal security policies, the pattern is clear. The perceived security challenges may compromise human rights that are handled by a comprehensive use of information power. EU PNR will emerge virtual bastions all around external borders. However, it may be explained by counterbalancing serious crimes. The proposed EES will stigmatise third country nationals giving a comprehensive tool to law enforcement agencies to sanction and in that way manage the outflow of irregular migration. It means that the managerial attitude of selecting desired persons from migration flows and security orientation compromise the respect of human rights standards. So that, according to the proposed methodological tool, the proposed institutional arrangements are not constellated optimally concerning social beneficiality.

In both cases of planned and existing systems, the human rights related indicator underperformed compared to the established standards. In the meantime, transparent operation has been found to be balanced with accountability. Therefore, in the current theoretical framework, the planned and the existing systems are found not to operate optimally concerning social beneficiality. As underlying factor, reactive security-oriented patterns have been disclosed that are to be counterbalanced by a comprehensive use of information power compromising (high) human rights standards.

Accepting the above limitations, projection capacity of the proposed methodological tool is proven due to the revealed same patterns. In this way, observing law enforcement large-scale IT systems planned to operate in the area of freedom, security and justice, the projection capacity of the proposed methodological tool is tested.

Accepting the limitations, the tool is suited to establish social preferences in different time and/or in different circumstances. Due to its standardised nature, comparing the results changes, i.e. dynamics could be demonstrated.

Concerning the establishment of eu-LISA, the attitude of the Member States is clear. Intelligence always has been a grey byway in democratic systems. Decision-makers are interested in a deeper cooperation to increase the efficiency and the amount of the stored data and access quality. If an over-regulated process occurs, not only the rights of criminals are infringed. Technological and scientific developments make intense control possible. The control tries to tackle public security problems. However, this solution raises many legal and ethical conflicts as well. Conversely, decision-makers shall harmonise their endeavours with the checks and balances of the rule of law. This double requirement defines the perceptions of the political players and of the state administration,

which builds up the *surveillant assemblage* nature of the operational management of law enforcement large-scale IT systems.

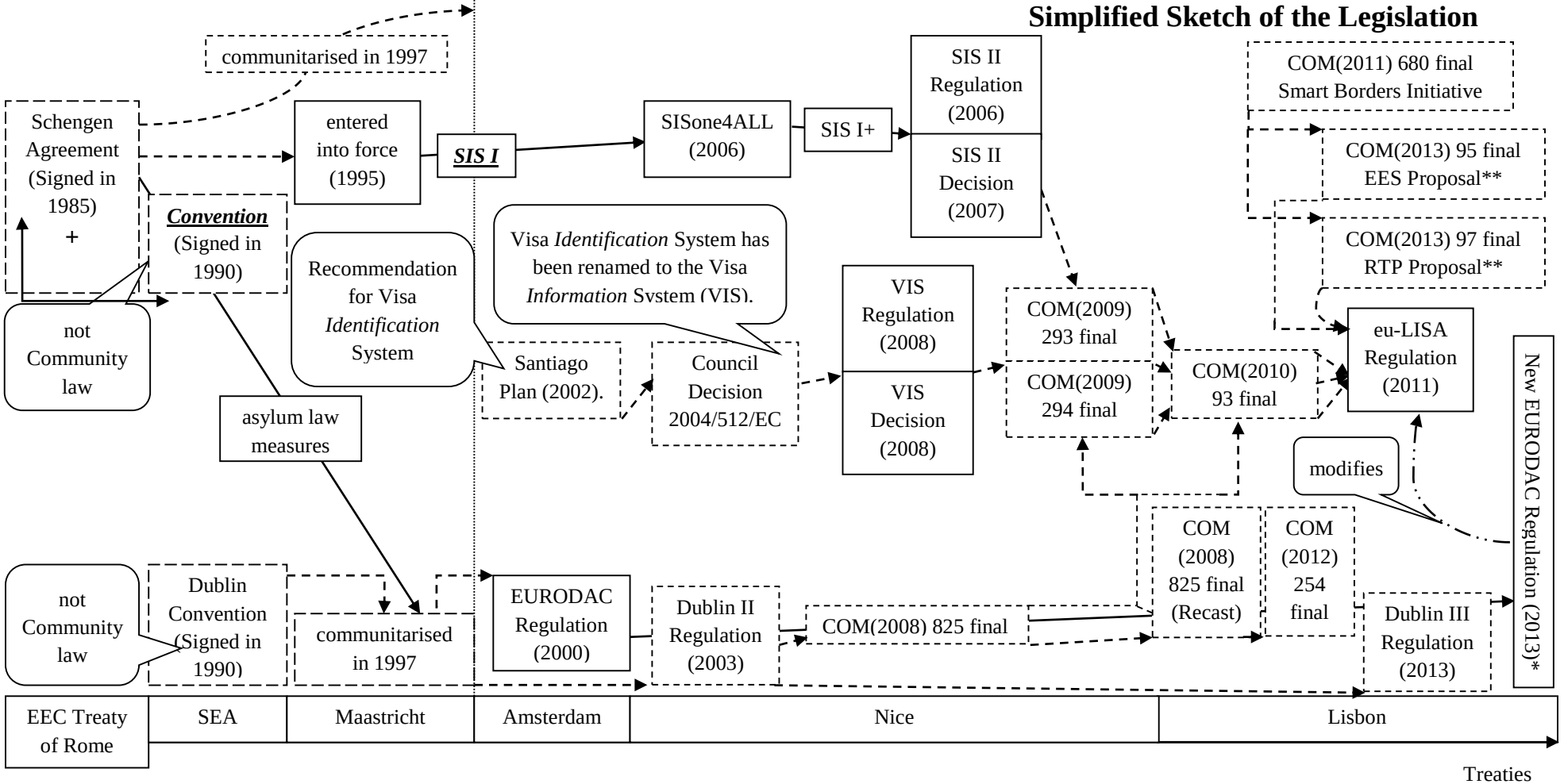
Legal and irregular migration are two sides of the same regulation field. Law enforcement large-scale IT systems approach the end points of legal and irregular migration, since they can be used to facilitate and to secure border crossings of EU and third country nationals. The smart borders initiative presents the newest endeavours for the development of new (and related) large-scale IT systems in the area of freedom, security and justice. New technologies shall be harnessed to meet all the requirements including enhancing security and facilitating travel at the external borders.

