University of Pécs,

Faculty of Law, Doctoral School of Law

Zoltán Dóczi

Synopsis of

Ph.D. dissertation

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

Supervisor:

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

habilitated professor

Gothenburg, 2016

I. Research Scope

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. 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.

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 (hereinafter: EU) through observing eu-LISA[1], 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.

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

[1] Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

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 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.

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 multitude of existing and even the planned systems raises the problem of their connectedness with each other and with Justice and Home Affairs Agencies (hereinafter: JHA Agencies).[4] 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.

[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] 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.

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.

II. Methodology and Analysis

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.

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.

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. 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.

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. 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.

In line with the proposed methodological tool, these systems has 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 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.

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 if the same social preference patterns come out of the analyses of existing and of 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.

III. Results

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.

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.[5]

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, that 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.[6] 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.

[5] Aldrich, Richard, J., "Transatlantic Intelligence and Security Cooperation", *International Affairs (Royal Institute of International Affairs 1944-),* 80(4), p. 736.

[6] Pattavina, April (ed.), *Information Technology and the Criminal Justice System,* University of Massachusetts at Lowell, Sage Publications, 2005, pp. 261-271.

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.

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 the so-called *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". [7] 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 aslo 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.

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

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

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.

Again, 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.[8] Moreover, less unsatisfactory data transfer is observable not only on the management but also on the cooperation level.

All in all, economies of scale and security orientation compromise the respect of human rights standards. Therefore, according to the proposed methodological 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.[9] 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

[8] 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. 369.

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

hand, accountability of the European Agencies is ensured by the European Parliament and the European Data Protection Supervisor. Furthermore, the European Court of Justice[10] 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 to 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.

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".[11] 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.

To challenge the above results, comparable planned systems are the Entry/Exit System (hereinafter: EES) and the Registered Traveller Programme (hereinafter: RTP) restrictively to transparency due to its indirect and complementary relation to law enforcement purpose and patterns of PNRs[12] which are limited due to the established

[10] *Ibid*, Art. 24, p. 13.

[11] 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, quoted from the title.

[12] PNR: Passenger Name Record.

theoretical framework of EU law enforcement large-scale IT systems. Therefore, the Proposal for an EU PNR[13] 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.

As far as the respect of human rights is concerned, the Proposal for an EU PNR and the EES Proposal[14] are fundamentally different, since EU PNR will use unverified data for profiling purposes. Its results are planned to be used pre-emptively. In contrast, 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 reside 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

[13] 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.

[14] 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.

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. However, 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.

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.

Concerning respect of human rights indicator, based on profiling results of PNR data, persons may be denied for acts predicted to be committed by them. It matches the universes established by BIGO.[15] 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

[15] Bigo, Didier, The (in)securitization practices, *op. cit.,* pp. 209-225.

data protection principles within the area of freedom, security and justice.[16] 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 reached using Automated Border Control systems that are just plans in several Member States.

Besides, it shall not be mixed that the not optimal operation concerning social beneficiality is not the equal to not 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

[16] 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.

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.

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.

IV. 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.