***

To extend the point of the problem's interpretation, the society's acceptance of new technologies in criminal justice is crucial to be taken into account. Concerns with a new technology will decrease if the technology is fully integrated, accepted in the society. Several unanswered question are raised by its combination with the pure type immigration control that is envisioned to 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. These questions are clearly connected to the double requirement of enhancing security and facilitating travel as it was the key underlying dilemma in the context of the current research. The presented results on security and openness of *Schengenland* may help in their strategic assessment, which may be the subject of a further study.

TABLE OF APPENDICIES

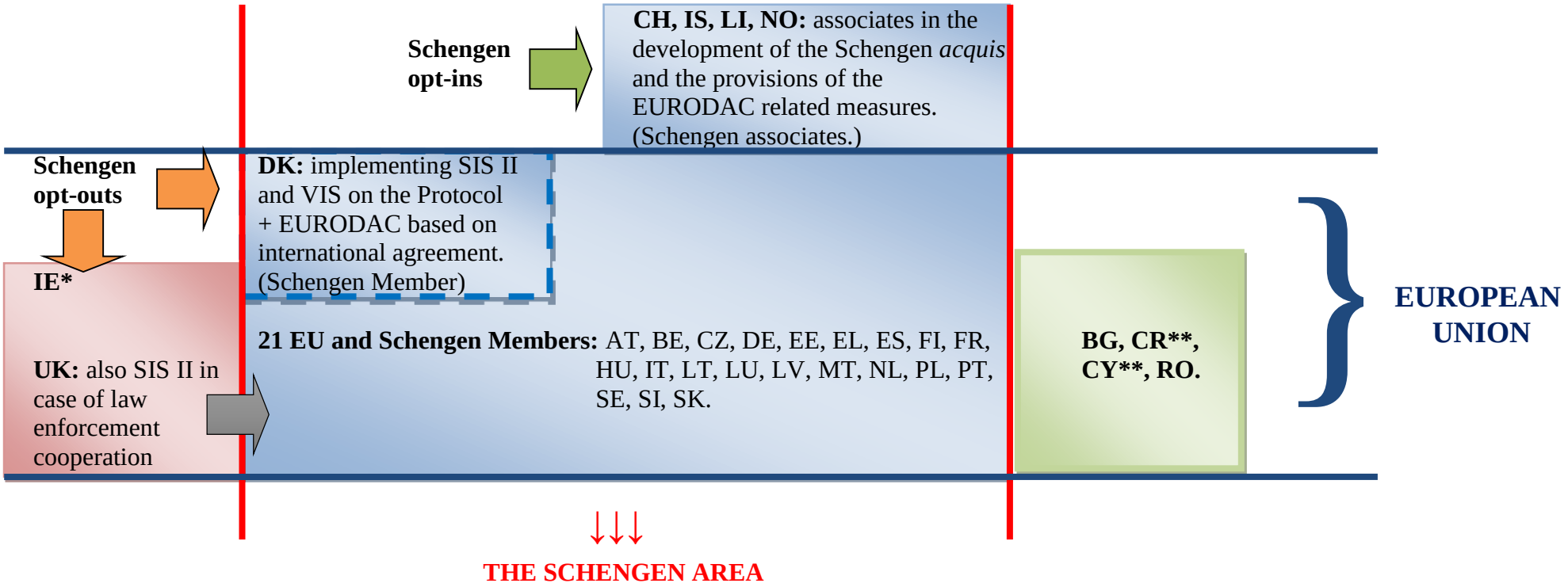
Appendix A: The Development of the Operational Management of EU Law Enforcement Large-Scale IT Systems – Simplified Sketch of the Legislation



* may be amended by COM(2014) 382 final

** together with COM(2013) 96 final

Appendix B: *La géométrie variable* – the Matrix of Scope of SIS II, VIS and EURODAC

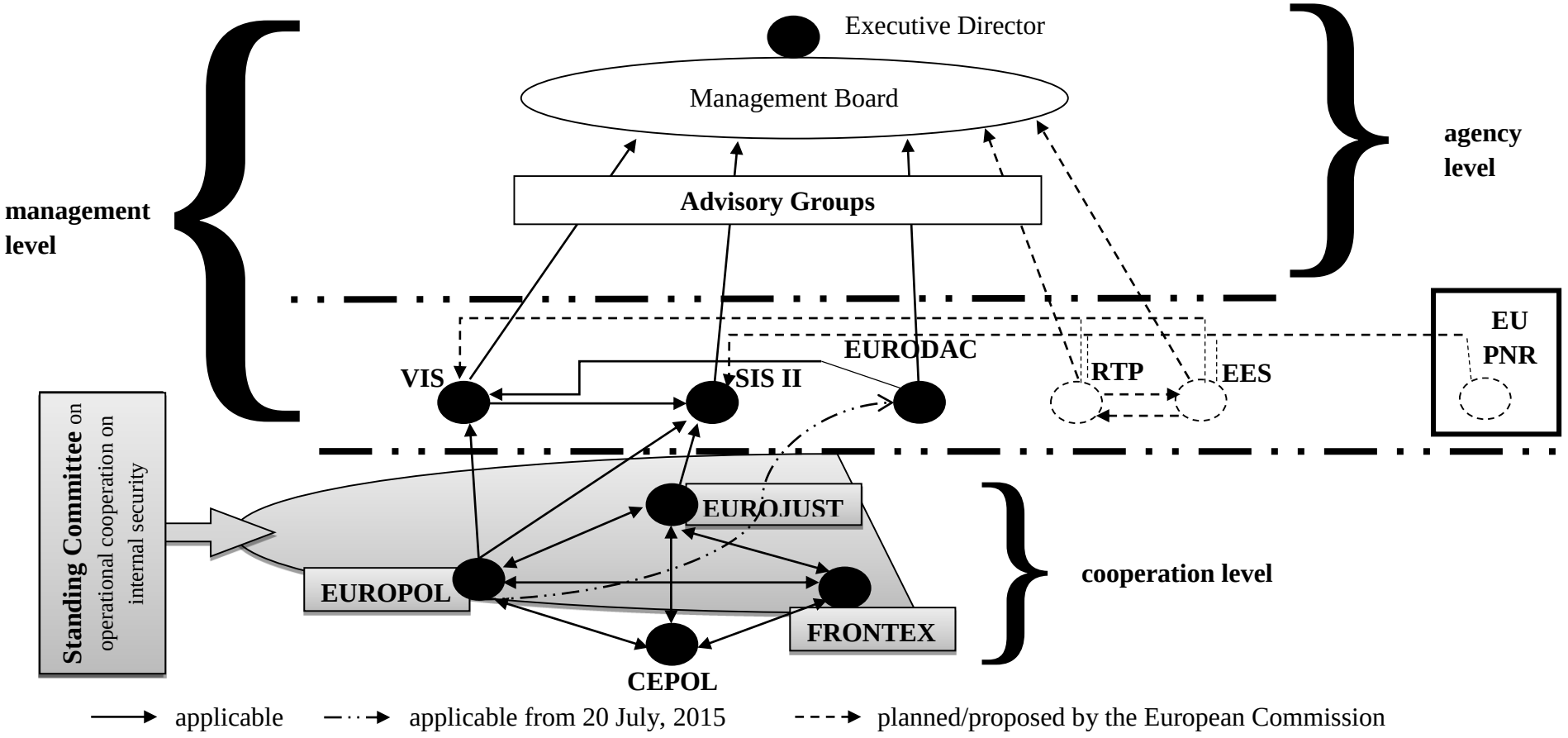


use SIS II, VIS and EURODAC; use EURODAC; use SIS II in case of law enforcement cooperation and EURODAC + obliged to the future use of VIS based on the accession treaties

* as of writing, preparation for joining SIS II in case of law enforcement cooperation

** as of writing, preparatory activities to be integrated into the SIS II

Appendix C: Relationship of eu-LISA with JHA Agencies and the Indirect Interconnectedness – the Extended Layer Model



Bibliography

Primary Sources

UN Documents

Conventions

The Universal Declaration of Human Rights (1948)

Convention Relating to the Status of Refugees (1951)

International Convention on the Elimination of All Forms of Racial Discrimination (1965)

International Covenant on Civil and Political Rights (1966)

Protocol

Protocol Relating to the Status of Refugees (1967)

CoE Documents

Convention

Convention for the Protection Human Rights and Fundamental Freedoms, Rome, 4.IX. 1950.

Judgements of the European Court of Human Rights

Mc Veigh and others v. United Kingdom, Application no. 8022/77, Commission decision of 18 March 1981.

Kinnunen v. Finland, Application no. 18291/91, Commission decision of 13 October 1993.

Van Kück v. Germany, Application no. 35968/97, judgment of 12 June 2003.

S. and Marper v the United Kingdom, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

EU Documents

Treaties

Single European Act, OJ L 169, 29.6.1987.

Treaty on European Union, OJ C 191, 29.7.1992.

Treaty of Amsterdam Amending the Treaty on European Union, the Treaties establishing the European Communities and Relates Acts, OJ C 340, 10.11. 1997, pp. 1-144.

Treaty of Nice Amending the Treaty on European Union, the Treaties establishing the European Communities and Certain Related Acts, OJ C 80, 10.3.2001, pp. 1-87.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 83, 3.30.2010, pp. 1-388.

Consolidated Version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13-390.

Charter of Fundamental Rights of the European Union, OJ C 83, 3.30.2010, pp. 389-403.

Treaty of Accession of Croatia (2012). OJ L 112, 24.4.2012.

Communitarised International Treaties

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, pp. 38-43.

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, pp. 40-47.

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, pp. 5-17.

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, pp. 52-79.

Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, pp. 13-18.

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, pp. 36-49.

Convention between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, Prüm, 27.5.2005. Source: 10900/05 Prüm Convention, Brussels, 7.7.2005.

Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention, 19.8.1997, OJ C 254, pp. 1-12.

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders. OJ L 239, 22.9.2000, pp. 19-62.

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, pp. 39-49.

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, pp. 8-12.

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, pp. 21-32.

Judgement of the Court of Justice of the European Union

Huber v Bundesrepublik Deutschland, Case C-524/06, reference for a preliminary ruling, judgement of 16 December 2008.

MA and Others vs. Secretary of State for the Home Department, Case C-648/11, request for a preliminary ruling, judgement of 6 June 2013.

International Agreements

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82, 21.3.2006, pp. 15-19.

Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to Australian customs service, OJ L 213, 8.8.2008, pp. 49-57.

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215, 11.8.2012, pp. 5-14.

Regulations

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, pp. 1-10.

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, pp. 1-22.

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, pp. 1-5.

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, pp. 1-10.

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, pp. 29-31.

Regulation (EC) 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105, pp. 1-32.

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, pp. 1-3.

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, pp. 4-23

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, pp. 60-81.

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, pp. 56-58.

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, pp.1-58.

Regulation (EU) No 439/2010 of the European Parliament and of the Council of 19 May 2010 establishing a European Asylum Support Office, OJ L 132, 29.5.2010, pp. 11-28.

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, pp. 19-22.

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, pp. 1-17.

Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 304, 22.11.2011, pp. 1-17.

Regulation (EU) No 603/2013 of the European Parliament and the Council of June 26 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 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 on requests for the comparison 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), OJ L 180, 29.6.2013, pp. 1-30.

Regulation (EU) No 604/2013 of the European Parliament and the Council of June 26 2013 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), OJ L 180, 29.6.2013, pp. 31-59.

Regulation (EU) No 1052/2013 of the European Parliament and the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ L 295, 6.11.2013, pp. 11-26.

Directives

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, pp. 31-39.

Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status, OJ L 326, 13.12.2005, pp.13-34.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75-82.

Directive 2008/115/EC of the European Parliament and the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nations, OJ L 348, 24.12.2008, pp. 98-107.

Council Decisions and Decisions of the European Parliament and of the Council

Council Decision 1999/435/EC of 20 May 1999 concerning the definition of the Schengen *acquis* for the purpose of determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the *acquis*, OJ L 176, 10.7.1999, pp. 1-16.

Council Decision 1999/436/EC of 20 May 1999 determining, in conformity with the relevant provisions of the Treaty establishing the European Community and the Treaty on European Union, the legal basis for each of the provisions or decisions which constitute the Schengen *acquis*, OJ L 176, 10.7.199, pp. 17-30.

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, pp. 43-47.

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, pp. 20-23.

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

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, pp. 44-48.

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, pp. 63-84.

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, pp. 3-4.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, pp. 1-11.

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, pp. 129-136.

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, p. 50.

Decision No 1105/2011/EU of the European Parliament and of the Council of 25 October 2011 on the list of travel documents which entitle the holder to cross the external borders and which may be endorsed with a visa and on setting up a mechanism for establishing this list, OJ L 287, 4.11.2011, pp. 9-12.

Council Implementing Decision (EU) 2015/215 of 10 February 2015 on the putting into effect of the provisions of the Schengen *acquis* on data protection and on the provisional putting into effect of parts of the provisions of the Schengen *acquis* on the Schengen Information System for the United Kingdom of Great Britain and Northern Ireland, OJ L 36, 12.2.2015, pp. 8-10.

Commission Regulation

Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 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 222, 5.9.2003, pp. 3-23.

Commission Decisions

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, pp. 62-64.

Commission Implementing Decision 2011/636/EU of 21 September 2011 determining the date from which the Visa Information System (VIS) is to start operation in a first region, OJ L 249, 27.9.2011, pp. 18-19.

Commission Implementing Decision 2012/233/EU of 27 April 2012 determining the date from which the Visa Information System (VIS) is to start operation in a second region, OJ L 117, 1.5.2012, pp. 9-10.

Commission Implementing Decision 2012/274/EU 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, pp. 20-22.

Commission Implementing Decision 2012/512/EU of 21 September 2012 determining the date from which the Visa Information System (VIS) is to start operation in a third region, OJ L 256, 22.9.2012, pp. 21-22.

Commission Implementing Decision 2013/122/EU of 7 March 2013 determining the date from which the Visa Information System (VIS) is to start operations in a fourth and a fifth region, OJ L 65, 8.3.2013, pp. 35-36.

Commission Implementing Decision 2013/493/EU of 30 September 2013 determining the third and last set of regions for the start of operations of the Visa Information System (VIS), OJ L 268, 10.10.2013, pp. 13-16.

Commission Implementing Decision 2014/540/EU of 28 August 2014 determining the date from which the Visa Information System (VIS) is to start operations in a 16th region, OJ L 258, 29.8.2014, pp. 8-10.

Commission Decision C(2014)9310/F1 on the request by Ireland to accept Regulation EU No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 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 on requests for the comparison 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), 11.12.2014.

Commission Implementing Decision 2015/731/EU of 6 May 2015 determining the date from which the Visa Information System (VIS) is to start operations in the 17th and 18th regions, OJ L 116, 7.5.2015, pp. 20-21.

Memorandum of Understanding

Memorandum of Understanding on Cooperation between Frontex and Eurojust, Warsaw, 18.12.2013.

EU Policy Documents

Action Plan of the Council and the Commission on How to Implement the Provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice, OJ C 19, 23.1.1999, pp. 1-15.

The Hague Programme: strengthening freedom, security and justice in the European Union OJ C 53, 3.3.2005. pp. 1-14.

Conclusions of the European Council

EUCO 23/11 European Council 23/24 June 2011, Conclusions, Brussels, 24.6.2011.

Commission Documents

COM(2007) 654 final Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, Brussels, 6.11.2007.

COM(2008) 68 final Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Examining the creation of a European Border Surveillance System (EUROSUR), Brussels, 13.2.2008.

COM(2008) 69 final Communication from the Commission to the European Parliament, the Council and the Committee of the Regions Preparing the next steps in border management in the European Union, Brussels, 13.2.2008.

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.

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.

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.

COM(2009) 66 final Proposal for the Regulation of the European Parliament and the Council establishing a European Asylum Support Office, Brussels, 18.2.2009.

COM(2009) 293 final 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, Brussels, 24.6.2009.

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.

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.

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.

COM(2010) 61 final Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), Brussels, 24.2.2010.

COM(2010) 93 final Amended Proposal a Regulation (EU) No .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, Brussels, 19.3.2010.

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.

COM(2011) 32 final Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 2.2.2011.

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, 1.6.2011.

COM(2011) 346 final Report from the Commission to the Parliament and the Council on the Development of the Visa Information System (VIS) in 2010 (submitted pursuant to Article 6 of Council Decision 2004/512/EC), Brussels, 14.6.2011.

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.

COM(2011) 873 final Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR), Brussels, 12.12.2011.

COM(2012) 11 final Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.12012.

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.

COM(2013) 95 final Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, Brussels, 28.2.2013.

COM(2013) 96 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP), Brussels, 28.2.2013.

COM(2013) 97 final Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, Brussels, 28.2.2013.

COM(2014) 154 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions An open and secure Europe: making it happen, Brussels, 11.3.2014.

COM(2014) 199 final Communication from the Commission to the European Parliament, the Council on EU Return Policy, Brussels, 28.3.2014.

COM(2014) 382 final Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 604/2013 as regards determining the Member State responsible for examining the application for international protection of unaccompanied minors with no family member, sibling or relative legally present in a Member State, Brussels, 26.6.2014.

COM(2015) 240 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions A European Agenda on Migration, Brussels, 13.5.2015.

COM(2015) 490/2 final Communication to the European Parliament, the European Council and the Council Managing the refugee crisis: immediate operational, budgetary and legal measures under the European Agenda on Migration, Brussels, 29.9.2015.

SWD(2013) 47 final Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing an entry/exit system to register entry and exit data of third-country nationals crossing the external borders of the Member States of the European Union, Brussels, 28.2.2013.

SWD(2013) 49 final Commission Staff Working Document, Detailed Explanation on the Proposal by Chapters and Articles, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council, Brussels, 28.2.2013.

SWD(2013) 50 final Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, Brussels, 28.2.2013.

SWD(2013) 52 final Commission Staff Working Document, Detailed Explanation on the Proposal by Chapters and Articles, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, Brussels, 28.2.2013.

Joint Statements

Statement 235/06 Joint Statements of the long-term management of SIS II and VIS. 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, p. 102.

Other Preparatory Documents

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

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

13305/09 Paquet législatif portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice – Localisation du siège de l'agence, Brusseles, 15.9.2009.

13484/09 Comments 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, Brussels, 21.9.2009.

11312/4/09 Proposal for an Information Management Strategy for the EU internal security, Brussels, 6.11.2009.

17024/09 The Stockholm Programme – An open and secure Europe serving and protecting the citizens, Brussels, 2.12.2009.

5038/10 Proposition de règlement du Parlement européen et du Conseil portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice – siège de l'agence, Brusseles, 7.1.2010.

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.

5816/10 Interim report on cooperation between JHA Agencies, Brussels, 29.1.2010.

8196/10 Commentaires de la délégation française sur la proposition de règlement du Parlement européen et du Conseil portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice - Article 15 et suivants, Brussels, 31.3.2010.

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

5676/11 Draft Scorecard – Implementation of the JHA Agencies report, Brussels, 25.1.2011.

EUCO 79/14 European Council 26/27 June 2014: Conclusions, Brussels, 27.6.2014.

Academic Literature

Books and Monographs

Andersen, Stine, "Non-Binding Peer Evaluation within an Area of Freedom, Security and Justice", in Holzhacker, Ronald L. and Luif, Paul (ed.), *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation after the Lisbon Treaty*, New York, Springer, 2014, pp. 29-48.

Bárd, Petra (ed.), *The Rule of Law and Terrorism*, Budapest, HVG-ORAC Publishing Ltd., 2015.

Beck, Ulrich, *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Frankfurt am Main, Subrkamp Verlag, 1986.

Blutman, László, "A nem uniós állampolgárok szabad mozgására vonatkozó szabályozás a mai Európai Unióban", in Tóth, Judit (ed.), *Schengen – A magyar-magyar kapcsolatok az uniós vízumrendszer árnyékában*, Budapest, Lucidus, 2000, pp. 63-92.

Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Heidelberg, Springer, 2012.

Boeles, Pieter, *Fair Immigration Proceedings in Europe*, The Hague, Martinus Nijhoff Publishers, 1997.

Boeles, Pieter and Heijer, Maarten den and Lodder, Gerrie and Wouters, Kees, *European Migration Law*, Antwerpen and Oxford and Portland, Intersentia, 2009.

Brouwer, Evelin, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, "Immigration and Asylum Law and Policy in Europe", vol. 15, Leiden, Martinus Nijhoff Publishers, 2008.

Coleman, Nils, *European Readmission Policy: Third Country Interests and Refugee Rights*, "Immigration and Asylum Law and Policy in Europe", vol. 16, Leiden, Martinus Nijhoff Publishers, 2009.

Ericson, Richard V. and Haggerty, Kevin D., *Policing the Risk Society*, New York, Oxford University Press, 2001 (reprint), originally published in 1997.

Giddens, Antony, *The Consequences of Modernity*, Stanford, Stanford University Press, 1990.

Kardos Kaponyi, Elisabeth, *Fight Against Terrorism and Protecting Human Rights: Utopia or Challenge?*, Budapest, BCE (Budapesti Corvinus Egyetem), 2012.

Laukó, Károly (ed.), *Bűnüldözés, adatvédelem, Schengen*, Budapest, BM Kiadó, 2004.

Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, 2nd ed., Washington, CQ Press, 2003.

Meloni, Annalisa, *Visa Policy within the European Union Structure*, Berlin, Springer, 2006.

Mohay, Ágoston and Szalayné Sándor, Erzsébet, "The Protection of Fundamental Rights Post Lisbon", in Laffranque, Julia (ed.), *The protection of fundamental rights post-Lisbon: The interaction between the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights*

and national constitutions, Tallinn, Tartu University Press, 2012, pp. 501-532.

Opeskin, Brian and Perruchoud, Richard and Redpath-Cross, Jillyanne (ed.), *International Migration Law,* New York, Cambridge University Press, 2012.

Pajó, Ágnes, "Schengen, az EU kapujának őre", in *Az információs jogok kihívásai a XXI. században*, Budapest, Adatvédelmi Biztos Irodája, 2009, pp. 121-138.

Papagianni, Georgia (ed.), *Institutional and Policy Dynamics of EU Migration Law*, "Immigration and Asylum Law and Policy in Europe", vol. X., Leiden, Martinus Nijhoff Publications, 2006.

Pattavina, April (ed.), *Information Technology and the Criminal Justice System*, University of Massachusetts at Lowell, Sage Publications, 2005.

Peers, Steve (ed.), *EU Immigration and Asylum Law: Text and Commentary*, "Immigration and Asylum Law and Policy in Europe", vol. XII., Leiden, Martinus Nijhoff Publications, 2006.

Peers, Steve, *EU Justice and Home Affairs Law*, "Oxford European Community Law Series", 2nd ed., Oxford and New York, Oxford University Press, 2006.

Sandor-Szalay, Elisabeth, "EU and EHCR - de Facto and Formal Accession of the EU to the European Convention on Human Rights", in: Jaskiernia, Jerzy (ed.), *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka: International Standards' Influence on Development of Democracy and Protection of Human Rights*, Warsaw, Wydawnictwo Sejmowe, 2013, pp. 295-307.

Journals and Periodicals

Adamson, Fiona B., "Crossing Borders: International Migration and National Security", *International Security,* 31(1), pp. 165-199.

Aldrich, Richard, J., "Transatlantic Intelligence and Security Cooperation", *International Affairs (Royal Institute of International Affairs 1944-),* 80(4), pp. 731-753.

Andreas, Peter, "Redrawing the Line: Borders and Security in the Twenty-First Century", *International Security,* 28(2), pp. 78-111.

Balázs, László, dr., "A visszafogadási egyezmények alkalmazásának tapasztalatai az Európai Unióban, illetve a hazai joggyakorlatban", *Migráció és Társadalom,* 1(2), 2012, pp. not indicated.

Baldaccini, Anneliese, "Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases", *European Journal of Migration and Law,* 10(1), 2008, pp. 31-49.

Bauböck, Rainer, "Towards a Political Theory of Migrant Transnationalism", *International Migration Review,* 37(3), 2003, pp. 700-723.

Bárd, Petra and Borbíró, Andrea, "Kontrollálatlan kontrolltársadalom", *Kriminológiai tanulmányok,* 47(1), 2010, pp. 87-112.

Beck, Ulrich, "Living in the world risk society – A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics", *Economy and Society,* 35(3), 2006, pp. 329-345.

Besters, Michiel and Brom, Frans W.A., "'Greedy' Information Technology: The Digitalization of the European Migration Policy", *European Journal of Migration and Law,* 12(4), 2010, pp. 455-470.

Bigo, Didier, "The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts", *Security Dialogue,* 45(3), 2014, pp. 209-225.

Blasi Casagran, Cristina, "The Future EU PNR System: Will Passenger Data be Protected?", *European Jorunal of Crime, Criminal Law and Criminal Justice,* 23(3), 2015, pp. 241-257.

Broeders, Dennis, "The New Digital Borders of Europe – EU Database and the Surveillance of Irregular Migrants", *International Sociology,* 22(1), 2007, pp. 71-92.

Brouwer, E.R., "Eurodac: Its Limitations and Temptations", *European Journal of Migration and Law*, 4(2), 2002, pp. 231-247.

Carrera, Sergio, "What Does Free Movement Mean in Theory and Practice in an Enlarged EU?", *European Law Journal*, 11(6), 2005, pp. 699-721.

Császár, Mátyás, "Az Európai Unió intézményi aktusai a Lisszaboni Szerződés után", *Európai jog,* 11(1), 2011, pp. 31-39.

De Capitani, Emilio, "The Schengen system after Lisbon: from cooperation to integration", *ERA Forum,* 15(1), 2014, pp. 101-118.

Dóczi, Zoltán, "Internal Security of *Schengenland*: What do we need SIS II for?", *BiztPol Affairs,* 2(2), 2014, pp. 18-28.

Dóczi, Zoltán, "The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice", *Acta Juridica Hungarica,* 54(2), 2013, pp. 164-183.

Haggerty, K. D. and Ericson, R. V.: "The Surveillant Assemblage", *British Journal of Sociology,* 51(4), 2000, pp. 605–622.

Hailbronner, Kay, "Readmission Agreements and the Obligation on States under Public International Law to Readmit their Own and Foreign Nationls", *Zeitschrift*

für ausländisches öffentliches Recht und Völkerrecht, vol. 57, 1997, pp. 1-49.

Hendow, Maegan and Cibea, Alina and Kraler, Albert, "Using technology to draw borders: fundamental rights for the Smart Borders initiative", *Journal of Information, Communication and Ethics in Society*, 13(1), 2015, pp. 39-57.

Jandl, Michael, "Irregular Migration, Human Smuggling, and the Eastern Enlargement of the European Union", *International Migration Review,* 41(2), 2007, pp. 291-315.

Kaponyi, Erzsébet, "A Közös Európai Menekültügyi Rendszer és az alapvető jogok védelme", *Pro Publico Bono Online Támop Speciál,* 1(1), pp. 1-58.

Kohara, Masahiro, "International Power and International Security", *Progress in Informatics*, 1(1), 2005, pp. 39-46.

Neumayer, Eric, "Unequal Access to Foreign Spaces: How States Use Visa Restrictions to Regulate Mobility in a Globalized World", *Transactions of the Institute of British Geographers,* New Series, 31(1), 2006, pp. 72-84.

Newman, Abraham L., "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Protection Directive", *International Organisation,* 62(1), 2008, pp. 103-130.

Mahmood, Shiraz, "The Schengen Information System: An Inequitable Data Protection Regime", *International Journal of Refugee Law*, 7(2), 1995, pp. 179-200.

Mitsilegas, Valsamis, "Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, and Strengthening the State", *Indiana Journal of Global Legal Studies,* 19(1), pp. 3-60.

Peers, Steve, "An EU Immigration Code: Towards a Common Immigration Policy", *European Journal of Migration and Law*, 14(1), 2012, pp. 33-61.

Peers, Steve, "Key Legislative Developments on Migration in the European Union: SIS II", *European Journal of Migration and Law*, 10(1), 2008, pp. 77-104.

Peers, Steve, "Legislative Update: EC Immigration and Asylum Law, 2008: Visa Information System", *European Journal of Migration and Law*, 11(1), 2009, pp. 69-94.

Roots, Lehte, "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies,* 5(2), pp. 108-129.

Şchiopu, Aura and Bobin, Florin, "European Agenda on Security for 2015-2020, Instrument Supporting the Joint Action of the Members States against New Challenges", *European Journal of Public Order and National Security,* 6(2), 2015, pp. 33-36.

Schuster, Liza, "Dublin II and Eurodac: examining the (un)intended(?) consequences", *Gender, Place & Culture: A Journal of Feminist Geography,* 18(3), 2011, pp. 401-416.

Stepper, Péter, "The Challenges for Common European Asylum Policy: The Practice of Detention in Hungary", *BiztPol Affairs,* 2(2), 2014, pp. 29-49.

Szalayné Sándor, Erzsébet, "Alapjogok (európai) válaszúton – Lisszabon után", *Jogtudományi Közlöny,* 68(1), pp. 15-27.

Taylor, Ian, "The International Drug Trade and Money-Laundering: Border Controls and Other Issues", *European Sociological Review,* 8(2), 1992, pp. 181-193.

van der Ploeg, Irma, "The illegal body: 'Eurodac' and the politics of biometric identification", *Ethics and Information Technology,* 1(4), 1999, pp. 295-302.

Vogel, Dita, "Migration Control in Germany and the United States", *International Migration Review,* 34(2), 2000, pp. 390-422.

Wood, William B., "Forced Migration: Local Conflicts and International Dilemmas", *Annals of the Association of American Geographers,* 84(4), 1994, pp. 607-634.

Zaiotti, Ruben, "Performing Schengen: myths, rituals and the making of European territoriality beyond Europe", *Review of International Studies,* 37(2), 2011, pp. 537-556.

Lecture

Malmström, Cecilia, *Europe and migrants – progress and setbacks,* The Tore Browaldh Lecture 2014, "Tore Browaldh Lecture Series", Gothenburg University, School of Business, Economics and Law, 3.11.2014, 16.15-18.00.

On-Line Sources

Aus, Jonathan P., "Eurodac: A Solution Looking for a Problem?", Working Paper No. 9, AREN, Centre for European Studies, University of Oslo, May, 2006, https://www.sv.uio.no/arena/english/research/publications/arena-publications/workingpapers/working-papers2006/wp06_09.pdf, [1.12.2014.].

Berger, Melissa and Heinemann, Friedrich, "Why and how there should be more Europe in asylum policies", Center for European Economic Research, January 2016, http://ftp.zew.de/pub/zew-docs/policybrief/pb01-16.pdf, [20.1.2016.].

Bertozzi, Stefano, "Schengen: Achievements and Challenges in Managing an Area Encompassing 3.6 million km²", CEPS Working Document No. 284/February 2008,

Centre for European Policy Studies, 2008, http://www.ceps.eu/system/files/book/1597.pdf, [1.12.2014.].

"Best Practice Operational Guidelines for Automated Border Control (ABC) Systems", *FRONTEX Research and Development Unit,* 31.8.2012, http://www.frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf, [9.3.2013.].

Bigo, Didier and Brouwer, Evelien and Carrera, Sergio and Guild, Elspeth and Guittet, Emmanuel-Pierre and Jeandesboz, Julien and Ragazzi, Francesco and Scherrer, Amandine, "The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda", *CEPS Paper in Liberty and Security in Europe*, No. 81, February 2015, Centre for European Policy Studies, https://www.ceps.eu/system/files/LSE81Counterterrorism.pdf, [7.1.2016.].

Bigo, Didier and Carrera, Sergio and Hayes, Ben and Hernanz, Nicholas and Jeandesboz, Julien, "Justice and Home Affairs *Databases* and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals", *CEPS Paper in Liberty and Security in Europe*, No. 52, December 2012, Centre for European Policy Studies, http://aei.pitt.edu/38961/1/No_52_JHA_Databases_Smart_Borders[1].pdf, [10.3.2013.].

Brouwer, Evelin, "The Other Side of the Moon: The Schengen Information System and Human Rights: A Task for National Courts", CEPS Working Document No. 288/April 2008, Centre for European Policy Studies, 2008, http://www.ceps.eu/files/book/1642.pdf, [27.10.2014.].

Dóczi, Zoltán, "Good Practices in the return and reintegration of irregular migrants: Member States' entry bans policy & use of readmission agreements between Member States and third countries", *European Migration Network (EMN) Focussed Study 2014: Hungary*, Brussels, European Commission, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-studies/13a.hungary_rentry_bans_and_reintegration_study_final_en_version.pdf [3.9.2014.].

"Kézikönyv a menekültügyre, határokra és bevándorlásra vonatkozó európai jogról", *Európai Unió Alapjogi Ügynöksége, Európa Tanács,* 2. kiadás, Belgium, 2014, http://fra.europa.eu/sites/default/files/handbook-law-asylum-migration-borders-2nded_hu.pdf, [1.12.2014.].

Hayes, Ben, Dr. and Vermeulen, Mathias, Borderline: The EU's New Border Surveillance Initiatives, "Assessing the Costs and Fundamental Rights Implications of EUROSUR and the 'Smart Borders' Proposal", Heinrich Böll Foundation, June 2012, http://www.boell.de/downloads/DRV_120523_BORDERLINE_-_Border_Surveillance.pdf, [2.3.2013.].

Gonzalez-Fuster, Gloria and Gutwirth, Serge, "When 'digital borders' meet 'surveilled geographical borders': Why the future of EU border management is a problem", 2011, http://works.bepress.com/cgi/viewcontent.cgi?article=1055&context=serge_gutwirth, [10.3.2013.].

Guild, Elspeth and Carrera, Sergio and Geyer, Florian, "The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?", *CEPS Policy brifing*, No. 154, March 2008, Centre for European Policy Studies, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334058, [10.3.2013.].

Jeandesboz, Julien and Bigo, Didier and Hayes, Ben and Simon, Stephanie, "The Commission's legislative proposals on Smart Borders: their feasibility and costs", *European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens and Constitutional Rights, Justice, Freedom and Security*, Brussels, 2013, PE 493.026, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493026/IPOL-LIBE_ET(2013)493026_EN.pdf, [24.10.2014.].

"Long-Term Forecast, Flight Movements 2010-2030", *EUROCONTROL*, Released Issue, Edition Number: v1.0, 17.12.2010, https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/forecasts/long-term-forecast-2010-2030.pdf, [2.3.2013.].

"Smart Borders Package", *European Commission, DG Home Affairs,* http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130228_01_en.htm#/c_, [9.3.2013.].

Press Releases

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

7215/13 "Press Release, 3228th Council meeting, Justice and Home Affairs", *Council of the European Union Press,* Brussels, 7-8.3.2013.

9179/12 "Press Release, 3162th Council meeting, Justice and Home Affairs", *Council of the European Union Press,* Luxembourg, 26-27.4.2012.

IP/10/1535 "Commission presents a new set of EU measures to better protect European citizens", *Europa Press Releases RAPID,* Brussels, 22.11.2010.

IP/11/781 "European Council: The Commission will take forward and intensify the work on migration and asylum policy", *Europa Press Releases RAPID*, Brussels, 24.6.2011.

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

List of the Author's Related Publications

Major English-Language Publications

Peer Reviewed Journal Articles

Dóczi, Zoltán, "Internal Security of *Schengenland*: What do we need SIS II for?", *BiztPol Affairs,* 2(2), 2014, pp. 18-28.

Dóczi, Zoltán, "The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice", *Acta Juridica Hungarica,* 54(2), 2013, pp. 164-183.

Paper

Dóczi, Zoltán, "Good Practices in the return and reintegration of irregular migrants: Member States' entry bans policy & use of readmission agreements between Member States and third countries", *European Migration Network (EMN) Focussed Study 2014: Hungary*, Brussels, European Commission, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-studies/13a.hungary_rentry_bans_and_reintegration_study_final_en_version.pdf [3.9.2014.]. Author certification may be emailed by request.

Major Hungarian-Language Publication

Paper

Dóczi, Zoltán, "Jó tagállami gyakorlatok a harmadik országok illegálisan tartózkodó állampolgárai kiutasításának és visszailleszkedésének tekintetében: A tagállamok beutazási és tartózkodási tilalmi politikája & a tagállamok és harmadik országok között fennálló visszafogadási egyezmények gyakorlata", *European Migration Network (EMN) Focussed Study 2014: Hungary*, Brussels, European Commission, 2014, http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/european_migration_network/reports/docs/emn-studies/13b_hungary_national_report_return_reintegration_hu.pdf [8.11.2014.]. Author certification may be emailed by request.